NORTON ROSE FULBRIGHT

International Comparative Legal Guides

Practical cross-border insights into digital health law

Digital Health 2026

Seventh Edition

Contributing Editor

Roger Kuan

US Head of Digital Health and Precision Medicine Practice

Norton Rose Fulbright

iclg International Comparative Legal Guides



ISBN 978-1-83918-480-2
ISSN 2633-7533

Published by
Global Legal Group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
customer.service@glgroup.co.uk
www.iclg.com

Publisher
Ben Lawless

Production Editor
Maya Tyrrell

Head of Production
Suzie Levy

Creative Lead
Wilfried Tshikana-Ekutshu

CEO
Jason Byles

Printed by
Ashford Colour Ltd.

Cover image
iStock

Strategic Partners

iclg International Comparative Legal Guides

Digital Health 2026

Seventh Edition

Contributing Editor:

Roger Kuan
Norton Rose Fulbright

©2026 Global Legal Group Limited.
All rights reserved. Unauthorised reproduction by any means, digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Introductory Chapter

1 Introduction
Roger Kuan, Norton Rose Fulbright
David Wallace, Johnson & Johnson

Expert Analysis Chapters

8 The Bio-Industrial Technology Stack: A New Framework for National Sovereignty in the Century of Biology
Dr. Milad Alucozai, Jason Novak, Dr. Nathanael Green & Sophia Poirier, Norton Rose Fulbright

22 The Geopolitical Tipping Point: Forecasting Global Bio-Industrial Technology Stack (BITS) Dominance Through 2050
Dr. Milad Alucozai, Jason Novak, Dr. Nathanael Green & Ebony Christian, Norton Rose Fulbright

32 Evolution of Digital Health Reimbursement in the United States, Germany, the United Kingdom and France
Stephen A. Hull, Tarek Hamdan, Kirstin Osthoff & Dr. Eric Lam, Avania B.V.

39 Regulatory Strategy for Digital Therapeutics and Artificial Intelligence-Enabled Devices
Dr. Acacia Parks, Nick Butt, Sophia Farcas & Dr. Angela Johnson, Avania B.V.

Q&A Chapters

53 **Austria**
Dr. Daniel Larcher, ATLAS Attorneys at Law
Dr. Mariella Rieder, Prewave GmbH

63 **Belarus**
Kirill Laptev, Vladislav Zhavnerchik,
Anastasiya Pyshnaya-Muryna & Anna Zhdanovich,
Anischenko Laptev

75 **Belgium**
Olivier Van Obberghen, Pieter Wyckmans,
Amber Cockx & Chaline Sempels, Quinz

89 **Chile**
Mónica Pérez, José Ignacio Mercado, Camila Suárez &
Mariana Guzmán, Carey

99 **China**
Yong Kai Chang, Chaoran (Oliver) Zhu &
Jianing (Joy) Qiu, Allen & Gledhill LLP Shanghai
Representative Office

109 **France**
Catherine Mateu & Pierre Camadini,
Armengaud Guerlain

118 **Germany**
Jana Grieb, Steffen Woitz, Dr. Claus Färber &
Dr. Christian Lebrecht, McDermott Will & Schulte

131 **Israel**
Adv. Eran Bareket & Adv. Alexandra Cohen,
Gilat, Bareket & Co., Reinhold Cohn Group

144 **Italy**
Sonia Selletti, Claudia Pasturenzi & Chiara Screpanti,
Astolfi e Associati Studio Legale

155 **Japan**
Masanori Tosu & Kenji Tosaki,
Nagashima Ohno & Tsunematsu

164 **Korea**
Jin Hwan Chung, Eileen Jaiyoung Shin & Sungil Bang,
Lee & Ko

173 **Lithuania**
Raminta Matulytė, Irma Kunickė, Dovydas Gudžiūnas &
Marijus Dingilevskis, Sorainen

182 **Mexico**
Carla Calderón, Marina Hurtado Cruz,
Daniel Villanueva & Carlos Vela Treviño,
Baker McKenzie Abogados, S.C.

195 **Singapore**
Gloria Goh, Koh En Ying, Tham Hsu Hsien &
Alexander Yap, Allen & Gledhill LLP

207 **Switzerland**
Tobias Meili, Carlo Conti, Martina Braun &
André S. Berne, Wenger Plattner

218 **Taiwan**
Tsung-Yuan Shen, Rachel Chen & Nita Ye,
Lee and Li, Attorneys-at-Law

228 **United Kingdom**
Pieter Erasmus, Emma Drake, Tristan Sherliker &
Mario Subramaniam, Bird & Bird

241 **USA**
Roger Kuan, Jason Novak & Apurv Gaurav,
Norton Rose Fulbright

From the Publisher

Welcome to the seventh edition of *ICLG – Digital Health*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to digital health laws and regulations around the world, and is also available at www.iclg.com.

This year, the *Guide* has an introductory chapter which provides an overview of digital health.

In addition, four expert analysis chapters cover the bio-industrial technology stack, evolution of digital health reimbursement in the United States, Germany, the United Kingdom and France, and regulatory strategy for digital therapeutics and AI-enabled devices.

The question-and-answer chapters, which in this edition cover 18 jurisdictions, provide detailed answers to common questions raised by professionals dealing with digital health laws and regulations.

As always, this publication has been written by leading digital health lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editor Roger Kuan of Norton Rose Fulbright for his leadership, support and expertise in bringing this project to fruition.

Ben Lawless
Publisher
Global Legal Group



Introduction


Roger Kuan


David Wallace

Norton Rose Fulbright
Johnson & Johnson

What is Digital Health?

The rapid convergence of digital technologies with healthcare over the past decade has fundamentally reshaped how healthcare is developed, delivered, reimbursed, and regulated. What began as digitisation of records and workflows has, by 2026, evolved into artificial intelligence (AI)-enabled, data-native healthcare systems that increasingly operate in real time and at population scale.

Digital health now represents a shift away from episodic, provider-centric care toward continuous, patient-centred, data-driven care models. These models integrate clinical data, real-world evidence, genomics, imaging, wearable and sensor data, and patient-reported outcomes to support individualised prevention, diagnosis, treatment, and monitoring. The modern digital health paradigm emphasises personalisation, interoperability, automation, and outcomes-based care, supported by cloud infrastructure and advanced analytics.

A defining change in 2026 is the transition of AI from experimental deployment to embedded clinical and operational infrastructure forcing digital health companies to treat AI models as regulated product components subject to lifecycle controls, auditability, and post-market monitoring. AI is now routinely used for clinical decision support, workflow automation, triage, imaging interpretation, drug development, and population health management, with regulators and payors increasingly demanding transparency, validation, and post-market performance monitoring.

At the same time, governments and regulators have moved aggressively to address trust, safety, and accountability. Regulatory frameworks for software as a medical device (SaMD), AI/machine learning (ML)-enabled medical devices, digital therapeutics (DTx), and real-world data have matured, reducing uncertainty while raising the bar for evidence generation, cybersecurity, data governance, and lifecycle compliance.

From a market perspective, digital health growth has continued, but with a clear shift from speculative adoption to enterprise-scale procurement, platform consolidation, and reimbursement-aligned deployment. Health systems and life sciences companies now prioritise solutions that demonstrate measurable clinical outcomes, cost reduction, and workflow efficiency, rather than standalone point solutions. For digital health companies, the post-pandemic market has shifted decisively from rapid pilot adoption to disciplined, enterprise-scale procurement. Buyers now prioritise regulatory readiness, reimbursement alignment, cybersecurity posture, and demonstrable outcomes over feature velocity or novelty. A November 2020 report by Precedence Research published on *GlobeNewsWire* indicates that the global digital health market is poised to grow at a compound annual growth rate of around 27.9% over the next seven years to reach approximately US$833.44 billion by 2027.[1]

Digital Health Ecosystem

The digital health ecosystem continues to consist of five core constituents, but their roles and interactions have materially evolved.

Life sciences companies

Life sciences companies now integrate digital health across the full product lifecycle – from AI-enabled drug discovery and digital biomarkers in clinical trials to companion software, real-world evidence generation, and post-market surveillance. Software, data, and algorithms are increasingly treated as regulated product components, not ancillary tools, particularly in precision medicine, digital diagnostics, and combination products.

Pharmacies

Pharmacies have expanded beyond traditional dispensing roles to become digital care-access points, supporting remote patient monitoring, medication adherence programmes, pharmacogenomic services, and integration with telehealth and hospital-at-home models. Data interoperability and last-mile digital fulfilment are now core competitive differentiators.

Providers

Providers and health systems have shifted toward hybrid care models that combine in-person care with virtual care, remote monitoring, and AI-supported clinical workflows. Provider adoption in 2026 is increasingly driven by labour constraints, burnout reduction, and automation of administrative tasks, with AI copilots and ambient documentation becoming standard in many clinical settings.

Payors

Payors play a central role in shaping digital health adoption through coverage decisions, value-based reimbursement models, and outcomes measurement. By 2026, payors are

more actively engaging in digital health validation, requiring real-world performance data, cybersecurity assurances, and economic evidence before reimbursement or large-scale deployment.

Patients

Patients are no longer passive recipients of care but active participants in data generation, care navigation, and long-term condition management. Consumer expectations around transparency, personalisation, data access, and digital experience now directly influence provider and payor procurement decisions, as well as regulatory policy.

Role of digital health solutions

Despite advances, ecosystem participants still face fragmentation across data systems, regulatory regimes, reimbursement models, and operational workflows. Modern digital health solutions are therefore less about isolated innovation and more about infrastructure, orchestration, and trust.

In 2026, successful digital health solutions:

- Enable secure, interoperable data exchange across clinical, research, and commercial settings.
- Support AI-driven decision-making with regulatory-grade validation and governance.
- Integrate seamlessly into clinical workflows rather than adding burden.
- Align with reimbursement and value-based care models.
- Demonstrate measurable clinical, economic, and operational outcomes.

The result is an ecosystem increasingly oriented toward scalable, evidence-based, and regulation-ready digital health platforms, rather than experimental or consumer-only technologies.

Traditional Healthcare Paradigm

"One size fits all" approach

Disease diagnosis and treatment have traditionally been based on efficacy validation models that neatly packaged patient populations into distinct buckets (often focused just on the disease state in question) that rarely allowed for differentiation between the individual constituents. This "one size fits all" approach did not enable true personalisation of patient diagnosis and treatment based on their innate individual characteristics (e.g., genome, epigenome, proteome, microbiome, metabolome, morphology, etc.) and exposome (e.g., lifestyle, environmental exposure, socioeconomic status, etc.).

One main reason why the healthcare industry adhered to the "one size fits all" paradigm for so long was the lack of capable and affordable tools and methodologies that could accurately monitor and determine all aspects of an individual's innate characteristics and then utilise that data to precisely tailor treatments or infer clinical outcomes for an individual. Because of recent digital health advances and availability of large volumes of relevant data, digital health companies now have the technical capability and market expectation to deliver genuinely personalised care at scale. The cost of generating and processing data that is indicative of an individuals' uniqueness (e.g., whole genome sequencing, proteomic analysis, high resolution imaging, etc.) has recently come down to such an extent that it is readily accessible to the masses and recent advances in AI (more specifically ML) techniques have powered the analysis of large and complex datasets generated by these tools to make clinically relevant insights that can help guide the diagnosis and treatment of patients based on their individual uniqueness.

Provider-centric model

Until recently, healthcare services were delivered to patients primarily through a provider-centric model whereby patients seeking medical attention were required to go to a medical practitioner, clinic or hospital to be diagnosed and/or treated for their condition. This approach was largely driven by the healthcare industry's slow adoption of new IT (e.g., Internet of Things (IoT), wireless video communication, text messaging, electronic medical record systems, etc.) and the lack of digital health tools (e.g., wireless diagnostic medical devices, wearables, mobile apps, etc.) that allow for remote patient diagnosis and monitoring.

In the last few years, the healthcare industry's adoption of new IT technologies and other digital health tools has accelerated significantly, ushering in a new patient-centric paradigm (e.g., telemedicine, virtual healthcare, etc.) whereby healthcare services are delivered remotely, almost on-demand, to patients regardless of where they are. When the COVID-19 pandemic took hold of the world, a measure of urgency was also added as the provider-centric approach to healthcare now included a component of danger that patients would be exposed to COVID-19 if they visited their providers in person.

Siloing of health information and data

Data access and analytics are the fuel that drives digital health. Patient health information has traditionally been either stored as physical files at a provider site (e.g., doctor's office, clinic, hospital, etc.) or in electronic health record (EHR) management systems that are incompatible with one another. This resulted in health data being siloed where they were stored, which hindered the seamless communication and sharing of health data. This also prevented the use and aggregation of such data to power analytics tools (many of which are driven by AI/ML) that are used in a variety of different applications, including drug discovery, diagnostics, DTx, pre-surgical planning and clinical decision support.

Fragmentation of constituents

There is substantial fragmentation between the major constituents of the Digital Health Ecosystem, which makes it difficult for them to access, navigate or transact with each other. The inefficiencies caused by this fragmentation add unnecessary cost and delay to the delivery of care to patients. Further, it makes it difficult for patients to access the full range of products and services that are available to treat their health or wellness condition.

New Digital Technologies

A host of different digital technologies are helping to provide the infrastructure and know-how to drive the digital health revolution in healthcare.

Wireless connectivity and Internet of Medical Things (IoMT)

Wireless/mobile devices (e.g., mobile phones, wearables, medical devices, mobile applications, etc.) allow patients to access their healthcare providers and resources from anywhere around the world with wireless or Wi-Fi data connectivity. In turn, this also allows their healthcare providers to monitor their current health status and condition. This amalgamation of devices can all be connected to enterprise healthcare information systems using networking technologies to form an IoMT that allows for uniform transfer of medical data over a secure network.

Big Data analytics/storage

The voluminous quantity of medical data captured and transmitted through an IoMT is then stored and analysed using Big Data storage and analytics systems that manage, curate and process the data to generate predictive insights and/or visualise the data to aid analysts in quickly interpreting the data. A 2017 white paper from Stanford University School of Medicine estimates that 153 exabytes of healthcare data was generated in 2013, and that was projected to grow to 2,314 exabytes by the year 2020.[2] Analytics can be performed on the data using traditional statistical data analysis tools or more advanced AI/ML methodologies.

Enabling New Digital Health Solutions

The adoption of digital technologies in healthcare has given rise to a number of different categories of transformative digital health solutions.

Remote patient monitoring and delivery of care

Perhaps the most visible and impactful of the categories of digital health solutions are telemedicine/telehealth and virtual care. The year 2020 was a banner year for telehealth as the COVID-19 pandemic led to an exponential leap in the number of patient consults using telehealth platforms due to social-distancing measures and to minimise exposure.

A 2020 report by Amwell found that before COVID-19, fewer than 1% of all physician visits in the US were conducted via telehealth; in just over a month after the start of the pandemic, analysis of health claims data found that this number had increased to over 50%. Of those patients who used telehealth platforms, over 90% said that they planned to continue using those platforms post-COVID-19.[3] The digital technologies that enable telehealth are wireless/mobile devices and the applications that run on them. Telehealth has now transitioned from emergency adoption to baseline care infrastructure, with virtual care increasingly embedded into longitudinal care pathways rather than episodic consultations.

Moving beyond virtual doctor's visits through telehealth platforms is the concept of virtual care, whereby healthcare providers remotely deliver the full range of health services to patients by remotely monitoring patient condition and vitals (remote patient monitoring) using IoMT-connected wearables and wireless medical devices; and communicate with patients to provide treatment advice and answer their questions using wireless/mobile devices that enable live and secure video, audio and instant messaging communication. This next step in the evolution of telehealth will truly change the traditional provider-centric model of healthcare delivery to patients to a patient-centric model where the wide range of healthcare services can be delivered virtually on-demand and remotely wherever the patient is located.

Big Data analytics and AI/ML-powered healthcare solutions

- **Personalised/precision medicine**
  Personalised/precision medicine is another digital health solution that has recently gained traction. These are healthcare models that are powered by Big Data analytics and/or AI/ML to ensure that a patient's individual uniqueness (e.g., genome, microbiome, exposome, lifestyle, etc.) factors into prevention and the treatment (e.g., therapeutics, surgical procedures, etc.) of a disease condition that the patient is suffering from. An example of this would be companion diagnostic tests that are used to predict a patient's response to therapeutics based on whether they exhibit one or more biomarkers. Large quantities of patient records, including measured data of one or more patient biomarkers, the therapeutic(s) the patient is taking and the patient's clinical outcome, can be analysed using Big Data statistical software tools to determine the biomarker(s) associated with a particular clinical outcome when the patient is treated with a particular therapeutic; or be used to train AI/ML algorithms that can identify biomarker(s) of relevance and infer patient clinical outcomes when treated with a particular therapeutic.
- **AI/ML-enabled diagnostics**
  The application of advanced AI/ML algorithms and techniques to process healthcare data enables critical clinical insights that link previously unrelated data inputs (e.g., imaging features, genomic/proteomic/metabolomic/microbiome biomarkers, phenotypes, disease states, etc.) to disease conditions and progression. This has resulted in diagnostic tests that have a high degree of predictive accuracy for some previously difficult-to-diagnose health conditions such as dementia, depression, Alzheimer's, and also enabled more non-invasive methods to diagnose and monitor disease conditions (i.e., cancer) that previously required surgical biopsies or other more invasive techniques.
- **Intelligent drug design and discovery**
  The same data that is used to train AI/ML algorithms for personalised/precision medicine purposes can also be re-purposed to train algorithms that can be used for intelligent drug design and clinical cohort selection applications that aid in the discovery and the clinical study of new or novel therapeutics and re-purposing of existing therapeutics.
  For example, an AI/ML algorithm trained to predict biological target response and toxicity can be used to design novel (i.e., non-naturally occurring) chemical structures that have strong binding characteristics to a biological target with correspondingly low chemical and/or systemic toxicity. This ability to design a therapeutic compound "backwards" from looking at desired attributes (e.g., binding strength, toxicity, etc.) and then custom designing a therapeutic compound with those attributes, instead of traditional drug discovery methods that screen millions of compounds for the desired attributes, is potentially game-changing. Not only does it hold the promise to shorten the initial drug target discovery process as it moves away from looking for the proverbial "needle in a haystack" to a "lock and key" approach, but

it will likely lead to drugs that have greater efficacy and fewer side effects for larger groups of patients.

Those novel chemical compounds can then be administered to clinical cohorts selected using AI/ML algorithms trained to choose the most suitable patients to enrol for clinical trials used to study the efficacy and toxicity of the compounds. Currently, it takes an average 10–15 years and US$1.5–2 billion to bring a new drug to market with approximately half of the time and investment consumed during the clinical trial phases of the drug development cycle. One of the main stumbling blocks in the drug development pipeline is the high failure rate of clinical trials. Less than one-third of all Phase II compounds advance to Phase III. More than one-third of all Phase III compounds fail to advance to approval. One of the primary factors causing a clinical trial to fail is clinical cohort selection that fails to enrol the most suitable patients to a clinical trial.[4] Minimising errors in clinical cohort selection can potentially shorten the clinical trial phase and reduce the risk of clinical trial failures that are not attributable to the drug being studied.

Digital hospital

Traditional hospital workflows can be highly inefficient because of disorganisation in patient treatment workflows and difficulties that clinicians have in readily accessing or utilising patient medical information. Through the use of digital medical information management tools, much of this inefficiency can be eliminated by ensuring less workflow downtime and gaps in the way that a patient is diagnosed and treated once he is admitted to a hospital and allowing patient medical information to be accessed anywhere within the hospital through a multitude of different means (e.g., workstation terminals, mobile devices, etc.) and from information stored externally from the hospital.

EHR aggregation platforms

Large volumes of good-quality patient EHR data is the fuel that drives many Digital Health Solutions. The old adage of "garbage in, garbage out" applies particularly well to ML technologies. Flawed or nonsense input data that is fed to even the most sophisticated ML algorithm will invariably produce nonsense outputs or predictions. The integration of cloud-based EHR databases with advanced data extraction tools (e.g., natural language processing, automated annotations, etc.) has enabled companies to aggregate large volumes of good-quality EHR data from fragmented (i.e., unaffiliated) clinical sources (e.g., sole practitioners, clinics, hospitals, etc.) distributed throughout the US and the rest of the world.

Digital Health Legal Issues

There are many important legal issues that apply to digital health. These issues can be broadly divided into two categories: intellectual property rights (IPRs); and regulatory compliance.

IPRs

With respect to IPRs, there are registrable IPRs (e.g., patents, copyrights, etc.) and unregistered IPRs (e.g., data rights, trade secrets, know-how, etc.).

Patents and copyrights

With respect to digital health and patents, the most burning issue is subject-matter patentability (or what qualifies as patentable). A series of US Supreme Court cases in the past 10 years have cast a shadow over the patentability of software (see *Alice Corporation Pty. Ltd. v. CLS Bank International*) and diagnostic methods (see *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*[5] and *Association for Molecular Pathology v. Myriad Genetics, Inc.*).[6] Successfully navigating these patentability hurdles is often a critical part of protecting the substantial investments that companies make in bringing their digital health solutions into the marketplace. Some recent US Supreme Court and Federal Circuit cases have begun to chip away at the patentability hurdles for diagnostics innovation (see *Hikma Pharmaceuticals USA Inc. v. Vanda Pharmaceuticals Inc.*[7] and *CardioNet, LLC v. InfoBionic, Inc.*)[8] and the current expectation is that future cases will continue to swing toward protection of this important area of innovation. In other jurisdictions around the world, computational software-driven innovations face similar hurdles toward patentability.

Copyrights can be used to protect software, including code for learning platforms such as various machine and deep-learning models. Copyrights can also be used to protect databases and some types of data content that which is itself original (e.g., structured compilations of genomic sequencing data, structured compilations of images, audiovisual recordings, detailed diagrams, etc.), but cannot protect factual data (e.g., raw genomic sequencing data, metabolite data, proteomics data, etc.). However, there may be other legal mechanisms that can be used to protect factual data, such as contract law and trade secret protection.

Trade secrets

Because of the current limitations of patent law, trade secret protection plays an outsized role in protecting digital health innovation relative to other industries. However, trade secret law has inherent limitations that make it less protective of innovation than patents. For example, trade secret law does not protect against third parties independently developing identical solutions (i.e., digital health innovations) and it requires that the trade secret owner marks their trade secrets and demonstrates that they are taking active measures to ensure that their trade secrets are not misappropriated.

Data rights

Digital health solutions tend to both generate and utilise large quantities of health data; therefore, data rights are a vital component of digital health IPRs that need to be protected. This is particularly true for digital health solutions that are powered by AI/ML algorithms as the accuracy of their predictions are largely determined by their training using large quantities of quality training data.

As discussed above, raw factual data is generally not protectable under copyright law, so the primary means used to guard data rights is currently with contract and trade secret laws. As the value of health data rights increases, the expectation is that the body of law dealing with data rights protection will also evolve to more adequately safeguard the rights of data owners.

Regulatory Legal Issues

Moving beyond IPRs, compliance with state and federal regulations is also essential for digital health companies seeking to successfully develop, market or implement digital health solutions in the US.

Data privacy

For digital health companies, data privacy compliance is no longer a back-office legal function but a product design constraint that directly impacts architecture, data flows, and commercial partnerships. Continued access to medical data relies on patient trust and the laws and regulations that underpin that trust. As data gathering and access are critical components of most digital health solutions, it is vital that digital health companies adopt data privacy policies and infrastructure that are compliant with the data privacy laws and regulations of the jurisdiction(s) in which they operate.

In the US, the most pertinent data privacy laws are the Health Insurance Portability and Accountability Act (HIPAA), California Genetic Information Privacy Act (GIPA), California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA). The jurisdictional boundaries of the HIPAA, GIPA, CCPA and CDPA are carved out based on both the entity gathering the data (HIPAA-Covered Entities and their Business Associates) and the legal residence of the individual whose data is being gathered. That is, the HIPAA only applies to a statutorily defined group of Covered Entities such as health plans (e.g., health insurance companies, Medicare, Medicaid, etc.), healthcare clearinghouses (e.g., billing service, community health information systems, etc.), and healthcare providers (e.g., physicians, clinics, hospitals, pharmacies, etc.) that are considered traditional healthcare data custodians. Importantly, this leaves a coverage gap for non-traditional healthcare data custodians such as the technology companies (e.g., Amazon, Apple, Facebook, Google, etc.) that have recently entered the healthcare marketplace through their IoT and mobile app product offerings that can diagnose and treat healthcare-related issues. The first state to attempt to fill the HIPAA coverage gap was California when it enacted the CCPA in 2018. The CCPA provides privacy rights and consumer protection for data obtained from residents of California irrespective of the type of business. The California GIPA came into effect in 2022 and it places data collection, use, security and other disclosure requirements on direct-to-consumer genetic testing companies and provides their customers with access and deletion rights. The Virginia CDPA came into effect in 2023 and is the most recent state-level data privacy law to come into effect. It lays out clear regulations for companies that conduct business in Virginia regarding how they can control and process data. It also gives consumers the right to access, delete and correct their data, as well as opt-out of personal data processing for advertising purposes.

Generally, the HIPAA, GIPA, CCPA and CDPA regulate how businesses collect, handle and protect an individual's personal information (PI) to ensure their privacy and give them control over the sharing (informed consent) of their PI with third parties.

US Food and Drug Administration (FDA) regulatory

Another set of regulations that digital health companies need to consider are those that regulate the safety and efficacy of digital health solutions. The Federal Food, Drug and Cosmetic Act (FFDCA) and related laws are federal statutes that regulate food, drugs and medical devices. The FFDCA is enforced by the FDA, which is a federal agency under the US Department of Health and Human Services.

Depending on whether the digital health solution is a device, system or software, the FDA may enforce a number of different regulations and programmes, including: 510(k) certification; Premarket Approval (PMA); SaMD; Digital Health Software Pre-certification Program (Pre-Cert Program); and a Laboratory Developed Test regulated under the Clinical Laboratory Improvement Amendments programme. One technology area of focus for the FDA recently is AI/ML-powered digital health software, which is dynamic by design, requiring companies to design for model change management, version control, and post-deployment monitoring from the outset. The FDA established a Digital Health Center of Excellence in 2020 to further the advancement of digital health solutions and address the unique regulatory issues they pose.[9]

State-specific practice of medicine laws (telehealth and virtual health)

For telehealth and virtual health companies that provide physician consultations across state lines, the Interstate Medical Licensure Compact Commission regulates the licensure of physicians to practise telemedicine in member states.

The Interstate Medical Licensure Compact (IMLC) speeds up the licensure process for physicians practising telemedicine as it eliminates the need for them to individually apply for licences in each state they intend to practise in by allowing them to obtain an IMLC licence that is valid in all states that have joined the compact. The following states have joined the IMLC: Alabama; Arizona; Colorado; Idaho; Illinois; Iowa; Kansas; Maine; Maryland; Michigan; Minnesota; Mississippi; Montana; Nebraska; Nevada; New Hampshire; Pennsylvania; South Dakota; Tennessee; Utah; Vermont; Washington; West Virginia; Wisconsin; and Wyoming; as well as the District of Columbia, and Guam.[10]

The Stark Law and Anti-Kickback Statutes (AKSs)

Telehealth and virtual health providers who enter into business arrangements with third parties that incentivise care coordination and patient engagement are also subject to federal Stark Law and AKSs.

The Stark Law (or physician self-referral law) prohibits referrals by a physician to another provider if the physician or his immediate family has a financial relationship with the provider. The AKSs, meanwhile, bar the exchange of remuneration (monetary or in kind) for referrals that are payable by a federal healthcare programme like Medicare.

These laws provide another necessary consideration for telehealth companies as they can hinder opportunities for large health systems and companies to work together and to help smaller systems and hospitals develop their own platforms or take part in a larger telemedicine network.[11]

State and federal medical reimbursement laws and regulations

The year 2020 has been a banner year for telehealth. Even before the COVID-19 pandemic, the remote care delivery model had been gaining traction among patients, particularly those who have grown up with technology.

Currently, all 50 states and the District of Columbia now provide some level of reimbursement coverage for telehealth services for their Medicaid members. At the federal level, the Mental Health Telemedicine Expansion Act was passed as part of the Omnibus Appropriations and Coronavirus Relief Package and the CONNECT for Health Act of 2019 and has been introduced but not passed.

Conclusions

The digital health sector experienced explosive growth even before the COVID-19 pandemic accelerated its adoption by mainstream payors, providers and patients. With the continued rapid pace of change in digital health, the expectation is that the delivery of healthcare will continue to transform. Within this transformation there will be some common themes.

The ability to gather data, generate clinical insights and transform those insights into actionable clinical solution(s) will form the foundation of value creation within digital health. In this paradigm, data access becomes the new "oil rush" as data will fuel the analytics engines behind many future digital health solutions. As a result, traditional technology players such as Amazon, Apple, Facebook and Google, may create substantial competition for traditional healthcare providers. It remains to be seen whether those advantages will translate to success in the digital health marketplace.

Clinical adoption of digital health solutions will continue to be a challenge as there are significant clinician concerns about how to safely integrate these solutions into their day-to-day practice. Moreover, digital health companies must navigate the myriad of state and federal regulations/laws relating to data privacy, FDA regulatory, practice of medicine, and medical reimbursement in order for their solutions to even be accessible by clinicians in the first place.

Lastly, there are brewing geopolitical factors that may impact how well digital health companies succeed in the marketplace. Regional regulations on health data access and usage (e.g., General Data Protection Regulation, HIPAA, CCPA, etc.), reimbursement and product approval are additional requirements to contend with for companies that are foreign to the jurisdiction. Also, many countries have begun to aggressively invest in the gathering of healthcare data (especially whole genome data) on a national level, which can potentially be leveraged to give domestic companies an edge over foreign ones. Examples of this are the UK Biobank Whole Genome Sequencing Project and Beijing Genome Institute (BGI) Million Chinese Genome Project. It is conceivable (and likely) that the UK and China will implement data-access policies that specifically benefit domestic digital health companies to give them a home-grown advantage.

Endnotes

1 https://www.globenewswire.com/news-release/2020/11/17/2128470/0/en/Digital-Health-Market-Size-to-Hit-Around-US-833-44-bn-by-2027.html#:~:text=The%20global%20digital%20health%20market,27.9%25%20from%202020%20to%202027

2 Stanford University School of Medicine (2017). "Harnessing the Power of Data in Health, Stanford Medicine 2017 Health Trends Report". Retrieved from: https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf

3 Amwell (2020). "From Virtual Care to Hybrid Care: COVID-19 and the Future of Telehealth". Retrieved from: https://static.americanwell.com/app/uploads/2020/09/Amwell-2020-Physician-and-Consumer-Survey.pdf

4 Harrer, *et al.* "Artificial Intelligence for Clinical Trial Design". *Trends in Pharmaceutical Sciences* 40.8 (2019): 577–591.

5 https://supreme.justia.com/cases/federal/us/566/66

6 https://supreme.justia.com/cases/federal/us/569/576/#:~:text=Assoc.,Justia%20US%20Supreme%20Court%20Center

7 https://www.scotusblog.com/case-files/cases/hikma-pharmaceuticals-usa-inc-v-vanda-pharmaceuticals-inc

8 https://law.justia.com/cases/federal/appellate-courts/cafc/19-1149/19-1149-2020-04-17.html

9 https://www.fda.gov/news-events/press-announcements/fda-launches-digital-health-center-excellence

10 https://intouchhealth.com/half-of-the-country-has-joined-the-telemedicine-licensure-compact

11 mHealth Intelligence (2020). "Stark Law Changes Should Benefit Telehealth, Remote Patient Monitoring". Retrieved from: https://mhealthintelligence.com/news/stark-law-changes-should-benefit-telehealth-remote-patient-monitoring



Roger Kuan is a Partner at Norton Rose Fulbright LLP and US head of the Precision Medicine and Digital Health Practice Group, where he counsels companies that are uniquely positioned in the convergence of the life/medical sciences and technology industries on how to successfully navigate the complexities of the intellectual property (IP), data rights and regulatory challenges they encounter.

Roger has extensive experience in IP strategy and portfolio management (utility/design patents, trademarks, copyrights, and trade dress), data rights strategy, licensing and technology transactions, freedom-to-operate clearances, enforcement, monetisation, IP due diligence, and dispute resolution. His practice is focused in the life sciences sector (e.g., research tools, analytical instrumentation/software, digital therapeutics, medical devices, diagnostics, biomanufacturing equipment, etc.) with an emphasis in emerging technologies such as precision medicine (e.g., genomic sequencing platforms, AI/ML, computational genomics/bioinformatics, molecular diagnostics, companion diagnostics, etc.), digital health (e.g., mobile apps, clinical decision support, software, AI/ML imaging diagnostics, wearables, etc.) and 3D printing/bioprinting.

Norton Rose Fulbright
555 California Street
Suite 3300
San Francisco, 94104
California
USA

Tel: +1 628 231 6800
Email: roger.kuan@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/roger-kuan-1b5b824



David Wallace is a member of the Johnson & Johnson Law Department and is the Assistant General Counsel (AGC) of Patents for the Health Technology Team. In his role as AGC, David is primarily responsible for day-to-day activities regarding the patent aspects of the health technology initiatives across the Johnson & Johnson Family of Companies.

Johnson & Johnson
510 Cottonwood Drive
Milpitas, California 95035
USA

Tel: +1 408 273 5101
Email: dwalla34@its.jnj.com
LinkedIn: www.linkedin.com/in/david-wallace-957b24

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full-business law service. We have more than 3,500 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

Recognised for our industry focus, we are strong across all the key industry sectors: financial institutions; energy, infrastructure and resources; transport; technology; life sciences and healthcare; and consumer markets. Through our global risk-advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

At Johnson & Johnson, we believe good health is the foundation of vibrant lives, thriving communities and forward progress. That is why for more than 130 years, we have aimed to keep people well at every age and every stage of life. Today, as the world's largest and most broadly-based healthcare company, we are committed to using our reach and size for good. We strive to improve access and affordability, create healthier communities, and put a healthy mind, body and environment within reach of everyone, everywhere. We are blending our heart, science and ingenuity to profoundly change the trajectory of health for humanity.

www.jnj.com

Johnson & Johnson

The Bio-Industrial Technology Stack: A New Framework for National Sovereignty in the Century of Biology


Dr. Milad Alucozai


Jason Novak


Dr. Nathanael Green


Sophia Poirier

Norton Rose Fulbright

Introduction: The Industrialisation of Biology

We are standing at the edge of a new industrial era. If the last century was defined by the physics of the atom and the logic of the digital bit, this one will be defined by the engineering of the cell. Biotechnology is moving past its history as a field of artisanal discovery that relied on luck and manual labour. It is maturing into a predictable and scalable industrial force. We have arrived here because of a convergence that makes this moment distinct from the biotech sector of the last 25 years: the collision of massive computing power, generative AI, and high-throughput automation is finally allowing us to treat biology as a rigorous engineering discipline rather than an observational science.

This is no longer just about medicine or science; it is about a new fundamental economic architecture and the ability to define, scale, and secure the products of the future across various industries. From the food we grow to the essential medicines we stockpile, the ability to engineer and scale biology is becoming the central axis of global economic security.

This transition from science project to strategic infrastructure development fundamentally alters the geopolitical map. For decades, the United States (US) held a monopoly on biotechnology as a whole and effectively wrote the operating manual for modern life sciences. But as biotechnology development has evolved from pure research to complex engineering, that monopoly has fractured. We are now navigating a multipolar world where leadership is determined not just by who can discover a molecule, but by who can build it, scale it, and secure it, *i.e.* who can lead each layer of the 'Bio-Industrial Technology Stack' (BITS) explored in this chapter.

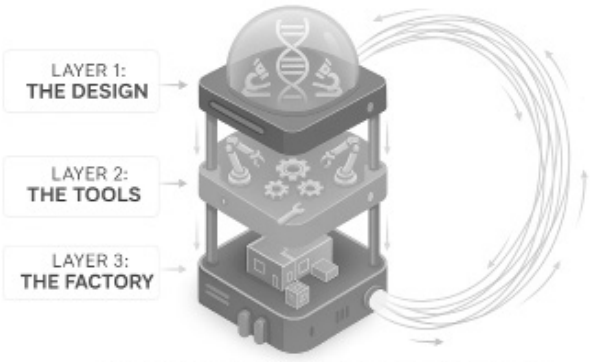
The Strategic Stakes

This shift matters because the logic of globalisation is being rewritten. For the past generation, the West optimised its bioeconomy for cost and efficiency, often outsourcing critical layers of production to the lowest bidder. But in a world of rising geopolitical friction, efficiency without resilience is a liability. Control over the BITS could become a prerequisite for national autonomy. It determines whether a nation can guarantee the supply of essential anti-infectives during a pandemic, secure novel compositions to combat chronic illness, and capture the value of a market projected to exceed $30 trillion by 2050.[1] The stakes are simple: whoever governs this infrastructure will determine who has access to the cures and materials of the future, and who remains dependent on the benevolence of others. This independence is increasingly tied to a fundamental transition to the era of human data. By moving away from legacy animal proxies and towards functional human systems and multimodal datasets, nations can build a sovereign 'Validation Engine'. This evolution allows for the generation of trial-quality insights before a drug ever enters a clinical setting, ensuring that the 'Code' layer of the stack is grounded in human-relevant truth rather than biological approximations. The stakes are even more important if one considers the implications of governing just one layer of that BITS – if one layer were essentially governed by a single nation or territory, that nation or territory can become the world's gate to full drug development.

Defining the Architecture: The BITS

To understand the mechanics of this competition, we must look beyond the abstract concept of 'biotech' and analyse the industrial machinery that powers it. We call this the **BITS (The Bio-Industrial Technology Stack)**. It is the integrated architecture required to translate biological data into physical reality at a massive scale.

The BITS framework reveals that national competitiveness is not a single metric, but rather a performance across three interconnected engines that define the functional boundaries of the bio-industrial stack:



BITS: BIO-INDUSTRIAL TECHNOLOGY STACK

- Layer 1: The Design Engine (The Code). This represents the upstream architecture where biology is transformed into a more rigorous engineering discipline. This is the 'programming' layer of the stack, where AI is leveraged to model targets and simulate biological systems with precision before they ever reach a laboratory setting. It serves as the fundamental source code of the bioeconomy.
- Layer 2: The Validation Engine (The Tools). This engine serves as the high-fidelity filter of the stack, bridging the

gap between digital design and physical truth through various tools, including analytical software and instrumentation. It explicitly incorporates digital infrastructure, specifically GPU fabrics and data commons, which should be viewed not as passive background assets but as active tools of clinical certainty. By utilising digital twins and mechanistic modelling, this layer provides the essential proof that the Design Engine's code remains valid in human systems before capital is committed to large-scale production in the factory. Crucially, the Validation Engine is the bridge that resolves the 'digital-only' leadership paradox. By establishing a sovereign truth layer, we ensure that the ingenious designs of the Code layer are not merely theoretical 'hallucinations' but are anchored in human-relevant data before a single dollar is committed to physical scale.

- Layer 3: The Execution Engine (The Factory). This constitutes the hard infrastructure of mass production and sovereign supply chains. While the Validation Engine focuses on proving efficacy, the Execution Engine is defined by the physical ability to manufacture and distribute millions of doses through bioreactors, active pharmaceutical ingredients (APIs), and specialised Contract Development and Manufacturing Organisation (CDMO) networks.

The true power of the BITS framework lies in its recursive nature. We must move beyond viewing these layers as a linear pipeline and instead treat them as the 'Sovereign Flywheel' illustrated above. In this model, performance data from the Execution Engine (Layer 3) flows back into the Design Engine (Layer 1), creating a closed-loop system where manufacturing yields refine our AI models. By treating every bioreactor as a data-collection node, we transform the Execution Engine from a cost centre into a strategic intelligence asset. This transforms biology from a series of disparate scientific milestones into a unified, self-improving industrial system.

The New Global Map

The distribution of power across this stack is uneven and shifting. This chapter provides an audit of the four primary powers shaping the BITS today. We examine: the US, the historical digital architect now fighting to maintain its top-layer dominance; Europe, a titan of research navigating a complex investment landscape; China, which has strategically pivoted to capture the downstream Factory layer while simultaneously signalling a paradigm shift to challenge the West's pre-eminence in upstream discovery; and India, which is rapidly evolving from a generic powerhouse into a hub of novel discovery. By comparing where these regions stood 25 years ago against their capabilities today, we can see the new fault lines of the global bioeconomy.

The BITS in 2000

Layer 1: The Design Engine (The Code)

In 2000, the US was the global leader in top-layer research and development (R&D), marked by a developing biotech ecosystem of universities, start-ups, larger biopharmaceutical companies, and government investment. The Human Genome Project, largely funded by the US National Institutes of Health (NIH), with its first draft announced in 2000, helped jump-start the ecosystem towards accelerating target identification, gene mapping, and upstream discovery tools.[2]

US investment in biomedical research was clear: between 1998 and 2003, the NIH's annual budget doubled, rising from $13.7 billion to $26.9 billion per year.[3] Also contributing to the US's dominance at the turn of the century was various policies and a robust regulatory framework that provided competitive advantages to US firms.[4] For example, the Bayh-Dole Act of 1980 and the 1986 amendment encouraged universities and businesses operating under federal research contracts to collaborate on development and commercialisation and the Drug Price Competition and Patent Term Restoration Act of 1984, also known as the Hatch-Waxman Act, restored patent term lost during the long FDA-approval process, eliminating some of the financial risk of R&D.[5] The FDA Modernization Act of 1997 reauthorised collection of user fees, shortened review times, and created a fast-track approval process for certain drugs, all of which encouraged investment in novel modalities.[6] Many of these policies spurred non-US firms to enter the US market along with an increased movement of biomedical scientists to the US.[7]

Together, these scientific breakthroughs, substantial federal investment, supportive legislative policies, and comprehensive talent pool cemented the US's position as the global leader in top-layer innovation at the start of the 21st century. The US had the greatest representation of drug patent inventors in the early 2000s when comparing the top 10 countries with the greatest inventor presence.[8] Additionally, the US far surpassed any other country in receiving biotechnology patents granted by the US Patent and Trademark Office and the European Patent Office.[9] The National Center for Science and Engineering Statistics found that in 2000, the US was second only to Europe, and well ahead of every other country, in the number of articles in biological and biomedical disciplines.[10] Between 2001 and 2010, US-headquartered companies accounted for 57% of the New Chemical Entities (NCEs), which alone exceeded the combined share of France, Germany, Japan, Switzerland, and the United Kingdom (UK).[11]

Europe entered the 2000s with a strong foundation in upstream drug development. The inception of a central regulatory pathway, the European Medicines Agency (EMA) in 1995, and a specific focus on biotechnology programmes, like the Biomolecular Engineering Programme, Biotechnology Action Programme, and BRIDGE, paved the way for European innovation in the pharmaceutical space.[12] Europe positioned itself as a strong leader in drug discovery through the second half of the 1900s. Looking at EU firms' contributions to NCEs in the 1970s, the four largest European countries were responsible for 55% of NCEs produced by major nations, outpacing the US by 24%.[13] Between 1993–2003, an analysis of global drug discovery found that Europe was responsible for 43.3% of all NCEs discovered in the US, Europe and Japan, demonstrating its high level of productivity in target and compound identification.[14] Pharmaceutical R&D expenditure in Europe was only slightly behind that of the US.[15] Further, Europe was the leader in biological and biomedical science articles published in 2000 and only second to the US in patenting activity in the pharmaceutical industry.[16] These initiatives and investments ensured that Europe maintained a prominent global role in the Design Architecture of BITS.

By 2000, China's contributions to the pharmaceutical industry were relatively small. In 1995, China's share of the pharmaceutical industry output was 2.5%.[17] At this point, China's pharmaceutical sector was largely generics-oriented, relying on a fast-follower and incremental improvement model rather than investing in first-in-class target and compound identification like the US and Europe.[18] Domestic

pipelines emphasised replication and me-too/me-better products, while novel molecular design and translational research capabilities were still nascent.[19] This limited upstream focus reflected the financial and technical constraints combined with a policy and IP environment that lacked any incentive for innovation.[20] A skills gap existed in China in part due to an influx of Chinese students pursing graduate education in the US and remaining there to build careers in academia and industry.[21] Also, Chinese patent law virtually excluded pharmaceuticals until the 1990s.[22] Strategic scientific moves like establishing the Chinese National Human Genome Center and the Beijing Institute of Genomics enabled China to join the International Human Genome Sequencing Consortium in 1999 and helped lay the groundwork for a domestic innovative ecosystem; however, these efforts did not immediately translate into an industry of robust proprietary discovery.[23] The broader regulatory framework was still maturing and clinical practice guidelines were not settled yet.[24] Thus, China did not yet have the robust infrastructure to have the same foothold on top-layer drug discovery as the US and Europe did at this point. Together, these factors meant that in 2000 China was primarily a participant in generics and an early chemistry outsourcing hub, rather than a leader in upstream target and compound identification.

Likewise, in 2000, India's productivity in the upstream drug discovery space lagged behind the US and Europe. The Indian Patent Act of 1970 largely shaped the trajectory of India's pharmaceutical innovation as product patents for pharmaceutical ingredients were abolished.[25] This created a process-patent regime that enabled reverse engineering of foreign patented drugs, a far less demanding endeavour than discovering targets and compounds.[26] This resulted in decades-long disincentive for innovative R&D. Coupled with the rise of domestic competitors and the imposition of drug price controls, this environment led many multinational companies to exit India, taking their investments and expertise with them.[27] Although major Indian firms did initiate proprietary discovery programmes in the 1990s, these pipelines were heavily reliant on out-licensing their compounds to global pharmaceutical companies for further development, validation, and capital.[28] Many of these ventures failed during the pre-clinical and clinical stages.[29] Thus, despite these efforts to engage in innovative research, aggregate productivity remained extremely low. For example, in 2000, fewer than 20 compounds reached the preclinical phase; of those, even fewer advanced through the three clinical phases, and none ultimately launched.[30] Success rates for Phase 2 trials were 17.4%, far below global averages (29–34%), possibly reflecting weak candidate selection and translational inefficiencies.[31] In short, India's upstream drug-discovery productivity was negligible on the global scale; policy-driven disincentives, chronic underinvestment, and structural skill gaps left the country far from any later ambitions to become a global innovation hub.

Layer 2: The Validation Engine (The Tools)

In the early 2000s, the Validation Engine of the BITS was characterised by production-scale DNA sequencing equipment, mature high-throughput screening (HTS) automation, strong structural biology access (X-ray crystallography and nuclear magnetic resonance), bioreactors, and broadly deployed analytical and cell-analysis platforms such as mass spectrometry, surface plasmon resonance (SPR), flow cytometry, and multimode microplate readers, protein and cell technology, kits and reagents, as well as a rising popularity in outsourcing preclinical research, validation, and clinical trial management to Contract Research Organizations (CROs).

The US had established a robust foundation of the Validation Engine through a combination of domestic manufacturing, strategic imports, and well-funded university programmes, enabling widespread access to cutting-edge instrumentation. US-based companies were at the forefront of producing essential discovery tools.[32] Applied Biosystems, now under Thermo Fisher Scientific, manufactured the main DNA sequencing machines used in the Human Genome Project.[33] The advent of next-generation sequencing (NGS) transformed DNA sequencing by enabling rapid, low-cost analysis.[34] Illumina, founded in 1998, accelerated this shift with its sequencing-by-synthesis technology, which became the foundational method underlying modern NGS.[35] Other US-based firms advanced laboratory instrumentation, delivering high-precision life sciences and analytical tools for genomics and molecular biology research. Agilent Technologies, spinning off from Hewlett-Packard (HP) in 1999 with the largest initial public offering in Silicon Valley history, expanded its life sciences portfolio, focusing on analytical instrumentation and mass spectrometry.[36] Bio-Rad Laboratories, with an established reputation for reliable and high-quality research equipment and diagnostics, entered the polymerase chain reaction (PCR) market with its thermal cycler in 1999, providing the industry a new tool for DNA amplification.[37] Beckman Coulter was a primary supplier of broadly used laboratory instruments, including flow cytometers, centrifuges and biochemical analysers.[38] Beckman Coulter was later acquired by Danaher, as a continued effort by Danaher to strengthen its leadership in the life sciences instrument market.[39] PerkinElmer regained its footing by integrating its life science and analytical instruments businesses and provided researchers spectroscopy, detection systems, and lab automation.[40] From a public investment standpoint, the NIH established the S10 program in the 1980s with the purpose of helping universities and research institutes acquire expensive, shared-use instruments.[41] These grants, aimed at supporting NIH-funded investigators, eliminated the need for matching funds and enabled universities to build centralised core facilities that served multiple departments. In summary, by 2000 the US supported a vibrant ecosystem of domestic instrument manufacturers, international OEM partnerships, and federally funded equipment grants to universities, enabling widespread access to the tools required for cutting-edge drug discovery. Expansion of biological findings in Layer 1 was largely driven by large pharmaceutical companies acquiring key findings and using in-house hardware platforms to streamline preclinical validation and regulatory-required testing. However, US CROs did present a strong opportunity for large companies to outsource their preclinical testing, clinical trials, logistics, data management, and other functions.[42] The US maintained its strong position as a biotech leader not only from the innovative research and discovery in Layer 1 but also from the domestic engineering of equipment and instrumentation that enabled the discovery, fostering a self-sufficient biotech ecosystem.

Europe primarily relied on domestic manufacturing for its instrumentation and automation equipment to enable Design Engine (Layer 1) discovery at European firms, drawing on its strength in engineering and the production of high-precision, high-quality tools.[43] Germany, Switzerland, the Netherlands and the UK had the most developed equipment and supplies industries in Europe, and major European manufacturers like Roche, QIAGEN, Analytik Jena, bioMérieux, and

Siemens Healthineers served both domestic and international demand, Europe and the US as key markets.[44] Roche, one of the first companies specifically set up to manufacture scientifically researched pharmaceuticals, made strategic decisions to further develop and focus on pharmaceuticals and diagnostics in the 1990s and launched the world's first automated laboratory diagnostics device.[45] QIAGEN was a leading supplier of DNA purification systems and molecular sample-preparation instrumentation and focused on developing advanced automated platforms for genomic analysis and sequencing workflows.[46] The German company Analytik Jena launched the first simultaneous TOC/TN analyser worldwide in 1991 and continued to provide a wide range of innovative analytical instruments through the 2000s.[47] bioMérieux, a French-based company, supplied *in vitro* diagnostics instruments and assays that served molecular diagnostics applications.[48] Other groundbreaking instrumentation platforms like SPR systems, fully engineered in Sweden, were exported across Europe and the world, making a global impact in biopharmaceutical R&D.[49] Like in the US, European universities and research institutions relied on government funding to acquire the necessary equipment to enable robust Design Engine (Layer 1) discovery.[50] European national governments and research councils coordinated to make state-of-the-art infrastructure and equipment available to researchers.[51] Like in the US, large pharmaceutical companies still ran substantial in-house validation while selectively outsourcing various functions to CROs for cost-savings and efficiency. Leveraging its engineering strength and strong scientific base, Europe built a competitive environment for producing high-quality instrumentation that enabled both domestic and international participation in upstream drug discovery.

In the late 1990s and early 2000s, China's scientific instrument industry was still nascent and remained largely uncompetitive relative to dominant US and European players. Foreign technology acquisition has been a central element of China's industrial strategy over the past two decades.[52] Firms that did innovate saw very little competitive impact in their respective sectors. For example, Bioer Technology launched the first Chinese-developed peltier-based thermal cycler in 1998, but China's pharmaceutical sector was focused on generics, not molecular biology R&D and upstream drug discovery, suggesting low institutional demand for PCR instruments and other high-end, advanced research technologies.[53] Those that did engage in upstream drug discovery relied on imported technology.[54] Thus, the primary instrumentation industry yielded low-value-added products and basic lab instruments.[55] China's entry into the World Trade Organization in late 2001 was a step towards establishing an innovative biotechnology sector; agreeing to implement better IP protections signalled a strategy shift from copying products to genuine engineering.[56] As China's manufacturing ecosystem developed, joint ventures between foreign and Chinese firms became more common, highlighting domestic capabilities in producing instruments and other products used in pharmaceutical research.[57] China's R&D services sector was also taking shape during this period. Foreign CROs, including Quintiles and MDS Pharma Services, established operations in 1996.[58] WuXi PharmaTech, founded in 2000, began with synthetic chemistry services and rapidly expanded across biopharmaceutical R&D; additional China-based CROs soon entered the clinical trial arena.[59] Taken as a whole, China had little influence on the global Validation Engine (Layer 2) market, but policy and investment began laying the structural foundation for technological and institutional expansion.

India's minimal contribution to upstream pharmaceutical research in the early 2000s resulted in a limited domestic market for biotech hardware and instrumentation. As a result, the country depended on imported high-end equipment and government-led coordination to access essential infrastructure.[60] India's strength in this layer was being a contract research hub.[61] As the demand grew, India's market of both small and larger CROs expanded.[62] Having strong expertise already in synthetic chemistry expertise and existing knowledge from generics development and manufacturing, the service offerings ranged from chemistry, biology and pharmacology.[63]

Layer 3: The Execution Engine (The Factory)

By 2000, the pharmaceutical manufacturing landscape was already at a global scale. The CDMO industry had already taken off, with global pharmaceutical manufacturers, fine chemical firms, and specialised service providers all playing different, but important roles in making drugs.[64] The major US and European biotech companies had established manufacturing infrastructure locally to support production and commercialisation.[65] These domestic manufacturing facilities supported both API and finished-dosage-form (FDF) manufacturing.[66] In 2000, the US and Europe were leaders in API production, topping the leaderboard for new applications of Certificates of Suitability by the European Directorate submitted by country.[67] At the same time, there was a growing trend by Western pharmaceutical companies to outsource APIs due to cost savings.[68] One report estimated that by 1997, the US shifted from a net exporter to importer of pharmaceuticals.[69] API Drug Master Files (DMFs) submitted to the FDA in 2000 indicated that the US was only responsible for 18% of the submissions, while Europe and India held 42% and 19% of active API DMFs, respectively.[70] At that time, China's share of API production was relatively small compared to the US and Europe, but as foreign companies increased outsourcing, China's role in API and intermediate manufacturing expanded rapidly.[71] India maintained the third-largest API manufacturing industry in the world at this point, second to only Europe and the US, supplying both domestic and global markets.[72] India also grew its position in the FDF manufacturing sector, largely driven by the outlawing of reverse-engineering foreign patented drugs that led to a shift to generics manufacturing.[73] China, still gaining traction with API production, had yet to meet the international production standards to be a competitive FDF manufacturing region.[74] By 2000, global pharmaceutical manufacturing had evolved into a highly interconnected ecosystem, with the US, Europe, India, and China each playing distinct roles in the biomanufacturing ecosystem.

The BITS Today

Layer 1: The Design Engine (The Code)

The US still leads the world in upstream biotech innovation, driving discovery through AI-powered initiatives, public–private research collaborations, and robust funding. Over the past 20 years, the US has been the leader in pharmaceutical R&D expenditure and during this time period, there has been a steady increase in spending in the US, outpacing both Europe and China heading into 2010 through 2020.[75] The US is home to half of the world's top 25 biotech companies by market capitalisation.[76] Also noteworthy is the US's consistent

position as a top producer of NCEs and new biological entities, alongside Europe; although between 2014 and 2018, US enterprises produced almost twice as many NCE or new biological entities as European enterprises.[77] Commitment to government-backed initiatives has remained, though the dramatic rise in NIH funding seen at the turn of the century has begun to stagnate.[78] The progress of AI models and deep learning has spurred the biomedical sector to adopt these platforms for accelerated and complex research. The first AI-discovered drug, rentosertib, was developed by Insilico Medicine, a Boston-based biotech company.[79] Pharmaceutical companies are partnering with Big Tech to accelerate a new era of AI-driven drug discovery; for example, Eli Lilly and Novartis are collaborating with Alphabet's Isomorphic Labs, which builds on DeepMind's AlphaFold breakthroughs, while EvolutionaryScale has teamed with Amazon Web Services and NVIDIA to power AI-native drug discovery research.[80] Commitment to advancing AI in the biomedical space is also a public priority. For example, the Advanced Research Projects Agency for Health, an agency within the Department of Health and Human Services, announced the TARGET programme in 2024, which will use generative AI to accelerate first-in-class antibiotic discovery.[81] Bridge2AI, funded by the NIH common fund, and the National Science Foundation's Directorate for Technology, Innovation, and Partnerships reflect the national-scale priority of combining biology and AI, strengthening model-informed drug discovery across universities and companies.[82] The US also retains a commanding share of global NCE R&D, with leading biotech hubs nested in academic ecosystems, and consistent venture investment into digital-biology startups. However, a notable gap that exists in the US is the lack of public 'biotech libraries' and national policy to facilitate these libraries.[83] Essential databases consisting of compiled genome and health records, research findings on candidate therapeutics, and metrics about cell functionality are not complete and difficult to access and use.[84] The private sector sees the value in these databases to scale AI for drug discovery: Illumina recently introduced Billion Cell Atlas, the world's largest genome-wide genetic perturbation dataset with AstraZeneca, Merck, and Eli Lilly and Company as founding participants and 10X Genomics, with the Arc Institute and Ultima Genomics, created the Virtual Cell Atlas, a large-scale CRISPR perturbational dataset.[85] However, the absence of comprehensive national life-science repositories and databases risks slowing innovation, duplicating efforts, and constraining reproducibility across the industry.

Europe has continued to have a strong position in foundational science, regulatory regimes, and enabling technologies, but its relative position at this Code layer (Layer 1) has slipped behind the US and like the US, is increasingly challenged by China's rising innovation output. Europe was only home to five of the world's top 25 biotech companies in market capitalisation in 2022.[86] A report put out by the European Federation of Pharmaceutical Industries and Associates acknowledges that the US consistently outpaces R&D spending and is increasingly competing with China.[87] For example, Europe now trails the US by over 26% in share of global biopharma R&D.[88] Although Europe leads ahead of the US and China in the volume of scientific publications across the biological, biomedical, and biotechnology fields, it trails on other innovation, production, and adoption metrics.[89] In 2023, China beat Europe for launching new active substances, now falling to third place in newly discovered medicines.[90] Europe's clinical-trial infrastructure is also eroding: Europe's share of global clinical trials has slowly declined and clinical-trial activity on advanced therapies is twice as high in the US and almost three times as high in China.[91] Europe's lag on AI investment is stark: the US invested six times as much as Europe in AI private companies and will have an impact on the implementation and adoption of AI in biotech.[92] While private companies are implementing AI in their processes, like AstraZeneca utilising BenevolentAI and Roche applying organoid-on-chip for understanding drug toxicity, AI is underutilised and underinvested.[93] There have been calls on EU policymakers to adopt new approaches to the biotech ecosystem to maintain its competitiveness on the global stage.[94]

China's desire to become a leader in pharmaceutical innovation has been reflected in the policy reform and increased spending.[95] Aligning their regulatory framework with global standards has aided the much-needed shift for China to go from the generic manufacturer to the global innovator.[96] The establishment of the New Drug Creation and Development programme in 2008 plus other coordinated government efforts over the past two decades, like China's 13th Five-Year Plan (2016–2020) and 14th Five-Year Plan (2021–2025), have aimed to develop biotechnology companies capable of competing at the global level and increase biotech-related R&D investments by over 10% annually.[97] The push to become a major player is evident: biotechnology patents granted in China surpassed the US in 2012 and has continued to trend upward. Recently, 2024 saw a record-high number of drugs approved by China's National Medicinal Products Administration; the majority of the drugs approved were domestically developed.[98] First-in-class drugs developed in China by Chinese firms include: BeBetter Med's ifupinostat, the first HDAC/PI3K dual-targeted inhibitor; and Akeso's ivonesimab, the first approved PD-1xVEGF bispecific antibody.[99] China also overtook the US and the EU as the leader of impactful publications in biotech in 2016 and continues to be a top country for the most-cited papers in this space.[100] China's involvement in global dealmaking has also surged, driven by a wave of licensing transactions for innovating assets emerging from China's booming biotech sector.[101] A reversal in China producing more PhDs than the US has also contributed to China's rise to dominance.[102] According to the US–China Economic and Security Review Commission's 'Made in China 2025' report, China has exceeded goals for domestic and overseas drug approvals.[103] Investment bank Stifel projected that China will be responsible for 37% of molecules licensed by large pharmaceutical companies in 2025, reflecting the innovation output of China.[104] Implementation of AI in drug discovery has been rapid; China is now the front-runner in AI-driven drug discovery patents and global pharmaceuticals are racing to strike deals with Chinese AI biotech firms.[105] Viewed holistically, regulatory reform, sustained public investment, deepening scientific talent, and the rapid integration of AI have transformed China into a central engine of global pharmaceutical innovation, with growing influence over the world's drug-discovery pipelines and overall biotech ecosystem.

India, like China, began the 21st century with a largely nascent drug-discovery base. Over the past 25 years, it has focused on policy reforms, infrastructure build-out, and a shift beyond generics towards new drug R&D to lay the groundwork to advance its bid to become an innovation hub. The government launched the Promotion of Research and Innovation in Pharma MedTech (PRIP) to roll out a suite of programmes aimed at boosting biotech competitiveness and ensuring long-term sustainability.[106] Priority areas span NCEs, new biological entities, phyto-pharmaceuticals, complex generics and biosimilars, precision medicine, medical devices, orphan

drugs, and antimicrobial resistance drug development.[107] PRIP's purpose is to focus on enhancing research infrastructure and supporting private sector entities and academic institutes, encouraging joint ventures between companies and institutes.[108] India also seeks to embrace AI in the life sciences and sees value in generative AI enhancing clinical-trial protocol development and execution, quality assurance, and regulatory submissions as well.[109] In line with India's initiative 'Make AI in India and Make AI Work for India', a Centre of Excellence for AI in Healthcare has been established to deliver scalable AI in the life sciences.[110] Private companies are also innovating; India-based Aurigene Pharmaceutical Services introduced an AI/machine learning (ML)-enabled drug-discovery platform which accelerates the drug-discovery timeline by 30%.[111] Despite these advances and a $300 billion bioeconomy goal by 2030, India is still far behind its counterparts. Regulatory policy reforms remain critical for sustaining pharma R&D growth, particularly in clinical-trial governance, IP protection, and pricing frameworks.[112] There is also a talent pipeline disparity that impacts knowledge creation and technology development.[113] India produces roughly one-quarter as many science PhDs as the US despite the US's population being roughly one-fourth of India's.[114] Further, India's education-to-employment model, which is narrowly focused on engineering and entrepreneurship, no longer aligns with the education needed to develop and sustain a highly technical biotech ecosystem.[115] India will continue to face challenges in funding scarcity to scale start-ups, infrastructure gaps that impede product development and testing, persistent talent shortages and limited global market access due to regulatory misalignment with the US FDA and EU EMA.[116]

Layer 2: The Validation Engine (The Tools)

In 2025, the Validation Engine layer's centre of gravity is shaped by access to AI-ready computer and data centres, advanced research instrumentation, and CRO-led validation to support increasingly advanced and expensive drug-discovery activities. The result is a re-ordering of competitive advantage: nations that can pair high-throughput instruments with scalable GPU fabrics and data commons, and then validate rapidly through CROs and adaptive trials, move targets from *in silico* to preclinical and clinical signal at unmatched speed.

The US has historically been well positioned in this space; US companies sustain innovation in instrumentation and hardware while concurrently relocating manufacturing offshore to achieve cost efficiencies.[117] Prioritising upstream drug discovery in the US continues to drive institutional demand for state-of-the-art DNA sequencing, HTS automation, bioreactors, and advanced analytical platforms. Illumina continues to be a market leader in instrumentation, with novel NGS platforms, *in vitro* diagnostic instruments, and microarray scanners and is now targeting the precision health ecosystem enabled by advancements in genomics, multiomics, data and AI.[118] As the field shifts towards a digital paradigm and increased reliance on AI- and ML-driven drug-discovery models, the US, both private and public entities, are investing in data infrastructure to support the biotech AI compute demand.[119] In the wake of the digital era, US firms have not lost sight of the continued need for innovative, precise, and efficient biotech instrumentation.[120] For instance, Thermo Fisher launched new platforms capable of deeper quantitation and biomarker discovery and improving the characterisation of complex biomolecules, and other leaders highlighted advances in mass spectrometers and small-footprint instruments designed for high-sensitivity analysis.[121] At the start of 2026, Illumina announced its Illumina Connected Multiomics, a cloud-based platform to analyse and visualise multiomic and multimodal biological data at scale.[122] 10x Genomics, founded in the early 2010s, made a name for itself in single-cell RNA sequencing technology and also develops spatial imaging platforms to map RNA molecules and spatial discovery platforms that enable whole transcriptome analysis.[123] Agilent has maintained a strong position for drug research instrumentation, with advanced multi-samplers and mass spectrometers that deliver enhanced sensitivity and analytical performance.[124] At the federal level, the US government is acutely aware of China's growing dominance in biotechnology, as well as the national security implications of AI and data science, prompting export controls on high-parameter flow cytometers and mass spectrometry equipment.[125] The recently passed BIOSECURE Act restricts federal agencies from procuring biotech equipment from 'biotechnology companies of concern' (BCC) and entering into, extending, or renewing a contract with any entity that uses biotech equipment or services from a BCC in performance of such federal contract.[126]

Europe continues to be a leader in producing advanced instrumentation to enable robust upstream drug discovery.[127] For instance, German company QIAGEN announced an upcoming launch of automated sample preparation instruments to increase laboratory throughput and automation for molecular diagnostics and genomics analysis.[128] Roche recently received a CE Mark for its automated mass spectrometry platform that offers the broadest *in vitro* diagnostic menu and is providing labs with advanced platforms (*e.g.*, cobas® modular analyser systems) that enhance throughput, run flexibility, and enable sample prioritisation.[129] However, the rise in competitors like China and India providing a more affordable manufacturing ecosystem has forced Europe to look at their investment strategy in order to remain a critical player in the biotech stack. Further, Europe's lag in adopting AI will likely affect the ability to scale up the necessary infrastructure needed to implement AI in drug discovery and remain competitive with China and the US.

Just as China has emerged as a top competitor in upstream drug discovery, it has steadily moved up the biotech toolchain.[130] Governments, both local and national, have been quick to adopt AI in physical lab infrastructure.[131] Funding initiatives have enabled firms and institutions to build out biofoundries, automated wet labs and industrial-scale screening facilities to advance research in the lab.[132] AI infrastructure is also a priority, with massive data centres and computing hubs being aggressively built, in part to fuel AI/ML biotech utilisation.[133] Domestic firms are growing their engineering capabilities to produce PCR and diagnostic instrumentation, and NGS solutions like the MGI sequencing platforms. BGI Group, a Chinese powerhouse in genomics and life sciences, maintains an instrumentation division that develops sequencers, lab-automation platforms, and novel products like single-cell RNA analysis sets and high-performance computing solutions for high-throughput sequencing environments.[134] China's CRO market is rapidly growing to keep up with the demand for preclinical research services and clinical trials.[135] For example, China has steadily launched more clinical trials than Europe and the US in the past five years.[136] In sum, a domestically supported BITS is developing, powered by China's growing Validation Engine ecosystem that supplies core instrumentation, automated-lab infrastructure, compute and an expansive CRO network.

The Validation Engine (Layer 2) in India is defined by a focused commitment to compute build-out, likely in part

to support the adoption of AI in life sciences research, and a mature CRO base, with top-end instrument manufacturing seeing a more gradual transformation. A landmark announcement in October 2025 committed $15 billion to Google's AI/data-centre hub in Visakhapatnam, materially upgrading national AI capacity for research and industry, including tech-bio.[137] Government programmes under the IndiaAI Mission highlight 38,000 GPUs and public investment to broaden access to AI infrastructure; private initiatives expand domestic GPU clouds.[138] India's CRO ecosystem – long established and cost-competitive – continues to attract global trials and outsourcing, with analyses pointing to APAC's doubling of clinical activity by the early 2030s and heavy investment by global CROs in local digital-trial platforms.[139] However, as discussed above in Layer 1, the uphill challenges India faces there will affect the downstream areas as well.

Layer 3: The Execution Engine (The Factory)

Within this Execution Engine layer (The Factory), the US is home to the world's largest biopharmaceutical industry and remains a leader in innovative biologics and complex drug manufacturing.[140] In 2025, major US biomanufacturing investment announcements were up from the previous years, indicating a potential reshoring of biomanufacturing.[141] The US is still a leader in innovative biologics and complex drug manufacturing. For example, the US accounts for 90% of the 6,000 FDA-registered biologics manufacturing facilities worldwide.[142] Analysing global shares of value-added output in pharmaceuticals between 1995 and 2020, the US ranks first in the world for pharmaceutical production.[143] Where the US is falling behind is in API and intermediates manufacturing, a space largely filled currently by China and India.[144] FDA data from 2019 shows that only 28% of API manufacturers were in the US, while 72% were overseas.[145] The US heavily relies on foreign APIs and intermediates.[146] The US is acutely aware of other countries rapidly developing their biotech ecosystems and its dependence on these foreign countries in the biopharmaceutical supply chain. Thus, one area of national discussion has been strengthening biopharmaceutical manufacturing domestically. Lawmakers introduced the Biomanufacturing Excellence Act of 2025 as an effort to reduce US dependence on foreign supply chains and to facilitate and accelerate manufacturing innovation.[147]

Europe continues to demonstrate strong capabilities in biologics and FDF manufacturing, underpinned by a sustained policy and investment commitment to retaining advanced pharmaceutical production within the region. Over the past two decades, major European pharmaceutical companies have expanded and modernised domestic manufacturing footprints, reflecting a strategic preference for resilience and control amid increasingly fragile global supply chains.[148] Several European countries now host state-of-the-art biologics production facilities capable of producing monoclonal antibodies, cell and gene therapies and other complex modalities at commercial scale and the region ranks first globally for new biologics investment.[149] Similar to the US, Europe recognises the intensifying global competition in the BITS and the risk of gradual erosion of market share if domestic capabilities are not actively invested in and supported. This recognition has translated into coordinated public-sector initiatives, some of which are aimed at preserving and strengthening leadership in biomanufacturing.[150] Notably, the EU launched the Strategy to Boost Biotechnology and Biomanufacturing to outline actions for stimulating the biotech industry and providing for long-term sustainability.[151] The Critical Medicines Act, proposed in March 2025, aims to strengthen manufacturing capacity within the EU while addressing supply chain vulnerabilities and structural market failures.[152] Complementary national-level incentives, ranging from grant incentives and competitive tax credits, further reinforce Europe's commitment to anchoring high-value biopharmaceutical manufacturing within its borders.[153] Taken together, these measures signal that Europe views biologics and advanced drug manufacturing not only as an economic asset, but as a strategic capability central to healthcare security, industrial competitiveness, and technological sovereignty.

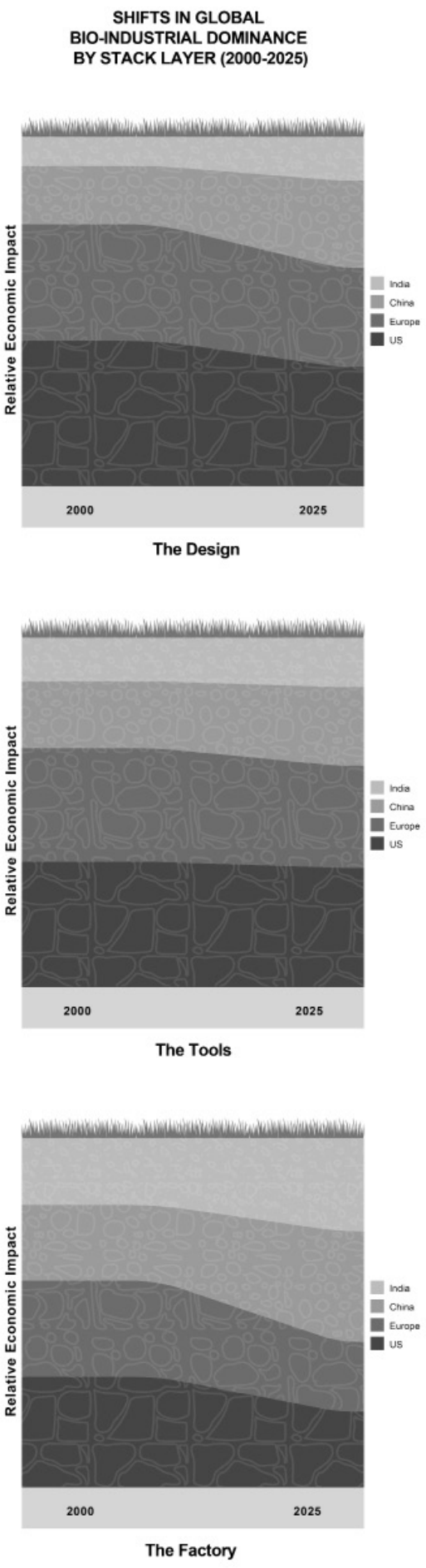
China has expanded its pharmaceutical manufacturing infrastructure over the past two decades, particularly in APIs and intermediates.[154] China now accounts for a substantial share of global API production capacity; in 2024, China became the leader in API DMFs at the FDA and today, upwards of 40% of the global production of APIs are coming out of China.[155] Biomanufacturing is supported by industrial clustering and large-scale plants capable of producing millions of tons of APIs annually.[156] China, making concerted efforts to meet international cGMP and ESP standards, has its sights set on more complex molecule manufacturing, expanding its generic API capabilities into the spaces that the US and Europe have historically dominated.[157] However, despite this progress, persistent regulatory, quality-assurance, and structural industry challenges suggest that China has not yet achieved parity with the US and Europe in complex molecule manufacturing, and significant gaps must be closed before it can claim sustained leadership in this domain.[158]

India has long been recognised as a global leader in generic drugs and API production, earning the nickname the 'pharmacy of the world' through its substantial share of affordable medicines abroad.[159] The Indian pharmaceutical industry is one of the largest globally by volume and manufactures over 500 different APIs and holds a commanding share of all APIs in the world.[160] Like China, India has articulated an ambition to evolve its robust ecosystem towards biologics and advanced therapies manufacturing.[161] However, regulatory uncertainty and IP constraints continue to be a barrier to innovation and commercialisation in these segments.[162]

Trends Over the Last 25 Years

How each geography trended in the past 25 years may provide insightful information on where the BITS is going to be in the future. To quantify these trends, we quantified the strength of a country in each layer based on the output and foothold the country had on the layer both in 2000 and in 2025. This quantification is depicted in the figure below.

See overleaf



As the data demonstrates, the global centre of gravity in biotechnology has evolved from western dominance to a more distributed, capability-specific competition across all layers of the BITS. Between 2000 and 2025, the US largely retained leadership in upstream discovery while ceding some share and resiliency in the downstream layers; Europe preserved depth in science and manufacturing but lost relative momentum in adoption and scale as efficient drug discovery relies on AI; China executed a fast multi-layer catch-up by coupling regulatory and capital mobilisation with rapid AI integration; and India translated generics excellence and CRO strengths into a base for innovation, though talent, policy, and data gaps tempered the pace. The practical implication is straightforward: national advantage now turns on integrated performance across layers, not any single metric such as publications or funding, and the trend lines show converging strengths with distinct vulnerabilities in each geography.

Layer 1 trends

Advancements in technology over the past 25 years have impacted the Design Engine (Layer 1): what was once a hypothesis-driven, lab-first discovery process is progressing towards an engineered, AI-enabled approach, culminating in a complex ecosystem of biology, chemistry and technology. Success in upstream drug discovery means capability to couple models with high-quality, human-relevant data and rapid validation loops. The US remains a top-layer architect, but a decrease of national investment and coalition puts the US at risk for impeded innovation. A lack of public biotech libraries, infrastructure, and national policy also contributes to the risk of falling behind in global competitiveness. Europe has maintained scientific depth but has noticeably under-invested in AI in life sciences at a time where all other major players are invested. This downward trend could put Europe at risk of losing its leadership position in biopharmaceutical innovation. China arguably saw the fastest catch-up during this period, having almost no presence in target and compound identification to being a global competitor. Policy alignment, AI integration, and talent resurgence have formed China's basis for the creation of an R&D hub and producing first-in-class drugs for the first time. Over time, India has addressed gaps in their biotech ecosystem to shift from reverse-engineering to innovation, and desires to be a biotech hub will continue to have slow progress if the struggles with regulatory reform, IP protection, and talent and education gaps persist.

Layer 2 trends

The Validation Engine (Layer 2) has evolved from just physical laboratory instrumentation to automated, digitally enabled platforms that provide researchers enhanced efficiency and precision. The US continues to lead in frontier tools, but manufacturing footprints for components have trended offshore. Europe maintains its reputation for cutting-edge instrumentation output but is falling behind in AI integration, which will cause delays in the Design Engine (Layer 1). China has been actively investing in domestic engineering of life science instrumentation platforms and AI infrastructure, and paired with its growing CRO industry, is trending towards a robust Validation Engine to support its Design Engine activities. India remains at the early stages of being a go-to supplier of high-end instrumentation but has committed to building AI infrastructure to support AI-enabled drug discovery.

Layer 3 trends

Over the past 25 years, the US has increasingly outsourced production and relied on foreign materials and operations, leading to growing calls for reshoring to safeguard against global supply chain instability and revitalise American manufacturing. However, the US has maintained leadership in biologics and complex drug manufacturing. Policy is moving to maintain resilience. Europe turned biomanufacturing into strategic hedge-modernised sites, concentrated biologics capacity, and region-wide industrial policy to secure critical medicines and sovereignty. China and India are dominant in APIs and intermediates manufacturing but have not yet caught up on biologics capabilities.

Conclusion: The Structural Imperative of the Bio-Industrial Stack

The transition of biotechnology from a discipline of discovery to one of engineering has fundamentally decoupled the design of a molecule from its physical execution. As this analysis has demonstrated through the BITS framework, the coming years will be defined by how nations navigate the friction between globalised innovation and the necessity of domestic infrastructure. The geopolitical map is no longer a static representation of R&D spend; it is a dynamic landscape of integrated, sovereign capabilities.

The BIOSECURE Act represents a significant pivot in this landscape – a formal recognition that the provenance of the 'Tools' (Layer 2) and the 'Factory' (Layer 3) is as critical as the ingenuity of the 'Code' (Layer 1). For a nation to maintain its leadership in a multi-polar world, it must resolve the paradox of 'digital-only' leadership. Owning the code without the means for production creates a systemic fragility that is no longer sustainable under shifting geopolitical pressures.

As the BITS continues to mature, we expect to see a more decentralised approach to the physical layers of the stack. While coastal hubs in the US remain the command centres for the digital architecture of biology around the world, the physical requirements of the stack provide a unique opportunity for geographic diversification in the US and abroad. In the US, for example, the Midwest is uniquely positioned to become the bedrock of the 'Bio-Industrial Engine'. By leveraging deep-seated industrial expertise, proximity to agricultural feedstocks, and a robust manufacturing workforce, the heartland can bridge the gap between coastal innovation and commercial-scale execution. This regional integration creates a more resilient domestic stack that is less susceptible to the supply shocks inherent in an outsourced model. Such an idea and model is one for immediate consideration across many territories around the world.

Ultimately, the stakes of the BITS go beyond market dominance. They concern the fundamental ability of a state to define, validate, and manufacture its own strategic requirements – from health security to industrial autonomy. History suggests we are at a crossroads similar to the mid-century space race or the turn-of-the-century mapping of the human genome. While those eras were defined by the pursuit of singular milestones, the current era is defined by the mastery of a general-purpose technology that will underpin the next century of materials, health, and economic stability. Ultimately, the coming years will distinguish those nations that viewed biotechnology as a series of disparate scientific breakthroughs from those that recognised it as a unified industrial system. To secure the stack is not merely an exercise in economic development; it is the fundamental prerequisite for sovereignty in the century of biology. A nation's standing in the multi-polar world of 2050 will be determined by its ability to integrate the Design, Validation, and Execution Engines into a singular, resilient architecture.

Endnotes

1 The Global Bioeconomy: https://www.naturefinance.net/wp-content/uploads/2024/05/ENG-TheGlobalBioeconomy_FINAL.pdf

2 https://www.genome.gov/25520478/online-education-kit-2000-working-draft; *After the Doubling*, Jay H. Hoofnagle, MD; https://onlinelibrary.wiley.com/doi/epdf/10.1002/hep.20342

3 *Id.*

4 The Global Biomedical Industry: Preserving U.S. Leadership, Executive Summary & Research Findings, DeVol, *et al.*

5 *Id.*

6 https://www.thefdalawblog.com/wp-content/uploads/2022/11/1997-FDAMA-Summary.pdf

7 *Id.* (Swiss firm Novartis AG established its main research hub in Massachusetts, Roche acquired majority stake in Genentech in 1990 and full ownership in 2009 and Sanofi acquired Genzyme in 2011); https://www.americanimmigrationcouncil.org/fact-sheet/foreign-born-stem-workers-united-states

8 Location of pharmaceutical innovation: 2000–2009, Yali Friedman; https://patentbaristas.com/wp-content/uploads/2010/11/Location-of-pharmaceutical-innovation-2000-2009.pdf

9 The competitiveness of European biotechnology: a case study of innovation (Graphs V.1 and V.2).

10 https://ncses.nsf.gov/pubs/nsb20214/publication-output-by-country-region-or-economy-and-scientific-field#:~:text=Table_title:%20Chart%20Table_content:%20header:%20%7C%20Publication%20year,States:%20330%2C543%20%7C%20United%20Kingdom:%2076%2C341%20%7C

11 *Id.*

12 https://www.ema.europa.eu/en/about-us/history-ema; Thirty years of European biotechnology programmes: from biomolecular engineering to the bioeconomy, Aguilar, *et al.*; *see also* 40 Years of Framework Programmes in 70 years of EU research: a brief history, Nikos Kastrinos.

13 The Global Biomedical Industry: Preserving U.S. Leadership, Executive Summary & Research Findings, DeVol, *et al.*

14 https://www.pnhp.org/system/assets/drupal/docs/Global-Drug-Discovery-Europe-is-ahead.pdf

15 https://www.efpia.eu/publications/data-center/the-pharma-industry-in-figures-rd/pharmaceutical-rd-expenditure-in-europe-usa-china-and-japan

16 https://ncses.nsf.gov/pubs/nsb20214/publication-output-by-country-region-or-economy-and-scientific-field#:~:text=Table_title:%20Chart%20Table_content:%20header:%20%7C%20Publication%20year,States:%20330%2C543%20%7C%20United%20Kingdom:%2076%2C341%20%7C; Location of pharmaceutical innovation: 2000–2009, Yali Friedman; https://patentbaristas.com/wp-content/uploads/2010/11/Location-of-pharmaceutical-innovation-2000-2009.pdf

17 Ni J, Zhao J, Ung CO, Hu Y, Hu H, Wang Y. Obstacles and opportunities in Chinese pharmaceutical innovation, Global Health, 2017 Mar 24;13(1):21. doi: 10.1186/s12992-017-0244-6, PMID: 28340579; PMCID: PMC5366105.

18 https://www.biopharminternational.com/view/china-today-biogenerics-china-evolving-industry

19 Agten, S., Wu, B. (2024). Innovation in the Chinese Biopharma Sector: From Me-too to First-in-Class. In: Biopharma in China. Palgrave Macmillan, Singapore.

20 *Id.*

21 https://thechinaproject.com/2020/05/12/end-of-an-era-a-history-of-chinese-students-in-america

22 *Id.*

23 The Internationalization Challenge: Where to Access Innovation Chapter 7.2.

24 Chen Y, Wang C, Shang H, Yang K, Norris SL. Clinical practice guidelines in China. BMJ. 2018 Feb 5; 360:j5158. doi: 10.1136/bmj.j5158. PMID: 29437564; PMCID: PMC5797982.

25 Differding E. The Drug Discovery and Development Industry in India—Two Decades of Proprietary Small-Molecule R&D. *ChemMedChem* 2017, 12, 786–818.

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.*

30 *Id.* at Figure 2.

31 *Id.*

32 *See e.g.,* https://www.chemeurope.com/en/news/14170/perkinelmer-launches-three-new-drug-discovery-reagent-platforms.html

33 https://archive.nytimes.com/www.nytimes.com/library/national/science/062700sci-genome-history.html

34 https://frontlinegenomics.com/a-brief-history-of-next-generation-sequencing-ngs

35 https://frontlinegenomics.com/a-brief-history-of-next-generation-sequencing-ngs; https://www.illumina.com/science/technology/next-generation-sequencing/illumina-sequencing-history.html; https://centuryofbio.com/p/illumina; China, Biotechnology, and BGI. How China's Hybrid Economy Skews Competition by Anna B. Puglisi and Chryssa Rask. Center for Security and Emerging Technology, May 2024.

36 https://portersfiveforce.com/blogs/brief-history/agilent?utm; https://www.agilent.com/content/dam/about/newsroom/media-room/asms2019/agilent-ASMS-history.pdf?srsltid=AfmBOooQqUapXyuCA1wsoX9l679apvNNBOZlAuVkPUw7Qv-F43Sl4e9K

37 https://www.bio-rad.com/en-us/about/our-history?ID=1757378124555

38 https://www.beckman.com/about-us/company-history/product-timeline

39 https://marnoa.ca/danaher-a-global-leader-in-bioprocessing-2

40 https://www.referenceforbusiness.com/history2/71/PerkinElmer-Inc.html#:~:text=Two%20years%20later%2C%20the%20company,in%20the%20years%20to%20come.&text=Agilent%20Technologies%20Inc.;%20Thermo%20Electron%20Corporation;%20Waters%20Corporation

41 https://orip.nih.gov/division-construction-instruments/s10-instrumentation-programs

42 https://pharmaphorum.com/views-and-analysis/a_history_of_contract_research_organisations_cros

43 Reiss T, Woerner S. The biotech equipment and supplies sector in Europe—is it European? *Journal of Biotechnology 98* (2002) 41–51.

44 *Id.*

45 https://www.roche.com/about/history

46 https://www.fundinguniverse.com/company-histories/qiagen-n-v-history

47 https://www.analytik-jena.kr/jp/company/about-us/history/product-history.html

48 https://www.institut-merieux.com/en/deep-rooted-history/a-pasteurian-tradition

49 https://ismr.org/the-biacore-story.html

50 https://wellcome.org/research-funding; https://eur-lex.europa.eu/EN/legal-content/summary/sixth-framework-programme-2000-2006-life-sciences-genomics-and-biotechnology-for-health.html

51 https://www.cobiotech.eu/european-biotech-hub/european-programmes-and-initiatives

52 https://itif.org/publications/2019/08/12/chinas-biopharmaceutical-strategy-challenge-or-complement-us-industry

53 https://www.agilent.com/about/companyinfo/history/timeline_1990s.html#:~:text=1994,into%20the%20routine%20laboratory%20environment; https://tile.loc.gov/storage-services/master/gdc/gdcebookspublic/20/23/70/94/74/2023709474/2023709474.pdf?utm

54 https://pubsapp.acs.org/cen/coverstory/84/8414pittcon7.html?utm_source=chatgpt.com&

55 *See* https://pubsapp.acs.org/cen/coverstory/84/8414pittcon7.html?utm

56 https://www.pharmexec.com/view/risks-and-rewards-pharma-post-wto-china

57 https://www.agilent.com/about/companyinfo/history/timeline_1990s.html#:~:text=1994,into%20the%20routine%20laboratory%20environment; https://tile.loc.gov/storage-services/master/gdc/gdcebookspublic/20/23/70/94/74/2023709474/2023709474.pdf?utm

58 Shi Y., Hu H., and Wang C. Contract Research Organization (CROs) in China: integrating Chinese research and development capabilities for global drug innovation, *Globalization and Health* 2014, 10:78.

59 https://tile.loc.gov/storage-services/master/gdc/gdcebookspublic/20/23/70/94/74/2023709474/2023709474.pdf?utm; Shi Y., Hu H., and Wang C. Contract Research Organization (CROs) in China: integrating Chinese research and development capabilities for global drug innovation, *Globalization and Health* 2014, 10:78.

60 https://www.niper.gov.in/central-instrumentation-laboratories

61 Differding E. The Drug Discovery and Development Industry in India—Two Decades of Proprietary Small-Molecule R&D, *ChemMedChem* 2017, 12, 786–818.

62 *Id.*

63 *Id.*

64 https://www.pharmtech.com/view/contract-manufacturing-through-years

65 https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/the-biologics-manufacturing-wars.pdf.coredownload.inline.pdf

66 https://www.nationalacademies.org/read/26420/chapter/6#76

67 https://asia.nikkei.com/static/vdata/infographics/chinavaccine-3

68 Daemmrich A. Pharmaceutical Manufacturing in America: A Brief History. AIHP 59 (2017) No. 3; https://repository.si.edu/server/api/core/bitstreams/75a66d01-ba23-476b-996c-84ab0812b0f6/content

69 Daemmrich A. Pharmaceutical Manufacturing in America: A Brief History, AIHP 59 (2017) No. 3; https://repository.si.edu/server/api/core/bitstreams/75a66d01-ba23-476b-996c-84ab0812b0f6/content

70 https://qualitymatters.usp.org/global-manufacturing-capacity-active-pharmaceutical-ingredients-remains-concentrated?source=email

71 https://asia.nikkei.com/static/vdata/infographics/chinavaccine-3; https://pharmexcil.com/v1/docs/ChinaAPIsExport&ImportTrends.pdf

72 https://qualitymatters.usp.org/geographic-concentration-pharmaceutical-manufacturing?utm; https://www.efpia.eu/media/rm4kzdlx/the-pharmaceutical-industry-in-figures-2023.pdf; https://www.nationalacademies.org/read/26420/chapter/6#76; https://globalresearchonline.net/journalcontents/v45-1/24.pdf

73 Differding E. The Drug Discovery and Development Industry in India—Two Decades of Proprietary Small-Molecule R&D, *ChemMedChem* 2017, 12, 786-818; https://www.nationalacademies.org/read/26420/chapter/6#72; https://www.nationalacademies.org/read/26420/chapter/6?utm

74 https://www.pharmamanufacturing.com/sector/contract-manufacturing/article/11364552/processing-engineering-contract-research-in-china-a-catalyst-for-pharmaceutical-industry-growth-pharmaceutical-manufacturing

75 https://www.efpia.eu/publications/data-center/the-pharma-industry-in-figures-rd/pharmaceutical-rd-expenditure-in-europe-usa-china-and-japan

76 Securing Europe's competitiveness, McKinsey Global Institute.

77 https://itif.org/publications/2024/02/29/not-again-why-united-states-cant-afford-to-lose-biopharma-industry

78 https://research.contrary.com/report/the-state-of-the-us-china-biotech-race; National Institutes of Health (NIH) Funding: FY1996-FY2026 Request | Congress.gov | Library of Congress; https://www.congress.gov/crs-product/R43341

79 https://www.orfonline.org/expert-speak/harnessing-ai-for-drug-discovery-the-race-to-innovate-and-govern?utm; https://www.drugtargetreview.com/news/157365/first-ai-designed-drug-rentosertib-named-by-usan/#:~:text=Insilico%20Medicine's%20AI%2Ddesigned%20drug,explore%20novel%20approaches%20to%20treatment

80 https://www.orfonline.org/expert-speak/harnessing-ai-for-drug-discovery-the-race-to-innovate-and-govern?utm

81 https://origin.arpa-h.gov/news-and-events/arpa-h-project-accelerate-discovery-and-development-new-antibiotics-using

82 https://www.nsf.gov/tip/updates/reflecting-nsf-tip-2025-looking-ahead-2026; https://arpa-h.gov/news-and-events/arpa-h-project-accelerate-discovery-and-development-new-antibiotics-using; https://itif.org/publications/2024/11/15/to-do-accelerate-ai-adoption-in-biopharma-research

83 https://www.biotech.senate.gov/final-report/chapters/chapter-1

84 https://www.cnas.org/publications/reports/biotech-matters-problems-with-life-science-databases-in-the-united-states

85 https://www.illumina.com/company/news-center/press-releases/press-release-details.html?newsid=fda84c92-b4b3-4691-a402-35555abe8605; https://www.10xgenomics.com/ai

86 Securing Europe's competitiveness, McKinsey Global Institute.

87 https://www.efpia.eu/a-strategy-for-european-life-sciences

88 https://itif.org/publications/2025/02/21/europe-trails-united-states-over-26-percent-share-global-biopharma-rd

89 https://ncses.nsf.gov/pubs/nsb20214/publication-output-by-country-region-or-economy-and-scientific-field#:~:text=Table_title:%20Chart%20Table_content:%20header:%20%7C%20Publication%20year,States:%203; Securing Europe's competitiveness, McKinsey Global Institute.

90 https://www.efpia.eu/a-strategy-for-european-life-sciences

91 *Id.*

92 Securing Europe's competitiveness, McKinsey Global Institute; https://www.labiotech.eu/trends-news/ai-biotech-europe-lag

93 https://www.orfonline.org/expert-speak/harnessing-ai-for-drug-discovery-the-race-to-innovate-and-govern?utm

94 https://www.efpia.eu/media/fzkbhzoe/a-competitiveness-strategy-for-european-life-sciences.pdf

95 https://www.fdd.org/analysis/policy_briefs/2025/03/19/aiming-for-parity-with-u-s-china-announces-increase-in-science-and-technology-spending

96 https://www.geneonline.com/a-decade-of-discovery-how-chinas-early-stage-innovations-are-changing-the-game-in-global-drug-development

97 https://research.contrary.com/report/the-state-of-the-us-china-biotech-race; Shi Y., Hu H., and Wang C. Contract Research Organization (CROs) in China: integrating Chinese research and development capabilities for global drug innovation, *Globalization and Health* 2014, 10:78.

98 https://pubmed.ncbi.nlm.nih.gov/40262297; https://globalforum.diaglobal.org/issue/march-2025/chinas-new-drug-approvals-again-hit-record-high-in-2024

99 https://www.fiercepharma.com/pharma/china-approves-4-new-drugs-including-global-first-class

100 https://merics.org/en/report/lab-leader-market-ascender-chinas-rise-biotechnology

101 https://www.sinodrugwatch.com/china-pharma-pulse-innovation-reform-global-dealmaking-surge; https://baipharm.chemlinked.com/news/2022s-top-10-cross-border-licensing-deals-involving-chinese-biopharma-companies; https://www.mckinsey.com/~/media/mckinsey/industries/life%20sciences/our%20insights/vision%202028%20how%20china%20could%20impact%20the%20global%20biopharma%20industry/vision-2028-how-china-could-impact-the-global-biopharma-industry

102 https://www.franklintempletonglobal.com/articles/2025/clearbridge-investments/china-emerging-as-a-global-biotechnology-player

103 https://www.uscc.gov/research/made-china-2025-evaluating-chinas-performance#_Toc213921806

104 *Id.*

105 https://www.orfonline.org/expert-speak/harnessing-ai-for-drug-discovery-the-race-to-innovate-and-govern?utm

106 https://www.investindia.gov.in/team-india-blogs/indias-prip-scheme-generics-leader-innovation-powerhouse-pharma-medtech

107 *Id.*

108 *Id.*

109 https://pharma.economictimes.indiatimes.com/news/pharma-industry/india-bets-on-generative-ai-to-reshape-drug-discovery-says-union-minister-jitendra-singh/125939402

110 https://iisc.ac.in/events/ministry-of-education-establishes-ai-centre-of-excellence-for-healthcare-tanuh-at-iisc

111 https://www.aurigeneservices.com/services/discovery/ai-assisted-drug-discovery

112 https://www.insightsonindia.com/2025/10/16/indias-biotech-surge-and-its-scaling-challenges; https://economictimes.indiatimes.com/industry/healthcare/biotech/pharmaceuticals/regulatory-policy-reforms-crucial-for-future-of-indias-pharma-rd-report/articleshow/113780854.cms?from=mdr&utm

113 https://timesofindia.indiatimes.com/city/goa/research-gap-in-india-indias-phd-science-pursuits-lag-behind-us-and-china-only-10000-doctoral-candidates-in-a-population-of-1-4-billion/articleshow/126060585.cms

114 https://timesofindia.indiatimes.com/city/goa/research-gap-in-india-indias-phd-science-pursuits-lag-behind-us-and-china-only-10000-doctoral-candidates-in-a-population-of-1-4-billion/articleshow/126060585.cms

115 https://etedge-insights.com/featured-insights/people-and-organizations/bridging-indias-skills-gap-for-the-21st-century-workforce

116 https://www.insightsonindia.com/2025/10/16/indias-biotech-surge-and-its-scaling-challenges

117 https://www.genengnews.com/insights/bioinstrument-manufacturers-go-global

118 https://www.illumina.com/systems.html; https://www.illumina.com/company/news-center/press-releases/press-release-details.html?newsid=97798370-799c-4e86-b76d-7ef38b42766f; https://www.illumina.com/company/news-center/feature-articles/2026--a-turning-point-for-precision-health.html

119 https://intuitionlabs.ai/articles/ai-compute-demand-biotech

120 https://www.sepscience.com/innovations-unveiled-highlights-from-asms-2025-12029

121 *Id.*

122 https://www.illumina.com/company/news-center/press-releases/press-release-details.html?newsid=97798370-799c-4e86-b76d-7ef38b42766f

123 https://www.10xgenomics.com

124 https://www.investor.agilent.com/news-and-events/news/news-details/2025/Agilent-to-Showcase-New-Products-and-Innovations-at-HPLC-2025/default.aspx

125 https://www.cnbc.com/2025/01/15/us-imposing-new-export-controls-on-biotech-equipment-over-china-concerns.html; https://research.contrary.com/report/the-state-of-the-us-china-biotech-race

126 https://www.arnoldporter.com/en/perspectives/advisories/2025/12/the-biosecure-act-becomes-law-in-the-united-states

127 https://www.omrglobal.com/industry-reports/european-life-science-instrumentation-market

128 https://www.omrglobal.com/industry-reports/european-life-science-instrumentation-market

129 https://www.roche.com/media/releases/med-cor-2025-12-11; https://www.prnewswire.com/news-releases/roche-announces-us-launch-of-next-generation-cobas-68008800-systems-and-software-enhancing-laboratory-efficiency-and-testing-capabilities-3026427-38.html

130 https://merics.org/sites/default/files/2025-04/MERICS%20Report%20Biotech_04-2025.pdf

131 https://decodingbio.substack.com/p/embodied-ai-in-biotech-why-china

132 https://decodingbio.substack.com/p/embodied-ai-in-biotech-why-china

133 https://spacenews.com/new-report-details-chinas-push-to-dominate-artificial-intelligence/#:~:text=The%20report%20says%20China%20has,into%20security%20insights%20using%20AI.&text=Get%20unlimited%20access%20to%20SpaceNews,monthly%2C%20quarterly%20or%20annual%20subscription.&text=Learn%20more%20about%20savings%20available,military%20readers%20on%20SpaceNews%20subscriptions

134 https://en.genomics.cn

135 https://pmc.ncbi.nlm.nih.gov/articles/PMC4240890

136 https://merics.org/sites/default/files/2025-04/MERICS%20Report%20Biotech_04-2025.pdf

137 https://blog.google/intl/en-in/company-news/our-first-ai-hub-in-india-powered-by-a-15-billion-investment

138 https://www.rcrwireless.com/20250425/fundamentals/top-five-ai-data-center-india

139 https://www.emergenresearch.com/industry-report/contract-research-organization-market

140 https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/the-biologics-manufacturing-wars.pdf.coredownload.inline.pdf

141 https://www.jll.com/en-us/insights/market-perspectives/us-life-sciences.html/?utm_source=thirdparty&utm_medium=referral&utm_campaign=am-us-ind-life-lab-1124&utm_term=media; https://www.prnewswire.com/news-releases/global-location-strategies-report-350-billion-us-pharmaceutical-manufacturing-investment-boom-challenged-by-labor-shortages-tariffs-and-policy-shifts-302599866.html

142 https://www.prnewswire.com/news-releases/global-location-strategies-report-350-billion-us-pharmaceutical-manufacturing-investment-boom-challenged-by-labor-shortages-tariffs-and-policy-shifts-302599866.html

143 https://itif.org/publications/2024/02/29/not-again-why-united-states-cant-afford-to-lose-biopharma-industry

144 https://www.raps.org/news-and-articles/news-articles/2024/11/usp-india-and-china-continue-their-api-manufacturi ; https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/the-biologics-manufacturing-wars.pdf.coredownload.inline.pdf; https://itif.org/publications/2024/02/29/not-again-why-united-states-cant-afford-to-lose-biopharma-industry

145 https://itif.org/publications/2024/02/29/not-again-why-united-states-cant-afford-to-lose-biopharma-industry

146 https://phslrx.com/u-s-reliance-on-foreign-sources-of-api

147 https://www.fiercepharma.com/manufacturing/lawmakers-look-support-domestic-manufacturing-bill-proposing-us-center-excellence

148 https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/the-biologics-manufacturing-wars.pdf.coredownload.inline.pdf

149 https://www.mabion.eu/science-hub/articles/why-europe-is-becoming-a-global-hub-for-biologics-manufacturing; https://www.prnewswire.com/news-releases/global-location-strategies-report-350-billion-us-pharmaceutical-manufacturing-investment-boom-challenged-by-labor-shortages-tariffs-and-policy-shifts-302599866.html

150 https://www.mabion.eu/science-hub/articles/why-europe-is-becoming-a-global-hub-for-biologics-manufacturing; https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1570; https://europa.eu/youreurope/business/running-business/developing-business/biotech/index_en.htm

151 https://www.mabion.eu/science-hub/articles/why-europe-is-becoming-a-global-hub-for-biologics-manufacturing; https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1570

152 https://health.ec.europa.eu/medicinal-products/legal-framework-governing-medicinal-products-human-use-eu/critical-medicines-act_en; https://commission.europa.eu/topics/public-health/european-health-union/modernising-eu-pharmaceutical-legislation_en

153 https://www.idaireland.de/latest-news/insights/the-future-of-biopharma-in-ireland; https://www.trade.gov/country-commercial-guides/belgium-biopharmaceuticals-0; https://www.genengnews.com/news/report-urges-eu-nations-to-boost-rd-through-tax-regulatory-policies

154 https://www.raps.org/news-and-articles/news-articles/2024/11/usp-india-and-china-continue-their-api-manufacturi

155 https://qualitymatters.usp.org/global-manufacturing-capacity-active-pharmaceutical-ingredients-remains-concentrated?source=email; https://cepa.org/article/biotech-blues-the-west-struggles-to-stay-ahead; https://pmc.ncbi.nlm.nih.gov/articles/PMC9395832

156 https://www.apifdf.com/blog/apis-export-from-china

157 https://phmo.com/news/18; https://www.businesswire.com/news/home/20251002258239/en/China-Biologics-Contract-Manufacturing-Market-Industry-Trends-and-Forecasts-Report-2025-2035-Profiles-of-ChemPartner-Biologics-JHL-Biotech-JOINN-Biologics-MabPlex-Mycenax-Biotech-WuXi-AppTec---ResearchAndMarkets.com

158 https://ispe.org/pharmaceutical-engineering/march-april-2024/evolving-chinas-regulatory-system-alignment-ich?; https://www.linkedin.com/pulse/chinas-biomedicine-industry-2024-kjeld-friis-munkholm-%E5%AD%9F%E5%8F%AF%E5%92%8C-6dupf

159 https://qualitymatters.usp.org/global-manufacturing-capacity-active-pharmaceutical-ingredients-remains-concentrated?source=email

160 https://www.drugpatentwatch.com/blog/indias-growing-importance-in-generic-drug-api-manufacturing/?srsltid=AfmBOop2UvlU2gTXR_fNtyooG39oaU7u4eL93d_xmWkYL_0Z38yUaaF0

161 https://www.pharmabiz.com/NewsDetails.aspx?aid=183511&sid=1

162 https://www.pharmabiz.com/NewsDetails.aspx?aid=183511&sid=1



Dr. Milad Alucozai, recognised by *Business Insider* as "one of the top 100 early-stage investors", is a neuroscientist, founder, and active investor dedicated to translating exceptional science and technology into scalable commercial ventures.
He currently serves as a Co-founder and General Partner at Pamir Ventures, an early-stage venture fund that invests in technical pioneers developing B2B companies utilising AI in antiquated industries. He is also a co-founder of Revalia Bio, a leading AI company enabling "Human Data Trials" to accelerate drug development with real human data before the first clinical trial begins.
Throughout his operating and investing career, Milad has played a crucial role in helping founders secure hundreds of millions in capital and facilitating billions in startup-pharma partnerships.

Pamir Ventures
One Embarcadero Center, Suite 1050
San Francisco, California 94111
USA

Tel: +1 617 432 7732
Email: milad@pamir.vc
LinkedIn: www.linkedin.com/in/miladalucozai



Jason Novak advises companies of all sizes on legal issues arising from emerging technologies, with a particular emphasis on AI/ML. His practice centres on "convergence" technologies – such as digital health, precision medicine, and alternative protein – that sit at the intersection of multiple industries. Drawing on cross-disciplinary training and deep in-house experience, Jason helps organisations navigate the complex legal and strategic challenges that come with blending traditionally distinct sectors.
Jason's work focuses on IP and data rights strategy, which are of particular importance and complexity in "convergence" fields. With data rights, data must be treated as an offensive asset. To that, Jason supports clients on transactions, protection, and strategic long-term planning. Jason's IP experience includes patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in- and out-licensing, freedom-to-operate, due diligence, IP training, risk management, and dispute resolution.

Norton Rose Fulbright
One Embarcadero Center, Suite 1050
San Francisco, California 94111
USA

Tel: +1 628 231 6811
Email: jason.novak@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/jason-novak-002102b



Dr. Nathanael Green is an associate in Norton Rose Fulbright's Houston office. His practice focuses on developing IP portfolios mainly for universities and life science companies. Nate counsels clients on portfolio strategies, which include preparing and prosecuting patent applications and developing patent landscape opinions. Nate has experience with technologies across the life science space, including cellular therapies, gene therapies, small molecules, diagnostic assays, medical devices, organic chemistry and drug screening. Nate also conducts due diligence review on IP portfolios for potential investment and acquisition.
Nate received his J.D. from University of Houston Law Center. Prior to a career in law, Nate performed biomedical research focusing on the intersection of metabolism and RNA transcription regulation in kidney cancer at Baylor College of Medicine, where he received a Ph.D. in pharmacology.

Norton Rose Fulbright
1550 Lamar Street, Suite 2000
Houston, Texas 77010-4106
USA

Tel: +1 713 651 5422
Email: nathanael.green@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/nathanael-green-phd-05433757



Sophia Poirier has a BS and MS in Biomedical Engineering, and her practice areas include patent prosecution and patent litigation. Sophia had a career in R&D and Regulatory Affairs before going to law school at the University of Texas School of Law. While completing her master's degree, Sophia conducted biomechanical research and co-authored peer-reviewed scientific papers.

Norton Rose Fulbright
98 San Jacinto Boulevard, Suite 1100
Austin, Texas 78701
USA

Tel: +1 512 536 2478
Email: sophia.poirier@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/sophia-poirier

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full-business law service. We have more than 3,500 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.
Recognised for our industry focus, we are strong across all the key industry sectors: financial institutions; energy, infrastructure and resources; transport; technology; life sciences and healthcare; and consumer markets. Through our global risk-advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

The Geopolitical Tipping Point: Forecasting Global Bio-Industrial Technology Stack (BITS) Dominance Through 2050


Dr. Milad Alucozai


Jason Novak

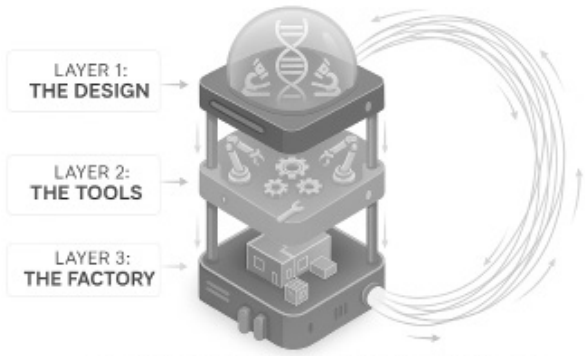

Dr. Nathanael Green


Ebony Christian

Norton Rose Fulbright

Executive Summary

Building upon the Bio Industrial Technology Stack (BITS) framework, this chapter forecasts how the interlocking engines of the Code, Tools, and Factory layers will be contested by the United States, European Union, India, and China through 2050. To lead the conversation, we must move beyond the standard call for "more funding" and frame this as a structural and philosophical shift in how a nation secures its future. As a refresher, we define the layers for the BITS framework as follows:



BITS: BIO-INDUSTRIAL TECHNOLOGY STACK

- Layer 1: The Design Engine (The Code). This represents the upstream architecture where biology is transformed into a more rigorous engineering discipline. This is the "programming" layer of the stack, where AI is leveraged to model targets and simulate biological systems with precision before they ever reach a laboratory setting. It serves as the fundamental source code of the bioeconomy.
- Layer 2: The Validation Engine (The Tools). This engine serves as the high-fidelity filter of the stack, bridging the gap between digital design and physical truth through various tools, including analytical software and instrumentation. It explicitly incorporates digital infrastructure, specifically GPU fabrics and data commons, which should be viewed not as passive background assets but as active tools of clinical certainty. By utilising digital twins and mechanistic modelling, this layer provides the essential proof that the Design Engine's code remains valid in human systems before capital is committed to large-scale production in the factory. Crucially, the Validation Engine is the bridge that resolves the "digital-only" leadership paradox. By establishing a sovereign truth layer, we ensure that the ingenious designs of the Code layer are not merely theoretical "hallucinations" but are anchored in human-relevant data before a single dollar is committed to physical scale.
- Layer 3: The Execution Engine (The Factory). This constitutes the hard infrastructure of mass production and sovereign supply chains. While the Validation Engine focuses on proving efficacy, the Execution Engine is defined by the physical ability to manufacture and distribute millions of doses through bioreactors, active pharmaceutical ingredients (APIs), and specialised CDMO networks.

The true power of the BITS framework lies in its recursive nature. We must move beyond viewing these layers as a linear pipeline and instead treat them as the "Sovereign Flywheel" illustrated above. In this model, performance data from the Execution Engine (Layer 3) flows back into the Design Engine (Layer 1), creating a closed-loop system where manufacturing yields refine our AI models. This transforms biology from a series of disparate scientific milestones into a unified, self-improving industrial system.

Each geographic region is pursuing distinct strategies to secure technological leadership, supply resilience, and talent advantages. The coming decades will be defined not just by innovation, but by the ability to integrate these engines into a unified national strategic asset.

For example, the US is clearly committed to furthering AI-enabled discovery and data sharing. It is also developing data-governance regimes at the federal and state level. To this end, while the National Institute of Standards and Technology (NIST) has set out AI governance guidelines, the US is still a good distance away from effectuating comprehensive data privacy and governance rules that are harmonised across states, as the EU has done across countries. The US will likely continue striving to re-shore drug manufacturing and hardware development to stay relevant in the Factory layer, but will lag behind China and India. On the other hand, the EU is advancing shared data spaces and regulatory streamlining but continues to face challenges with translation of pure R&D to manufacturing and digital competitiveness. While the General Data Protection Regulation (GDPR) is a robust data-governance regime, over-regulation can be a hindrance to data sharing and complex environmental regulatory schemes can continue to delay the translation of pure R&D into drug manufacturing. Meanwhile, China and India are executing state-led bioeconomy strategies to capture share across the three-layer R&D pipeline. China is quickly catching up as a global competitor in AI infrastructure and life sciences instrumentation (Layer 1), to support its growing presence in target and compound identification (Layer 1), all the while continuing to scale its biomanufacturing (Layer 3), while India is leveraging its generics leadership and kickstarting new

biofoundry programmes. India is also expressing willingness to partner internationally to climb the discovery stack and improve its presence in drug development.

United States AI-first Discovery and the Race to Re-shore Manufacturing

The US will likely maintain strength in AI-led discovery and strong upstream R&D even under tighter data-governance standards. However, the push to re-shore manufacturing will take considerable time to achieve and will likely still lag behind Chinese and Indian efforts.

Layer 1: The Design Engine (The Code)

The US will likely maintain strength in upstream R&D in 2050, as evidenced by its current posture and its heavy investment in cutting-edge technologies fuelled by AI and quantum computing. For instance, the US is scaling publicly funded AI for upstream R&D via programmes such as ARPA-H's digital/AI programmes and NIH's Bridge2AI to lower compute barriers for academia and biotech companies.[1] Publicly funded AI will likely accelerate multimodal genomics and simulation-heavy workflows, and increase access to compute power for intensive modelling. The US push to make AI accessible across industry and academia is designed to expand collaboration and data sharing. This supports broad *in silico* model development while parallel efforts to grow large-scale human-data pipelines continue to build the "data refineries" that anchor the Code layer. Together, these moves reinforce the US position by emphasising durable data assets rather than model intellectual property (IP) alone.

Under the NIH Data Management & Sharing Policy, the US is signalling increased focus on comprehensive data harvesting and sharing scientific data sets.[2] Regulators across agencies are charting a course to institutionalise model-informed drug development (MIDD) through efforts like the FDA's MIDD Paired Meeting Program and expanded use of *in silico* modelling and simulation in regulatory science.[3] Such efforts will encourage private sector and academia participants to curate shared data sets and lead to broader use of statistical modelling derived from preclinical and clinical data sources during early stage drug development and R&D.[4] This collaborative approach will allow industry, government, and academia to gather evidence reflective of the diversity of the population, teeing up breakthroughs in personalised medicine and guiding better regulatory decision making.[5]

Despite growth in AI, major players in the US drug discovery space will likely face data governance challenges due to bifurcated data privacy laws across states, e.g., the California Consumer Privacy Act/California Privacy Rights Act and Washington's My Health My Data Act, and the lack of comprehensive federal data privacy laws pre-empting a myriad of state laws. Additionally, the US has signalled a desire for tighter governance to mitigate and deter national security risks. Concurrently, federal law and regulations, including Executive Order (EO) 14117, 28 CFR Part 202 safeguards for controlled-access data, NIST's AI Risk Management Framework, and the FDA's AI/ML framework, are all tightening standards for data provenance, AI validation, and data security.[6]

More publicly funded genomic and phenotypic data will be reusable for drug discovery R&D, but teams seeking government grants must invest in governance, consent, and controlled-access workflows to maintain datasets. In the coming decades, we can expect continued movement toward documented, auditable model development. Looking ahead, by 2050, discovery teams winning federal funds will need well-documented, auditable data pipelines that cover lineage, fit-for-purpose AI model validation, and output monitoring that is aligned with FDA and NIST expectations, with "digital twin" approaches. Regardless of shifting postures from the Executive Branch, the US is likely to maintain a lead in AI in the coming decades, especially as AI models gain credibility and federal regulatory governance matures. Even if the overall US AI policy shifts to less focus on governance and more toward rapid innovation, agencies like FDA, NIH, and ARPA-H still have missions that prioritise evidentiary reliability and patient safety. Likewise, "Digital twin" style approaches such as mechanistic disease modelling and virtual populations will become more valuable when teams show credibility and compliance with US data governance policies and NIST, NIH, and FDA expectations.

Layer 2: The Validation Engine (The Tools)

Currently, the US leads in laboratory automation adoption, with North America holding the largest market share and automated clinical lab systems comprising about 61.5% of the 2024 market, reflecting pharma's drive for throughput and accuracy.[7] Growth in laboratory automated tools and hardware will likely continue in the coming decades, especially as COVID-19 has shaped policy prospectives to ensure supply-chain rigidity in biotech and pharmaceutical sectors.[8] As a result, by 2034, US single-use bioprocessing market size is likely to increase from about $11.1 billion to $39.24 billion, driven by the rise of single-use bioreactors, growing demand for biopharmaceuticals, and the rising trend of outsourcing research and manufacturing to contract research and manufacturing organisations, and automation.[9]

That said, a strategic moat for the US Tools layer may be shifting toward the generation of high-fidelity, biologically relevant datasets using these tools to improve the safety and efficacy testing essential for this layer. This transition is being validated at the highest regulatory levels. FDA Commissioner Marty Makary, M.D., M.P.H. said: "We are committed to modernising our regulatory processes to lower costs, shorten timelines, and increase our confidence in the safety and efficacy of pharmaceuticals." […] "Advancements in drug safety testing have given us better predictive insights and allowed us to radically reduce or eliminate animal testing — it's critical that we continue to advance in this field."

A primary driver of this shift is the ARPA-H CATALYST programme, a federal initiative designed to fast-track safer medicines from the lab to patients. Companies such as Revalia Bio, a key recipient of this government contract, are leading the effort to build advanced AI-driven models trained on Human Data Trials – living systems derived from donated human organs, organ-on-chip platforms, and multimodal datasets. The contract specifically backs a human-first approach to drug safety and efficacy, reducing reliance on legacy animal testing and accelerating the delivery of safer therapies to patients. By generating trial-quality insights from functional human systems before traditional clinical stages, these platforms establish a sovereign domestic Validation Engine that ensures the Code layer (Layer 1) is refined with maximum human relevance before reaching the factory floor. This represents a "smart move" toward capital efficiency, cutting costly late-stage failures and securing the US bio-industrial stack.

Another company that shares this mission of democratisation and is enabling the true strength of the US Validation Engine is Alloy Therapeutics. Alloy is operationalising this vision by providing the shared "plumbing" of drug discovery,

offering non-exclusive, affordable access to foundational transgenic platforms and discovery toolkits that were previously gated by high costs.

Companies such as Revalia and Alloy represent a new "shared utility" model for the bio-industrial stack. Their shared mission to build a tech stack that "brings others to the table" ensures that the US Validation Engine is not a collection of silos, but a unified national strategic asset that accelerates the entire pipeline from design to patient. By providing this "shared utility" model, Alloy and Revalia are setting a precedent for building a foundational infrastructure for the "Regulatory Gate" of next-generation therapies. This model is a good example of a move away from "black box" proprietary silos and toward standardised, repeatable platforms.

Layer 3: The Execution Engine (The Factory)

In response to COVID-19 era shortages exposing supply-chain fragility, recent successive executive orders, EO 14017, EO 14081, and EO 14336, focus on critical API stockpiles and domestic bioproduction.[10] The BIOSECURE Act further acts as a forcing function in the "tools" and "factory" layers, creating a protected market for domestic biomanufacturing by making sovereign supply chains a prerequisite for US government contracts and future M&A activity. Additionally, EO 14293 and the new FDA PreCheck initiative aim to streamline reviews for US manufacturing facilities with an aim to help the US regain footing in the manufacturing of tooling for drug discovery scale-up operations.[11] This policy direction is likely to guide the US's strategic positioning and, if maintained, will help the US stay relevant in this Factory layer in the coming decades.[12]

Lessons from 2020 have highlighted the fact that managing future drug shortages includes investment in work and tooling to change pharmacy automation and electronic health records.[13] The US is also signalling tariff use to bolster domestic drug manufacturing while reducing regulatory friction via FDA PreCheck for domestic drug manufacturers and increasing generic pharmaceutical manufacturing capacity with increased surety of demand from the government to manufacture at full capacity.[14] However, despite these policy tailwinds aimed at boosting domestic production, the US will likely lag in drug production.

The US is already behind in the Execution Engine (Layer 3), with a shrinking domestic share of API volume of only about 12% and escalating drug shortages straining current manufacturers.[15] While these figures underscore a significant gap in domestic production, targeted regional initiatives are beginning to offer a blueprint for recovery.

A notable example is the Applied Research Institute (ARI) in Indiana and its Heartland BioWorks initiative. This consortium represents a strategic pivot toward infrastructure sovereignty by creating a formal "lab-to-launch" corridor. By establishing a dedicated innovation headquarters and a network of pilot-scale facilities, Heartland BioWorks ensures that startups are not forced to offshore their production due to a lack of domestic validation tools. This proactive model demonstrates that non-traditional regions, such as the American Midwest, with its industrial expertise and proximity to agricultural feedstocks, provides the physical "Execution Engine" required to bypass foreign dependencies. Policymaker and investor focus on linking research-heavy nodes (e.g., ARI) with low-cost, high-scale manufacturing environments in industrial corridors such as from Michigan-to-Texas – through targeted tax incentives for "middle-out" biomanufacturing and cross-state regulatory alignment – is a logical path toward the goal of a BITS that is resilient against coastal disruptions and geopolitical volatility. Anchoring these layers in the heartland may provide an opportunity to bridge the gap between coastal digital innovation and commercial-scale sovereign production.

Likewise, cuts to federal R&D funding, cancellations of BARDA mRNA contracts, and restrictive immigration could drive a scientific talent drain and reduce the scope of contracted drug-discovery work.[16] The majority of US grants targeted for termination were awarded by NSF and NIH and funded cutting-edge biomedical research across all three BITS layers.[17]

A more profound structural vulnerability of the Factory layer is the intellectual talent, which is the human capital that make scientific discovery and drug production possible. American Progress estimates that NIH and NSF funding cuts will result in a $10–16 billion annual decrease in US economic output.[18] Compounding this, a recent poll indicates that 75% of scientists are considering leaving the US following funding and R&D disruptions.[19] This potential exodus comes at a time when competitors like China are actively recruiting talent through programmes like the High-End Foreign Expert Recruitment Plan. If such a loss in human capital were to materialise, this could trigger a massive downturn in the biotech sector and a dramatic decline in upstream R&D and manufacturing as the US loses the talent necessary to scale laboratory discoveries into therapies for patients.

European Union — From Strong Science to Scaled Translation

The EU will likely retain strong science and upstream R&D dominance, but will experience slower translation to manufacturing than other regions.

Layer 1: The Design Engine (The Code)

The EU is a top-tier powerhouse in biotech with significant publication output that has historically outpaced research publications authored by the US and China, especially in advanced therapies for tissues, gene, and cell therapies.[20] However, the EU struggles to translate research into patient therapies compared with the US and China.[21] Although the EU accounts for 12% of global biotech market value *versus* the US at 60%, there are a limited number of top-ranked EU biotech research hubs scattered across Member States.[22] Hence, the EU's digital competitiveness lags particularly in Germany, Belgium, and Ireland, its key R&D manufacturing hubs.[23]

Contributing factors leading to Europe's persistent gap in translating strong biotech research into actual therapies stem from a combination of structural, regulatory, financial, and digital barriers.[24] Fragmented and often slow regulatory processes, limited flexibility around early access, and a lack of concentrated world-class innovation hubs compared with the US and China are also factors.[25] These regulatory frictions amplify the "no man's land" in early-stage financing, where companies between seed and Series A often cannot secure capital because investors perceive higher regulatory risk and weaker exit markets. Furthermore, the EU's diffuse, nationally siloed business environment also prevents companies from adopting globally scalable models, causing many to relocate or stagnate. Weak digital infrastructure and the constraints of GDPR create challenge to the build-up of EU-wide health data commons, limiting real-world evidence generation and the AI-driven discovery pipelines that fuel innovation in the US and China. Together, these factors create an ecosystem where scientific excellence exists, but translation into therapies lags behind global competitors. The EU's Pharmaceutical Strategy's lack of emphasis on supporting individual Member

States to modernise their digital infrastructure to support development of new medicines may constrain adoption of digitalisation and data-intensive drug-discovery goals.[26]

Despite current gaps in digitalisation, the EU is steering the trajectory of the region toward increased use of AI, digital collaboration, and secure sharing of health data via the Apply AI Strategy, Data Governance Act establishing Common European Data Spaces, and health data initiatives such as 1+ Million Genomes, COMPASS-AI, and the Genome of Europe.[27] Such initiatives should enable secure cross-border genomic data access and harmonised quality measures. In the coming decades, the EU's policy agenda should allow the EU to maintain academic prowess in pure R&D with robust data sets powering AI and digital modelling.

Layer 2: The Validation Engine (The Tools)

Recognising translation and time-to-market bottlenecks, the region is exploring solutions to gain footing in manufacturing. The EU Bioeconomy strategy and proposed EU Biotech Act, along with regulatory sandboxes and an EU Biotech Hub, are policy tools designed to simplify pathways for biotech companies to navigate regulatory framework to market and support scale-up operations.[28] The efforts are also intended to address complex regulatory friction at the Member State and EU level, such as permitting long approval timelines as compared with the US for certain biologics manufacturing operations.[29] If these initiatives prove fruitful they may be able to cut down on regulatory delays and complexity and allow more therapies and biotech hardware to be produced in EU manufacturing facilities.[30]

Layer 3: The Execution Engine (The Factory)

On the drug manufacturing front, the EU remains pivotal for branded APIs, as about 43% of branded APIs come from the EU.[31] However, the EU is still exposed to regional concentrated imports due to dependence on foreign generic APIs, with 45% coming from China.[32] Also, Member State drug price cost-containment policies curb manufacturers' ability to recoup high operating costs that have exacerbated supply shortages.[33] To address this, the European Commission's proposed Critical Medicines Act would prioritise resilience over price and streamline joint procurement, setting the course to increased procurement and demand for pharmaceutical ingredients while creating supply-chain resilience that would help EU drug manufacturers increase capacity.[34]

Overall, Europe's global share of biopharma R&D has declined relative to the US, underscoring the urgency of digitalisation, translational funding from pure R&D to drug manufacturing, and incentives. If these policy interventions are implemented and prove fruitful it could help the EU to reverse the decline and gain more footing in Layers 2 and 3 in 2050.

China — Coordinated Bioeconomy Scale-up

When addressing the competitive landscape of China and the West, it is important to understand the differing scholarly paradigms between the West and China that drive a strategic asymmetry, illustrated by the growth velocity in China of certain layers in BITS. To this, China is executing a state-led bioeconomy push, prioritising the Design Engine's velocity for the benefit of the state. The contrast between the Western focus on individual autonomy and informed consent with collectivist frameworks can and likely will impact speed of development. As such, it is a competitive variable not to be ignored or boiled down to a moral or ethical debate.

Layer 1: The Design Engine (The Code)

China's national strategy positions biotech as a pillar of economic and security policy, with the 14th Five-Year Plan targeting leadership in genomics, synthetic biology, biologics, and clinical technologies by 2035.[35] China's 14th Five-Year Plan prioritises reorganising national laboratory systems across AI and biopharma to boost its footing in pure scientific research and its standing across all three layers of the drug discovery R&D stack.[36]

At a time when the US is pulling R&D funding, limiting immigration, and as a majority of US scientists are reportedly considering moving abroad, a scientific talent drain and counter-migration of expertise could result in a zero-sum talent war critically reshaping the 2050 forecast of the BITS. China has consolidated elite talent programmes and established the High-End Foreign Expert Recruitment Plan to recruit and retain global expertise trained abroad in strategic science and technology to accelerate industrial innovation.[37] Notably, during the previous 13th Five-Year period, which ended in 2020, Chinese pharmaceutical companies grew their R&D investments by about 8%.[38] By 2024, roughly 26.7% of development-stage drugs involved Chinese R&D, and China accounted for 24% of the world's first-in-class pipeline, signalling rising discovery capacity.[39] This growth trajectory will likely continue for Chinese pharma R&D, bolstered by Chinese economic and policy objectives, making China a dominant player in layer one.

Layer 2: The Validation Engine (The Tools)

In the Tools layer, the Asia-Pacific region is projected to be the fastest-growing market for single-use bioprocessing, advanced robotics, and laboratory automation, and may outpace the US to become a dominant player. In 2024, North America dominated the single-use bioprocessing market with a 42% revenue share.[40] However, Chinese biomanufacturers may disrupt this trend, benefitting from accelerated adoption of AI with greater efficiency and less capital expenditure compared to other geographic competitors in drug discovery.[41]

Layer 3: The Execution Engine (The Factory)

In 2024, China was a leader in the first-in-class drug pipeline, trailing only the US.[42] However, for APIs, Chinese manufacturers have a greater role in the initial unregulated production steps, while their role in final active ingredients varies widely across drugs.[43] Although China's role in final API production varies by product, China is still reliant on foreign early-stage key starting materials (KSMs) and intermediates to produce APIs, which reinforces upstream dependence across global supply chains.[44] There are also persistent concerns over IP and quality that remain an international friction point even as the Chinese sector expands across Layer 3.[45] That said, the "Made in China 2025" industrial policy has helped transform China from a low-cost manufacturing hub to a titan of high-tech global innovation in biomedicine and AI.[46] The Made in China 2025 initiative had a goal of transforming China into a self-sufficient leader in drug discovery through state support, subsidies and IP acquisition to become a manufacturing superpower by 2050. This, along with large domestic demand for pharmaceuticals (due to a high aging population), government subsidies, state procurement, direct leverage over stockpiles, and increased major multinationals investment from manufacturers like AstraZeneca, will fuel expansive manufacturing footprints for decades to come.[47]

India — From Generics Scale to Discovery Enablement

India is a generics manufacturing powerhouse climbing the BITS to become a contender in all three layers of drug discovery by 2050.

Layer 1: The Design Engine (The Code):

India is actively bolstering its position in rapid drug discovery using AI technologies and leveraging academic, industry, and international partnerships.[48] In 2022, India's bioeconomy was estimated to be valued at $137.2 billion and it is expected to reach $300 billion in the next five years.[49] India is also home to more than 800 biotechnology companies and its scientific publication volume is steadily increasing.[50] In 2024, India partnered with the US to foster rapid drug discovery under Critical and Emerging Technology (iCET) and the Indo-US Science and Technology Forum to accelerate AI, quantum computing, and advanced wireless-enabled discoveries that will benefit pharmaceutical innovation in upstream R&D.[51] Additionally, India's investment in improved infrastructure is projected to enable bioinformatics and nanotechnology with faster go-to-market capability, growing its pharma market to roughly $130 billion by 2030.[52] Along these lines, the Biotechnology for Economy, Environment & Employment (BioE3) initiative seeks to make India a global biomanufacturing hub by 2050 and a leader in sustainably fast-tracked R&D.[53] The BioE3 initiative will establish Bio-AI hubs, national data-governance protocols, and a network of biofoundries to standardise scale-up and automation and will channel funding across academia, startups, and industry.[54] Also, Indian startups are expected to lead growth in drug discovery and delivery technologies.[55] Although early clinical development often migrates offshore due to clinical-trial ecosystem constraints, BioE3 and increased bioeconomic growth could challenge this practice, encouraging rapid R&D and clinical trials to take place in India.[56]

Layer 2: The Validation Engine (The Tools)

On the Tools side, the BioE3 initiative signals rapid mid-stream capacity building even as the US remains revenue-dominant globally.[57] India's single-use bioprocessing market is projected to see a compound annual growth rate of about 18.4%, reaching $3.63 billion in revenue by 2030.[58] The BioE3 and Biotechnology Research Innovation and Entrepreneurship Development (Bio-RIDE) initiatives will both establish biofoundries that will likely be a boon to drug-discovery firms, startups, and academia by providing access to biotech tooling, hardware, standardised processes, automation, and integrated facilities for early scaling up of proof-of-concept drug developments.[59] Each of these government-backed bio-tooling investments will likely increase India's standing in Layer 2 by 2050.

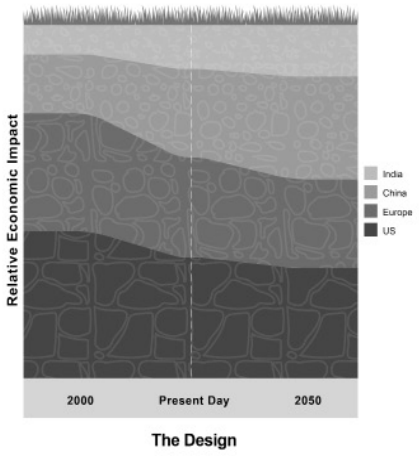
Layer 3: The Execution Engine (The Factory)

In the Factory layer, India supplies an estimated 50% of US generic pharmaceuticals, which make up about 90% of US prescription volume, cementing India's role in global access.[60] However, India relies on China for roughly 70% of its API imports and many KSMs.[61] These are structural vulnerabilities BioE3 may mitigate over time with government subsidies, production-linked incentive schemes, and increased support for biomanufacturing to promote critical API production by Indian pharma companies.[62] Overall, BioE3 and Bio-RIDE efforts are likely to grow India's market share as a global API provider and make it an attractive alternative in the Chinese-dominated API market.

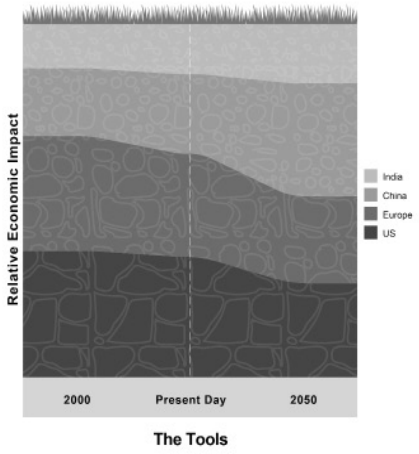
The Ground is Shifting Beneath Our Feet

As with chapter 1, we quantified the strength of a country in each layer based on the output and foothold the country had on the layer. Using the trends discussed in chapter 1 and the forward-looking outlook of each layer discussed in this chapter, we provided a quantitative estimate for how the stack may look in 2050, as depicted in the figure below.

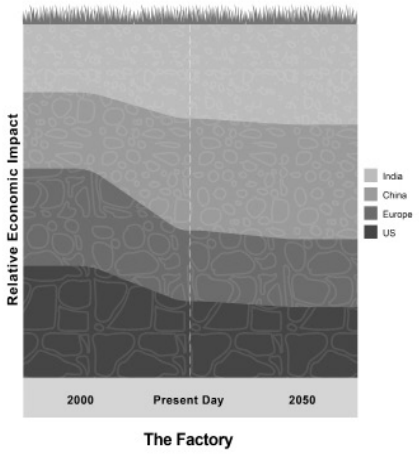
PROJECTED SHIFTS IN GLOBAL BIO-INDUSTRIAL DOMINANCE BY STACK LAYER (2000-2050)



The Design



The Tools



The Factory

As is readily apparent, the BITS world continues to change. The ground beneath our feet, once stable and predictable, is shifting and will continue to shift given current trends and momentum. The future of drug discovery will increasingly rely on harvesting shareable data and validated AI models; automated, single-use, and digital lab infrastructure; and streamlined regulatory frameworks that increase manufacturing and resilient supply chains, prioritising surety of demand. The EU will likely lead in AI-governance frameworks and will continue to progress with digitalisation and AI across its biotech hubs. The US, with the EU following suit, will likely maintain a dominant position in digital tools and AI for rapid drug discovery, but both regions face structural constraints in scaling domestic biomanufacturing compared to the coordinated industrial policies observed in the Asia-Pacific region. Conversely, China's current trajectory positions it as a global powerhouse capable of scaling end-to-end capabilities across the BITS through a coordinated industrial policy, while India is successfully leveraging biofoundries and global partnerships to transition into more of a contender across all three layers of the stack.

There are many nations and territories involved in our bio-industrial future. The world must be aware of this ongoing transition and rethink ways to navigate this transition. Take the West for example; the West must move beyond digital discovery and redirect its focus to the physical and procedural layers of the bio-industrial stack. This requires a multifaceted approach to domestic resilience that extends beyond geographic diversification.

In the West, the US is a good example to apply this multifaceted approach. While the American Midwest provides a critical engine for large-scale bioproduction – leveraging its industrial expertise and proximity to feedstocks – the stack should be secured as a unified industrial system as a prerequisite for sovereignty in the century of biology. The future of drug discovery requires moving beyond digital discovery to reclaim the physical and procedural layers of the bio-industrial system through five strategic pillars:

1. National Data Commons: The US should establish unified, auditable pipelines for AI validation to fix the "digital only" leadership paradox and maintain an edge in the Design Engine.
2. The Benchmarking Mandate: The US should look to define the digital standards and weights and measures for biological AI, ensuring its authority and influence with the "Regulatory Gate" for next-generation therapies.
3. Infrastructure Accessibility: The US must democratise access to high-end automation and biofoundries so that startups are not forced to offshore their production due to a lack of domestic validation tools.
4. Incentivising Sovereign Capital: The US must utilise demand-side levers – such as advance market commitments and strategic stockpiling – to make domestic manufacturing a commercial reality.
5. Addressing the Human Capital Crisis: The US must frame talent retention as a prerequisite for sovereignty. With 75% of scientists considering leaving the US, the US Design Engine faces a terminal risk that no amount of funding can fix without the people to lead it.

This is a world issue, not just a US issue. Each nation or region invested in the global bio-industrial system should understand its place now and where it desires to be in the 2050 BITS world. Ultimately, the stakes of the BITS transcend market dominance. The stakes concern the fundamental ability of a state to secure the general-purpose technology that will define the next century of materials and health. History suggests we are at a crossroads similar to the mid-century space race or the mapping of the human genome. The coming decade will reveal a stark divide between nations that viewed biotechnology as a collection of scientific breakthroughs and those that recognised it as a unified, sovereign industrial system. To secure the stack is no longer merely an act of optimisation; it is a prerequisite for sovereignty in the century of biology.

Endnotes

1 *Bridge to Artificial Intelligence (Bridge2AI)*, https://commonfund.nih.gov/bridge2ai; *ARPA-H Launches Program to Help AI-enabled Medical Tools Maintain Peak Performance* (Aug. 29, 2024), https://arpa-h.gov/news-and-events/arpa-h-launches-program-help-ai-enabled-medical-tools-maintain-peak-performance#:~:text=August%2029%2C%202024-,ARPA%2DH%20launches%20program%20to%20help%20AI%2Denabled%20medical%20tools,medical%20imaging%20and%20diagnostic%20tools; ARPA-H Sees Promise in AI with Newest Funding Projects (Nov. 26, 2024), https://govciomedia.com/arpa-h-sees-promise-in-ai-with-newest-funding-projects/#:~:text=UPGRADE%20gives%20health%20care%20facilities,their%20ideas%20to%20the%20agency.%E2%80%9D

2 *Data Management & Sharing Policy Overview*, https://grants.nih.gov/policy-and-compliance/policy-topics/sharing-policies/dms/policy-overview

3 *Model-Informed Drug Development Paired Meeting Program*, https://www.fda.gov/drugs/development-resources/model-informed-drug-development-paired-meeting-program

4 *Modeling & Simulation at FDA*, https://www.fda.gov/science-research/about-science-research-fda/modeling-simulation-fda; *275 Million New Genetic Variants Identified in NIH Precision Medicine Data*, (Feb. 19, 2024), https://allofus.nih.gov/article/announcement-275-million-new-genetic-variants-identified-nih-precision-medicine-data

5 *Modeling & Simulation at FDA*, https://www.fda.gov/science-research/about-science-research-fda/modeling-simulation-fda; *275 Million New Genetic Variants Identified in NIH Precision Medicine Data*, (Feb. 19, 2024), https://allofus.nih.gov/article/announcement-275-million-new-genetic-variants-identified-nih-precision-medicine-data

6 Required Security and Operational Standards for NIH Controlled-Access Data Repositories (Sept. 24, 2025), https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-159.html; Executive Order 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (Feb. 28, 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related; Executive Order 14110 – "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", Oct. 30, 2023 (Revoked Biden Administration EO); Executive Order 14179 – "Removing Barriers to American Leadership in Artificial Intelligence", (Signed: Jan. 23, 2025, Trump Administration).

7 *Laboratory Automation Market Size, Share, Trends and Forecast by Type, Equipment and Software Type, End-User, and Region, 2025–2033*, (last visited Jan. 4, 2026), https://www.imarcgroup.com/laboratory-automation-market ("Automated clinical laboratory systems lead the market with around 61.5% of market share in 2024. These systems are used in clinical diagnostic laboratories, healthcare facilities, and medical research centers. It includes a range of equipment and software solutions, from automated analyzers and sample processors to diagnostic instruments and laboratory information management systems (LIMS).").

8 ASHP, *Drug Shortages Statistics* (last visited Jan. 4, 2026), https://www.ashp.org/drug-shortages/shortage-resources/drug-shortages-statistics?loginreturnUrl=SSOCheckOnly; JAMA, Differences in Drug

Shortages in the US and Canada, https://jamanetwork.com/journals/jama/fullarticle/2825535

9 Nova Advisor, *U.S. Single-use Bioprocessing Market Size, Share, Growth, Report 2025 to 2034* (last visited Jan. 5, 2026), https://www.novaoneadvisor.com/report/us-single-use-bioprocessing-market

10 Exec. Order No. 14017; Exec. Order No. 14081; Exec. Order No.14336 (Directs the Office of the Assistant Secretary for Preparedness and Response (ASPR), within the Department of Health and Human Services, to develop a list of approximately 26 critical drugs vital to national health and security, and ready the SAPIR repository to receive and maintain the Active Pharmaceutical Ingredients (APIs) used to make these critical drugs. The Order charges the ASPR with obtaining a six-month supply of these critical APIs, with a preference for obtaining domestically-manufactured APIs if possible, and placing them in the SAPIR).

11 *FDA Announces New FDA PreCheck Program to Boost U.S. Drug Manufacturing* (Aug. 7, 2025), https://www.fda.gov/news-events/press-announcements/fda-announces-new-fda-precheck-program-boost-us-drug-manufacturing; Exec. Order No.14293.

12 *FDA Announces New FDA PreCheck Program to Boost U.S. Drug Manufacturing* (Aug. 7, 2025), https://www.fda.gov/news-events/press-announcements/fda-announces-new-fda-precheck-program-boost-us-drug-manufacturing; Exec. Order No. 14293.

13 ASHP, *Drug Shortages Statistics* (last visited Jan. 4, 2026), https://www.ashp.org/drug-shortages/shortage-resources/drug-shortages-statistics?loginreturnUrl=SSOCheckOnly

14 Johns Hopkins, *4 Ways the U.S. Can Strengthen its Pharmaceutical Supply Chain*, (Nov. 10, 2025), https://washingtondc.jhu.edu/news/4-ways-to-strengthen-the-drug-supply-chain ; Mordor Intelligence, US Tariffs 2025: *How They're Reshaping Global Pharma, Not Just Redirecting Trade* (last visited Jan. 4, 2026), https://www.mordorintelligence.com/signal/insights/us-tariffs-2025-reshaping-global-pharma

15 Vimala Raghavendran, *Over Half of the Active Pharmaceutical Ingredients (API) for Prescription Medicines in the U.S. Come From India and the European Union* (Apr. 17, 2025), https://qualitymatters.usp.org/index.php/over-half-active-pharmaceutical-ingredients-api-prescription-medicines-us-come-india-and-european

16 Mapping Federal Funding Cuts to U.S. Colleges and Universities (July 23, 2025), https://www.americanprogress.org/article/mapping-federal-funding-cuts-to-us-colleges-and-universities ("The situation has grown so dire that 75 percent of scientists now say they are considering leaving their positions in the United States for Europe or Canada. Countries have already started recruiting U.S. researchers looking to leave, with France even setting up a 'Safe Place For Science' program, which promotes 'a safe and stimulating environment for scientists wishing to pursue their research in complete freedom'."); *HHS Winds Down mRNA Vaccine Development Under BARDA* (Aug. 5, 2025), https://www.hhs.gov/press-room/hhs-winds-down-mrna-development-under-barda.html#:~:text=HHS%20has%20also%20instructed%20its,virus%20vaccines%20and%20novel%20platforms.&text=Note:%20All%20HHS%20press%20releases,up%20for%20HHS%20Email%20Updates;%20; https://www.dw.com/en/us-cancels-mrna-vaccine-contracts-worth-500-million/a-73542725#:~:text=Midhat%20Fatimah%20with%20AFP%2C%20AP,and%20flu%2C%22%20he%20added

17 Greta Bedekovics and Will Ragland, *Mapping Federal Funding Cuts to U.S. Colleges and Universities* (July 23, 2025), https://www.americanprogress.org/article/mapping-federal-funding-cuts-to-us-colleges-and-universities

18 Greta Bedekovics and Will Ragland, *Mapping Federal Funding Cuts to U.S. Colleges and Universities* (July 23, 2025), https://www.americanprogress.org/article/mapping-federal-funding-cuts-to-us-colleges-and-universities

19 Greta Bedekovics and Will Ragland, *Mapping Federal Funding Cuts to U.S. Colleges and Universities* (July 23, 2025), https://www.americanprogress.org/article/mapping-federal-funding-cuts-to-us-colleges-and-universities

20 *Europe's Share of Global Medicines R&D Shrinks by a Quarter in 20 years – As Sector's Declining Trends Continue* (Nov. 7, 2022), https://www.efpia.eu/news-events/the-efpia-view/efpia-news/europe-s-share-of-global-medicines-rd-shrinks-by-a-quarter-in-20-years-as-sector-s-declining-trends-continue/#:~:text=For%20Europe%20to%20start%20competing,research%20into%20therapies%20for%20patients ("Advanced Therapies Medicinal Products (ATMPs) – tissue, gene and cell therapies – used to prevent, treat and cure rare conditions including some cancers, where the US and China dominate.").

21 *Europe's Share of Global Medicines R&D Shrinks by a Quarter in 20 years – As Sector's Declining Trends Continue* (Nov. 7, 2022).

22 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* (Mar. 20, 2024), https://research-and-innovation.ec.europa.eu/document/download/47554adc-dffc-411b-8cd6-b52417514cb3_en; *Europe's Share of Global Medicines R&D Shrinks by a Quarter in 20 years – As Sector's Declining Trends Continue* (Nov. 7, 2022), https://www.efpia.eu/news-events/the-efpia-view/efpia-news/europe-s-share-of-global-medicines-rd-shrinks-by-a-quarter-in-20-years-as-sector-s-declining-trends-continue/#:~:text=For%20Europe%20to%20start%20competing,research%20into%20therapies%20for%20patients

23 *Europe's Share of Global Medicines R&D Shrinks by a Quarter in 20 years – As Sector's Declining Trends Continue* (Nov. 7, 2022), https://www.efpia.eu/news-events/the-efpia-view/efpia-news/europe-s-share-of-global-medicines-rd-shrinks-by-a-quarter-in-20-years-as-sector-s-declining-trends-continue/#:~:text=For%20Europe%20to%20start%20competing,research%20into%20therapies%20for%20patients

24 *Europe's Share of Global Medicines R&D Shrinks by a Quarter in 20 years – As Sector's Declining Trends Continue* (Nov. 7, 2022), https://www.efpia.eu/news-events/the-efpia-view/efpia-news/europe-s-share-of-global-medicines-rd-shrinks-by-a-quarter-in-20-years-as-sector-s-declining-trends-continue/#:~:text=For%20Europe%20to%20start%20competing,research%20into%20therapies%20for%20patients

25 *Europe's Share of Global Medicines R&D Shrinks by a Quarter in 20 years – As Sector's Declining Trends Continue* (Nov. 7, 2022), https://www.efpia.eu/news-events/the-efpia-view/efpia-news/europe-s-share-of-global-medicines-rd-shrinks-by-a-quarter-in-20-years-as-sector-s-declining-trends-continue/#:~:text=For%20Europe%20to%20start%20competing,research%20into%20therapies%20for%20patients

26 *Europe's Share of Global Medicines R&D Shrinks by a Quarter in 20 years – As Sector's Declining Trends Continue* (Nov. 7, 2022), https://www.efpia.eu/news-events/the-efpia-view/efpia-news/europe-s-share-of-global-medicines-rd-shrinks-by-a-quarter-in-20-years-as-sector-s-declining-trends-continue/#:~:text=For%20Europe%20to%20start%20competing,research%20into%20therapies%20for%20patients

27 European Data Governance Act, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act; *Apply AI Strategy* (Dec. 17, 2025), https://digital-strategy.ec.europa.eu/en/policies/apply-ai; *Commission Launches Flagship Initiative to Increase Use of AI in Healthcare*, (Oct. 21, 2025), https://digital-strategy.ec.europa.eu/en/news/commission-launches-flagship-initiative-increase-use-ai-healthcare; *European '1+ Million Genomes' Initiative*, https://digital-strategy.ec.europa.eu/en/policies/1-million-genomes

28 *Commission Takes Action to Boost Biotechnology and Biomanufacturing in the EU* (Mar. 19, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1570

29 *Commission Takes Action to Boost Biotechnology and Biomanufacturing in the EU* (Mar. 19, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1570

30 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* (Mar. 3, 2024), https://research-and-innovation.ec.europa.eu/document/download/47554adc-dffc-411b-8cd6-b52417514cb3_en

31 Vimala Raghavendran, *Over half of the active pharmaceutical ingredients (API) for prescription medicines in the U.S. come from India and the European Union* (Apr. 17, 2025), https://qualitymatters.usp.org/index.php/over-half-active-pharmaceutical-ingredients-api-prescription-medicines-us-come-india-and-european

32 *New Rules for Critical Medicines in the EU*, https://www.consilium.europa.eu/en/policies/critical-medicines-act

33 Vimala Raghavendran, *Over Half of the Active Pharmaceutical Ingredients (API) for Prescription Medicines in the U.S. Come From India and the European Union* (Apr. 17, 2025), https://qualitymatters.usp.org/index.php/over-half-active-pharmaceutical-ingredients-api-prescription-medicines-us-come-india-and-european

34 *New Rules for Critical Medicines in the EU* (last visited Jan. 5, 2025), https://www.consilium.europa.eu/en/policies/critical-medicines-act

35 China Daily, *Bioeconomy Prominent on Growth Agenda* (May 11, 2022), https://english.www.gov.cn/policies/policywatch/202205/11/content_WS627b169ec6d02e533532a879.html

36 Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035 (last visited Jan. 5, 2026), https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf; International Talent Programs in the Changing Global Environment (2024); National Academies of Sciences, Engineering, and Medicine, *International Talent Programs in the Changing Global Environment.* The National Academies Press (2024).

37 Emily Weinstein, *Chinese Talent Program Tracker* (last visited Jan. 5, 2026), https://chinatalenttracker.cset.tech

38 China Daily, *Bioeconomy Prominent on Growth Agenda* (May 11, 2022), https://english.www.gov.cn/policies/policywatch/202205/11/content_WS627b169ec6d02e533532a879.html

39 Millie Nelson, *China Biopharma Boom Aided by Returning Talent, BioXconomy* (Apr. 10, 2025).

40 BioSpace, *Single-use Bioprocessing Market Size to Surpass USD 151.48 Bn by 2034* (Oct. 30, 2025), https://www.biospace.com/press-releases/single-use-bioprocessing-market-size-to-surpass-usd-151-48-bn-by-2034

41 Ethan G., *China Biotech: Doing More with Less Capital, Deep Intelligence Pharma* (Dec. 11, 2025), https://www.dip-ai.com/use-cases/en/china-biotech-doing-more-with-less-capital

42 Niels Graham, *Pharmaceuticals are China's Next Trade Weapon*, (Nov. 7, 2025), https://www.atlanticcouncil.org/blogs/econographics/sinographs/pharmaceuticals-are-chinas-next-trade-weapon/#:~:text=The%20risk%20extends%20to%20research,%2Dclass%20(FIC)%20drugs

43 Marta E. Wosińska and Yihan Shi, *US drug supply chain exposure to China* (last visited Jan. 6, 2025), https://www.brookings.edu/articles/us-drug-supply-chain-exposure-to-china/#:~:text=One%20estimate%20shows%20current%20U.S.,the%20global%20supply%20of%20API

44 *Over Half of the Active Pharmaceutical Ingredients (API) for Prescription Medicines in the U.S. Come From India and the European Union* (Apr. 17, 2025), https://qualitymatters.usp.org/index.php/over-half-active-pharmaceutical-ingredients-api-prescription-medicines-us-come-india-and-european; Marta E. Wosińska and Yihan Shi, *US Drug Supply Chain Exposure to China* (last visited Jan. 6, 2025), https://www.brookings.edu/articles/us-drug-supply-chain-exposure-to-china/#:~:text=One%20estimate%20shows%20current%20U.S.,the%20global%20supply%20of%20API

45 *Pharmacy of the World: China's Quest to be the No. 1 Drugmaker* (Dec. 23, 2021), https://asia.nikkei.com/static/vdata/infographics/chinavaccine-2

46 James McBride and Andrew Chatzky, *Is 'Made in China 2025' a Threat to Global Trade?*, (May 13, 2019), https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade#:~:text=So%2C%20when%20we%20see%20a,know%2C%20discussed%20as%20revenge%20tourism

47 Simon Goodley, *AstraZeneca to Invest $2.5BN in Drugs Research and Manufacturing in Beijing* (Mar. 12, 2025), https://www.theguardian.com/business/2025/mar/21/astrazeneca-to-invest-in-drugs-research-and-manfacturing-in-beijing

48 BioSpectrum, *Global Bio-India 2023 Sets New Target of $200 B for Bioeconomy in 2025* (Dec. 4, 2025), https://www.biospectrumindia.com/news/96/23898/global-bio-india-2023-sets-new-target-of-200-b-for-bioeconomy-in-2025.html ("[Biotechnology Industry Research Assistance Council] BIRAC has signed MoU with Germany-based Miltenyi Biotec for cell and gene therapy research; with Japan-based Takeda Pharmaceutical to extend advisory and mentoring support to innovators and entrepreneurs while assisting them from ideation to market deployment of new-age healthcare solutions; with Foreign, Commonwealth and Development Office (FCDO) in the UK; and with India Health Fund.").

49 Jitendra Kumar, *US–India Collaborative Innovations for Rapid Drug Discovery* (June 12, 2024), https://www.bioprocessintl.com/bioregions/us-india-collaborative-innovations-for-rapid-drug-discovery

50 Jitendra Kumar, *US–India Collaborative Innovations for Rapid Drug Discovery* (June 12, 2024), https://www.bioprocessintl.com/bioregions/us-india-collaborative-innovations-for-rapid-drug-discovery; National Science Foundation, Publications Output: U.S. Trends and International Comparisons (Dec. 2023), https://ncses.nsf.gov/pubs/nsb202333/publication-output-by-region-country-or-economy-and-by-scientific-field#:~:text=Table_content:%20header:%20%7C%20Rank%20%7C%20Region%2C%20country%2C,or%20economy:%20Italy%20%7C%202022:%2090%2C586%20%7C

51 Jitendra Kumar, *US–India Collaborative Innovations for Rapid Drug Discovery* (June 12, 2024), https://www.bioprocessintl.com/bioregions/us-india-collaborative-innovations-for-rapid-drug-discovery

52 Jitendra Kumar, *US–India Collaborative Innovations for Rapid Drug Discovery* (June 12, 2024), https://www.bioprocessintl.com/bioregions/us-india-collaborative-innovations-for-rapid-drug-discovery

53 Ministry of Science & Technology, Govt. of India, Dept. of Biotechnology, *Biotechnology for Economy, Environment & Employment*, https://www.indiascienceandtechnology.gov.in/sites/default/files/file-uploads/sciencetechnologypolicies/1746189922_BioE3%20Policy%20Brohcure_compressed.pdf

54 Ministry of Science & Technology, Govt. of India, Dept. of Biotechnology, *Biotechnology for Economy, Environment & Employment*, https://www.indiascienceandtechnology.gov.in/sites/default/files/file-uploads/sciencetechnologypolicies/1746189922_BioE3%20Policy%20Brohcure_compressed.pdf

55 Jitendra Kumar, *US–India Collaborative Innovations for Rapid Drug Discovery* (June 12, 2024), https://www.bioprocessintl.com/bioregions/us-india-collaborative-innovations-for-rapid-drug-discovery

56 Jerin Jose Cherian, Arui Poomali, Aparna Mukherjee, *et al.*, *Increasing Early Phase Clinical Trials Capacity in India* (July 1, 2025),

https://pmc.ncbi.nlm.nih.gov/articles/PMC12216851 ("It is also worth noting that India has specifically shied away from early phase clinical trials. Indian innovators often pursue their early clinical development overseas, and international pharmaceutical giants are reluctant to engage with collaborators from India for early phase clinical development.").

57 Grand View Horizon, *India Single-use Bioprocessing Market Size & Outlook*, https://www.grandviewresearch.com/horizon/outlook/single-use-bioprocessing-market/india

58 Grand View Horizon, *India Single-use Bioprocessing Market Size & Outlook*, https://www.grandviewresearch.com/horizon/outlook/single-use-bioprocessing-market/india

59 Ministry of Science & Technology, Govt. of India, Dept. of Biotechnology, *Biotechnology for Economy, Environment & Employment, Implementation Plan for Biomanufacturing and Biofoundry Component of the BioRIDE scheme of Department of Biotechnology for 'Fostering High-Performance Biomanufacturing'*, https://bmi.dbtindia.gov.in/pdf/Implementation.pdf

60 Mohd Shakaeb Osman, *US Tariffs 2025: How They're Reshaping Global Pharma, Not Just Redirecting Trade* (Aug. 6, 2025), https://www.mordorintelligence.com/signal/insights/us-tariffs-2025-reshaping-global-pharma; Vimala Raghavendran, *Over half of the active pharmaceutical ingredients (API) for prescription medicines in the U.S. Come From India and the European Union* (Apr. 17, 2025), https://qualitymatters.usp.org/index.php/over-half-active-pharmaceutical-ingredients-api-prescription-medicines-us-come-india-and-european

61 *The Great Medicines Migration* (Apr. 5, 2022), https://asia.nikkei.com/static/vdata/infographics/chinavaccine-3

62 Chemox, *How India Became a Global Hub for APIs* (June 12, 2025), https://chemoxpharma.com/how-india-became-a-global-hub-for-apis



Dr. Milad Alucozai, recognised by *Business Insider* as "one of the top 100 early-stage investors", is a neuroscientist, founder, and active investor dedicated to translating exceptional science and technology into scalable commercial ventures.
He currently serves as a Co-founder and General Partner at Pamir Ventures, an early-stage venture fund that invests in technical pioneers developing B2B companies utilising AI in antiquated industries. He is also a co-founder of Revalia Bio, a leading AI company enabling "Human Data Trials" to accelerate drug development with real human data before the first clinical trial begins.
Throughout his operating and investing career, Milad has played a crucial role in helping founders secure hundreds of millions in capital and facilitating billions in startup-pharma partnerships.

Pamir Ventures
One Embarcadero Center, Suite 1050
San Francisco, California 94111
USA

Tel: +1 617 432 7732
Email: milad@pamir.vc
LinkedIn: www.linkedin.com/in/miladalucozai



Jason Novak advises companies of all sizes on legal issues arising from emerging technologies, with a particular emphasis on AI/ML. His practice centres on "convergence" technologies – such as digital health, precision medicine, and alternative protein – that sit at the intersection of multiple industries. Drawing on cross-disciplinary training and deep in-house experience, Jason helps organisations navigate the complex legal and strategic challenges that come with blending traditionally distinct sectors.
Jason's work focuses on IP and data rights strategy, which are of particular importance and complexity in "convergence" fields. With data rights, data must be treated as an offensive asset. To that, Jason supports clients on transactions, protection, and strategic long-term planning. Jason's IP experience includes patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in- and out-licensing, freedom-to-operate, due diligence, IP training, risk management, and dispute resolution.

Norton Rose Fulbright
One Embarcadero Center, Suite 1050
San Francisco, California 94111
USA

Tel: +1 628 231 6811
Email: jason.novak@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/jason-novak-002102b



Dr. Nathanael Green is an associate in Norton Rose Fulbright's Houston office. His practice focuses on developing IP portfolios mainly for universities and life science companies. Nate counsels clients on portfolio strategies, which include preparing and prosecuting patent applications and developing patent landscape opinions. Nate has experience with technologies across the life science space, including cellular therapies, gene therapies, small molecules, diagnostic assays, medical devices, organic chemistry and drug screening. Nate also conducts due diligence review on IP portfolios for potential investment and acquisition.
Nate received his J.D. from University of Houston Law Center. Prior to a career in law, Nate performed biomedical research focusing on the intersection of metabolism and RNA transcription regulation in kidney cancer at Baylor College of Medicine, where he received a Ph.D. in pharmacology.

Norton Rose Fulbright
1550 Lamar Street, Suite 2000
Houston, Texas 77010
USA

Tel: +1 713 651 5422
Email: nathanael.green@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/nathanael-green-phd-05433757



Ebony Christian received her J.D. at Georgetown University Law Center and focuses her practice on IP and patent law. Prior to joining Norton Rose Fulbright, she worked as a law clerk at the Office of General Counsel for the Defense Advanced Research Projects Agency, and has extensive engineering experience in aerospace, defence, and oil and gas industries.

Norton Rose Fulbright
98 San Jacinto Blvd STE 1100
Austin, Texas 78701
USA

Tel: +1 512 536 3019
Email: ebony.christian@nortonrosefulbright.com
URL: www.nortonrosefulbright.com/en-us/people/1017960

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full-business law service. We have more than 3,500 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.
Recognised for our industry focus, we are strong across all the key industry sectors: financial institutions; energy, infrastructure and resources; transport; technology; life sciences and healthcare; and consumer markets. Through our global risk-advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.
www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Evolution of Digital Health Reimbursement in the United States, Germany, the United Kingdom and France


Stephen A. Hull

Tarek Hamdan

Kirstin Osthoff

Dr. Eric Lam

Avania B.V.

I. Introduction

While the meaning of "digital health" can be exceedingly broad, national reimbursement systems have evolved to address two initial groupings for technologies subject to the US Food and Drug Administration (FDA) regulation in the US or CE mark in Europe: technologies are considered either software as a medical device (SaMD) or software in a medical device. However, within these broad regulatory categories, there are a vast range of different applications and the ways in which they fit into benefit categories and coding systems is far from uniform.

Despite very significant and growing investment, innovators continually challenge, and are often resisted by, conventional pathways for coding and reimbursement across major global markets. This chapter provides a high-level overview of the coding and payment pathways in the US Medicare programme, as well as the national, single-payer systems of Germany, the United Kingdom and France.

II. Evolution of Digital Coding and Coverage in the US Medicare Programme

In the eight years since the FDA cleared its first Prescription Digital Therapeutic (PDT), well over two dozen products have since been cleared, and the US Medicare programme continues to lack a benefit category or specific physician fee schedule (PFS) for such products. Other digital solutions have been incorporated into physician codes and fees for related services, captured in standard remote monitoring codes, or bundled within the fees for home-use durable medical equipment (DME). Essentially, digital solutions fall into four primary areas within the US Medicare framework:

- PDTs involving patient self-use software, which are not yet broadly covered by Medicare, with a few exceptions.
- Physician telehealth services, which are remote physician services specifically identified by Medicare.
- Remote patient and treatment monitoring, which have specific codes and constraints.
- Miscellaneous digital technologies billed incident to physician services, which are slowly emerging and typically require specific procedure coding.

Hence, in the Medicare programme, progress in the digital space has come in the form of smaller steps to address specific services in the digital realm. An overview of each of these areas is provided below.

PDTs

PDTs are defined as FDA-cleared or -approved software-based medical devices prescribed by a clinician that are intended to prevent, manage, or treat a medical condition. FDA-cleared PDTs to date span a range of clinical indications, from substance-use disorder to ADHD to insomnia.[1]

The most recent progress in the Medicare programme for PDTs is in the area of digital mental health treatment (DMHT) devices, for which the Centers for Medicaid and Medicare Services (CMS) issued three Healthcare Procedure Coding System (HCPCS) Level II codes for cognitive behavioural therapy when it occurs incident to physician behavioural services. These codes, however, must be billed by a physician and cannot be covered and paid for as a standalone service.

A key distinction is how CMS should pay for Software as a Service (SaaS), which does not fit into any Medicare standalone benefit category.

The Access to Prescription Digital Therapeutics Act of 2023 would establish, for the first time, a Medicare benefit category for FDA-cleared or -approved digital therapeutics. If enacted, CMS would have one year to establish a payment methodology considering factors including actual list charge, weighted median of payment rates, and ongoing use. Within two years, CMS would be required to issue product-specific HCPCS codes, and manufacturers would be required to annually report payment rates, distribution volumes, and user counts. If enacted, this legislation would bring new promise to a category of technologies not previously addressed in the US Medicare programme.

Separately, private insurers have considered, and in some cases covered, digital therapeutics using digital formularies designed to provide patient access to self-use applications for monitoring and self-management of disease and other health objectives. Prescription digital products, however, have been far less successful in gaining reimbursement among commercial payers.

Key milestones in the journey to code remote apps and digital technologies in the US are as follows:

- 2018–2020: CMS establishes payment for remote patient monitoring (RPM), including codes 99091, 99453, 99454, 99457 and 99458.
- 2022: CMS implements Level II HCPCS code A9291 for prescription digital behavioural therapy, FDA cleared, per course of treatment, effective April 1, 2022.
- 2022: The American Medical Association (AMA) approves five remote therapeutic monitoring (RTM) Current Procedural Terminology (CPT) codes, initially

aimed at respiratory and musculoskeletal conditions: 98975; 98976; 98977; 98980; and 98981.

- 2023: CMS finalises a new RTM device supply code for cognitive behavioural therapy monitoring (CPT 98978), with reimbursement to be determined by local Medicare Administrative Contractors.
- 2023: The bipartisan Access to Prescription Digital Therapeutics Act is introduced in Congress (S.723/H.R.1458), proposing to establish Medicare and Medicaid coverage and reimbursement for FDA-approved prescription digital therapeutic apps. The legislation has not yet been enacted.
- 2025: CMS establishes Medicare payment for physician-billed DMHT devices, furnished incident to physician behavioural services, enabling billing of digital cognitive behavioural therapy with three HCPCS Level II codes (G0552, G0553, and G0554).
- 2026: CMS will expand its payment policy for DMHT devices and requests public comment on payment policies for SaaS devices. Separately, CMS will add new services to the Medicare Telehealth Services List: G0473; CPT 90849; G0545; 92622; and 92623. CMS will also add two new codes for RPM: 99445; and 99470.

Remote digital monitoring technologies

The area of remote monitoring has seen far more success in the Medicare programme, starting with CMS's introduction of payment for RPM codes in 2018, with expanded codes added in 2019–2020, and the subsequent issuance in 2022 of RTM codes for respiratory and musculoskeletal conditions. Neither RPM nor RTM services meet the definition of telehealth and thus are not subject to telehealth place of service rules; they are classified as inherently non-face-to-face services.

RPM codes address three areas of activity: education and setup; supply of internet-connected devices; and treatment management by the physician of the patient's health condition.

RPM services automatically collect and transmit patient health data, such as blood pressure, weight, and glucose levels, using a connected medical device to their healthcare provider. The provider then uses this data to treat or manage (remotely monitor) the patient's condition.

In its CY 2026 final rule, CMS expanded RPM payment to include two new codes: CPT 99445 for remote monitoring of physiologic parameters (e.g., weight, blood pressure, pulse oximetry, respiratory flow rate) when data is transmitted for two to 15 days in a 30-day period, and CPT 99470 for monitoring treatment management services covering the first 10 minutes of clinical staff/physician time in a calendar month.

RTM codes are used in healthcare to track therapy adherence, therapy response, and digital therapeutic intervention through FDA-approved devices. They are intended for services that physical therapists, occupational therapists, and speech-language pathologists can furnish, when appropriate. The codes specifically focus on non-physiologic data related to the musculoskeletal, respiratory, or cognitive behavioural therapy domains, distinguishing them from RPM codes. In its final rule for 2026, CMS added four new codes to the RTM list to provide flexibility for shorter monitoring periods and briefer clinician interactions: 98984 (respiratory system device supply, two to 15 days); 98985 (musculoskeletal system device supply, two to 15 days); 98986 (cognitive behavioural therapy device supply, two to 15 days); and 98979 (treatment management services, first 10 minutes).

Telehealth services

Telehealth services, typically covered under Medicare Part B, are healthcare services that are provided using telecommunications technology, allowing patients to receive medical care remotely. Approved telehealth services span several areas:

- Office Visits: Routine evaluations and management services with healthcare providers.
- Mental Health Services: Psychotherapy and counselling.
- Consultations: Specialist consultations requested by another provider.
- Preventive Services: Certain screenings and risk-reduction visits.
- Chronic Care Management: Services like diabetes self-management training.

CMS maintains a Medicare Telehealth Services List with more than 250 eligible service codes. As of 2026, CMS will eliminate the previous "provisional" and "permanent" designations, treating all listed services as permanent while retaining authority to remove services if warranted.

In its 2026 final rule, CMS added several new services to the Medicare Telehealth Services List: group behavioural counselling for obesity; multiple-family group psychotherapy; an infectious disease add-on code for inpatient visits; and auditory integrated sound processor services (codes 90849, G0473, G0545, 92622, and 92623).

In addition, CMS finalised its proposal to permanently remove frequency limitations on certain nursing home and hospital telehealth visits that had been lifted temporarily during the COVID-19 public health emergency. CMS also finalised a proposal to permanently allow direct supervision of diagnostic imaging services via real-time telehealth (excluding audio-only), except for services using specified global surgery indicators.

Other physician-use digital technologies

Separate from RPM, RTM and telehealth services, there is a small number of physician CPT codes that can be billed for services that depend on specific digital technologies, either remote services or locally run algorithms that provide assistive or augmentative support to physician monitoring, interpretation or decision-making. Historically, CMS has considered most computer software and associated analyses and licensing fees to be indirect costs tied to costs for associated medical equipment. However, beginning with payment for Fractional Flow Reserve Computed Tomography (FFRct) in the CY 2022 PFS final rule (86 FR 65041), CMS has made intermediate, service-specific policies to allow for PFS payment of SaaS and Artificial Intelligence (AI) applications in certain circumstances.[2]

Apart from the code for FFRct, 75580, the AMA has issued seven category III codes for physician treatment and monitoring using digital technologies. Of these, five are related to digital treatment of amblyopia and two codes are related to autonomous algorithm-based recommendation system for insulin dose calculation and titration. Coverage of these codes is still evolving.

Digital solutions embedded within DME

Finally, a range of devices that are DME items may offer data transmission capabilities. Unfortunately, without

accompanying codes and physician payment for the digital services, reimbursement of services within the cost of the DME device itself is quite limited, as most DME devices are either purchased or provided via a 13-month lease.

In addition, if the primary function of a device is monitoring and measurement, CMS previously ruled that items used in the patient's home that provide monitoring and measurements for the physician/practitioner to evaluate the patient's condition and course of treatment do not fall under the Medicare benefit for DME.[3]

III. Reimbursement of Digital Solutions in Germany

Like the US Medicare programme, Germany has addressed different digital solutions according to the setting of care and payment pathway. These can be divided between outpatient remote monitoring services and patient self-use software applications.

Payment for remote software under the Digital Health Applications (DiGA) framework

Germany addressed the issue of reimbursable SaMD in its development of the DiGA pathway for medical applications and digital health treatments, under a law that was implemented in 2020,[4] and that was subsequently updated with the Digital Act (*Digitalgesetz*, DigiG) in 2024.

The DiGA programme provides rapid patient access to prescribed digital applications under the DiGA Fast-Track evaluation by *Bundesinstitut für Arzneimittel und Medizinprodukte* (BfArM), or alternatively through piecemeal local contracts with Statutory Health Insurances (SHI).

The DiGA programme provides a preliminary listing for one year to enable the manufacturer to produce evidence for clinical benefit of the DiGA. Evidence from at least a pilot study is needed for the application.

Similar to regulations in drugs, the DiGA is reimbursed at a manufacturer-determined price for the first year and, following that initial period, at a price negotiated between the manufacturer and the SHI head association (GKV-SpiV). Eligible devices are those:

- whose main function is essentially based on digital technologies;
- which are intended to support the diagnosis, monitoring, treatment, alleviation or compensation of diseases, injuries, or deficiencies; and
- which are used by the patient or the patient and the caregiver together.

As of November 2025, 47 DiGA devices had been approved and were listed, along with 16 that had previously been listed and were subsequently cancelled, and 10 were pending review.

To be listed, candidate technologies must satisfy certain requirements for data protection, IT security, interoperability, robustness, consumer protection, ease of use, support of healthcare providers, quality of medical content and patient safety. Sponsors must prove at least one positive healthcare benefit that could be a medical benefit with demonstrated clinical relevance in a retrospective study, or, preferably, a randomised control trial.

An initial, key limitation was that DiGA was only open to Class I or IIa devices, but this limitation was recently changed to include Class IIb devices, subject to an additional evidence review by the Joint Federal Committee on Healthcare (G-BA).

Separately, under the Digital Care and Nursing Modernization Act, a separate category of applications for Digital Nursing Applications (DiPA) was established, which are intended to "improve the state of health of care recipients or to improve communication with relatives and care professionals". Currently, as with DiGA, DiPA applications can be filed at the BfArM, but none are yet approved.

Outpatient monitoring services

Under the EBM (German Uniform Evaluation Standard) catalogue, nine procedure codes were added in 2022 to support telemonitoring, following a trial period that had commenced in 2019.

These telemonitoring codes range in reimbursement from approximately eight to 19 euros for physician or clinic services, with most fees limited to quarterly billing, along with a cardiac telemonitoring code that pays 136 euros per quarter. However, in July 2025, unified reimbursement for monitoring and transmission devices were added under two distinct companion codes that pay 68 and 396 euros, respectively.

Other hospital inpatient services that are supported with remote services would be bundled within the hospital admission diagnosis-related group payment, with no distinct payment.

IV. Reimbursement of Digital Solutions in the UK

The British National Health Service (NHS) has made the transition to digital and AI-based solutions a clear priority, with funding available to technologies that meet criteria under a Digital Technology Assessment Criteria (DTAC) framework, as well as positive appraisal by the National Institute for Clinical Excellence (NICE). NHS efforts are also supported by NICE's Evidence Standards Framework, a set of evidence standards for digital health technologies (DHTs) developed in partnership with NHS England that are designed to ensure new DHTs are clinically effective and offer value to the health and care system. This conceptual coverage, however, does not necessarily imply distinct reimbursement. As the NHS has devolved into a system of 42 Integrated Care Systems (ICSs), it has also divested day-to-day financial decisions and technology adoption choices to ICS commissioners, who decide what to commission based on perceptions of value in their local context. Unlike most pharmaceutical appraisals by NICE, DTAC determinations are not binding on local ICSs.

In concept, the NHS has identified three key criteria that DHTs must meet in order to receive funding:

1. Be appropriately CE/UKCA marked to be placed on the market in the UK, ensuring that the device is safe, and works as described by the manufacturer.
2. Pass the DTAC to ensure that they meet core standards for clinical safety, data protection, security, interoperability, accessibility, and usability.
3. Be recommended by NICE, to ensure they are plausibly cost-effective and therefore represent value for the NHS.

Whilst the NHS offers innovators perhaps the most refined and specific evaluation framework available in the world, there is an absence of dedicated funding and a clear pathway to obtain reimbursement. National tariffs for digital solutions are unlikely and rather, such services are paid under block contract. Though some may be contracted nationally by the NHS, a greater likelihood is local ICS engagement with subscription to digital solutions that bring promise to their

patients, as well as strong potential for economic savings. The latter consideration is likely to require clear support in the findings of NICE.

V. Reimbursement of Digital Solutions in France

France has only recently developed a framework for digital technologies, in part modelled after the German DiGA framework, for digital prescribed applications as well as remote monitoring and therapeutic technologies. For other physician-use AI technologies, France still relies on its traditional pathways for medical device evaluation. Here, a clinical assessment is implemented by the *Commission nationale d'evaluation des dispostifs médicaux et des technologies* (CNEDiMTS), which is the key committee of the *Haute Authorite de Sante* (HAS). Thus, the French pathways break down into three areas:

- Remote monitoring devices and software applications: The List of Medical Telemonitoring Activities (LATM) pathway.
- Patient self-use software applications: The *prise en charge anticipée numérique* (PECAN) pathway for therapeutics and telemonitoring.
- AI imaging and diagnostic tools: Evaluated as traditional medical devices, with possible reimbursement via the *Liste des Produits et Prestations Remboursables* (LPPR or "List of Reimbursable Products and Services") or bundled within existing general healthcare system payments.

Traditional pathway for digital tools

As with other devices, a digital therapeutic or diagnostic is considered innovative when the assessment rating is from *Amélioration du Service Attendu* (ASA) I to III. If the new digital healthcare product brings a minor improvement compared to the current strategy, the assessment is an ASA IV. In case of no improvements of the clinical value compared with other alternatives, the assessment is an ASA V (28).

As with other separately payable devices, this clinical evaluation is followed by a price negotiation between the manufacturer and the *Comité économique des produits de santé* (CEPS), which considers the strength of the HAS evidence rating as well as expected total expenditure (budget impact) of the new technology.

Because the HAS evaluation is driven primarily by comparative randomised evidence, the French process has historically provided very low evidence ratings for most devices, with fewer than 5% of devices receiving an ASA I, the top-level evidence rating.

LATM pathway telemonitoring

Following its implementation in June 2023, LATM provides reimbursement across several clinical areas, specifically: heart failure; renal failure; chronic respiratory insufficiency; and diabetes. Additional areas, such as oncology, can establish reimbursement through branded lines. LATM operates on a dual-payment model, compensating both the technology manufacturer and the healthcare provider performing remote monitoring. Required elements for approval include a favourable opinion by the HAS and a CNEDiMTS clinical evaluation, as well as an ARS (Regional Health Agency) administrative declaration, and an *Agence du Numérique en Santé* (ANS) interoperability certification.

PECAN reimbursement of patient applications

France has developed a special pathway called PECAN for therapeutics, if they have met the regulatory requirements of the EU AI Act, along with the Medical Device Regulation requirements.

PECAN is a transitional, one-year reimbursement pathway, which provides temporary reimbursement by the *Assurance Maladie* (French health insurance) for digital medical solutions that demonstrate promise but may not yet have complete evidence of clinical benefit. The mechanism effectively allows manufacturers and operators to access reimbursement while simultaneously finalising the clinical or organisational evidence required for eventual permanent listing on either the LPPR (for therapeutic digital devices) or the LATM (for telemonitoring solutions).

The PECAN pathway represents a policy innovation modelled in part after Germany's DiGA framework and accommodates both digital therapeutic devices (DTx) intended for patient self-use as well as remote medical monitoring systems that operate within healthcare facility or ambulatory care settings. PECAN extends reimbursement eligibility to two distinct categories of digital medical devices: DTx; and telemonitoring solutions.

As of September 2024, approximately 17 applications had been initiated for PECAN, with two successful approvals, five refusals, and one withdrawn application reported, reflecting a modest but growing uptake.

VI. Conclusions

Though no single country has yet addressed the different aspects of digital health reimbursement, progress is occurring across the US, Germany, France, and UK markets and now, in particular, is turning to recognise more autonomous use of software solutions directly by patients. At the same time, payment for physician services that are assisted or augmented by AI and other digital solutions is advancing as well. In all markets, this latter issue faces a number of hurdles, not the least of which are potential concerns by physician societies whose members also depend on the same payment systems.

A key challenge for innovator firms, as they prepare for the demands of these global markets, is to understand the elements of their technologies that will be reimbursable, as well as the coding and coverage parameters that will apply in each market. Very few technologies are able to seamlessly achieve reimbursement across all of the markets, and the clinical evidence demands are highly variable.

For companies seeking to define and optimise their market opportunities for digital technologies, Avania has an experienced team of market-access experts in each major geography of the world. Because every technology presents unique challenges, Avania specialises in customised solutions that help companies understand the priority and sequence of each market launch.

References

United States legislation and regulations

Access to Prescription Digital Therapeutics Act of 2023, S. 723, 118th Cong. (2023). https://www.congress.gov/bill/118th-congress/senate-bill/723

Access to Prescription Digital Therapeutics Act of 2023, H.R. 1458, 118th Cong. (2023). https://www.congress.gov/bill/118th-congress/house-bill/1458

Centers for Medicare & Medicaid Services. (November 1, 2024). *Medicare program; CY 2025 payment policies under the physician fee schedule and other changes to Part B payment and coverage policies* (Final rule). Federal Register, 89(221). https://www.cms.gov/newsroom/fact-sheets/calendar-year-cy-2025-medicare-physician-fee-schedule-final-rule

Centers for Medicare & Medicaid Services. (October 31, 2025). *Medicare and Medicaid programs; CY 2026 payment policies under the physician fee schedule and other changes to Part B payment and coverage policies; Medicare Shared Savings Program requirements; and Medicare prescription drug inflation rebate program* (Final rule). Federal Register, 90(212). https://www.federalregister.gov/documents/2025/11/05/2025-19787/medicare-and-medicaid-programs-cy-2026-payment-policies-under-the-physician-fee-schedule-and-other

Digital Mental Health Treatment Devices, 21 C.F.R. § 882.5801 (2024).

Computerized Cognitive Behavioral Therapy Device for Psychiatric Disorders, 21 C.F.R. § 882.5801 (2024).

Prescription Digital Cognitive Behavioral Therapy for Attention Deficit Hyperactivity Disorder, 21 C.F.R. § 882.5803 (2024).

U.S. Food and Drug Administration. (2023). *Software as a Medical Device (SaMD).* Digital Health Center of Excellence. https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd

German legislation and regulations

Digitale-Versorgung-Gesetz (Digital Healthcare Act), BGBl. I S. 2562 (2019). https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl119s2562.pdf%27%5D__1609459200000

Digitale Gesundheitsanwendungen-Verordnung (Digital Health Applications Ordinance) (DiGAV), BGBl. I S. 768 (2020).

Digitalgesetz (Digital Act) (DigiG), BGBl. I Nr. 101 (2024).

Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (Digital Care and Nursing Modernization Act) (DVPMG), BGBl. I S. 1309 (2021).

Bundesinstitut für Arzneimittel und Medizinprodukte (Federal Institute for Drugs and Medical Devices). (2023). *DiGA-Leitfaden: Das Fast-Track-Verfahren für digitale Gesundheitsanwendungen* (DiGA) *nach* § 139e SGB V (Version 3.5). https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/DiGA/Wissenswertes/_artikel.html

Sozialgesetzbuch, Fünftes Buch (German Social Code Book V) §§ 33a, 134 and 139e (SGB V).

GKV-Spitzenverband. (December 16, 2021). *Rahmenvereinbarung über die Maßstäbe für die Vereinbarungen der Vergütungsbeträge für digitale Gesundheitsanwendungen nach* § 134 Abs. 4 SGB V (Framework agreement). https://www.gkv-spitzenverband.de/gkv_spitzenverband/presse/fokus/fokus_diga.jsp

French legislation and regulations

Ministère de la Santé et de la Prévention (Ministry of Health and Prevention). (March 31, 2023). *Décret relatif à la prise en charge anticipée des dispositifs médicaux numériques à finalité thérapeutique et des activités de télésurveillance médicale* (Decree on early coverage of digital medical devices for therapeutic purposes and medical telemonitoring activities) (PECAN). *Journal Officiel de la République Française.*

Haute Autorité de Santé (French National Authority for Health). (2023). *Liste des activités de télésurveillance médicale (LATM): Guide d'évaluation et de remboursement* (List of medical telemonitoring activities: Evaluation and reimbursement guide). https://www.has-sante.fr

Agence du Numérique en Santé (Digital Health Agency). (2023). *La prise en charge anticipée numérique (PECAN): Guide pour les fabricants* (Digital early coverage: Guide for manufacturers). https://gnius.esante.gouv.fr/en/financing/reimbursement-profiles/early-access-reimbursement-digital-devices-pecan

Code de la sécurité sociale (French Social Security Code) art. L.165-1-5, R.165-91 (LPPR provisions).

Comité national d'évaluation des dispositifs médicaux et des technologies de santé (National Committee for the Evaluation of Medical Devices and Health Technologies) (CNEDiMTS). (2024). *Principes d'évaluation pour les dispositifs médicaux numériques* (Evaluation principles for digital medical devices). *Haute Autorité de Santé.*

United Kingdom frameworks and guidance

NHS England. (2021). *Digital Technology Assessment Criteria (DTAC).* NHS Transformation Directorate. https://transform.england.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac

National Institute for Health and Care Excellence. (2019, updated 2022). *Evidence standards framework for digital health technologies* [ECD7]. https://www.nice.org.uk/corporate/ecd7

Department of Health and Social Care. (2021). *A guide to good practice for digital and data-driven health technologies.* NHS AI Lab. https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology

NHS Digital. (2021). *DCB 0129: Clinical risk management: Its application in the manufacture of health IT systems* (Information standard). https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems

NHS Digital. (2021). *DCB 0160: Clinical risk management: Its application in the deployment and use of health IT systems* (Information standard). https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0160-clinical-risk-management-its-application-in-the-deployment-and-use-of-health-it-systems

European Union regulations

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Medical Device Regulation), 2017 O.J. (L 117) 1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745

Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L) 1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

Healthcare Procedure Coding System (HCPCS) and Current Procedural Terminology (CPT) codes

Remote Patient Monitoring

American Medical Association. (2019). CPT code 99091: Collection and interpretation of physiologic data. *Current Procedural Terminology* (CPT) codebook.

American Medical Association. (2019). CPT codes 99453-99458: Remote physiologic monitoring services. *Current Procedural Terminology* (CPT) codebook.

Remote Therapeutic Monitoring

American Medical Association. (2022). CPT codes 98975-98981: Remote therapeutic monitoring services. *Current Procedural Terminology* (CPT) codebook.

American Medical Association. (2024). CPT codes 98985, 98979: Remote therapeutic monitoring (two to 15-day data collection). *Current Procedural Terminology* (CPT) codebook.

Digital Mental Health Treatment

Centers for Medicare & Medicaid Services. (2022). HCPCS code A9291: Prescription digital behavioral therapy. *Healthcare Common Procedure Coding System* (HCPCS) Level II.

Centers for Medicare & Medicaid Services. (2025). HCPCS codes G0552-G0554: Digital mental health treatment devices and services. *Healthcare Common Procedure Coding System* (HCPCS) Level II.

Endnotes

1 S.723, 118th Congress (2023–2024): Access to Prescription Digital Therapeutics Act of 2023 | Congress.gov | Library of Congress. https://www.congress.gov/bill/118th-congress/senate-bill/723/text

2 CY2026 PFS Final Rule.

3 Centers for Medicare & Medicaid Services' (CMS') Healthcare Common Procedure Coding System (HCPCS) Level II Final Coding, Benefit Category and Payment Determinations. https://www.cms.gov/files/document/2023-hcpcs-application-summary-biannual-1-2023-non-drug-and-non-biological-items-and-services.pdf

4 The Digital Care Act (*Digitale Versorgung Gesetz*, DVG) came into force on December 19, 2019.



Stephen A. Hull is a veteran market-access expert specialised in medical technology and diagnostic technologies. He was formerly Founder and President of Hull Associates LLC, an international market-access firm, and also a Sr. Vice President at AdvaMed in Washington DC. Mr. Hull also served as a Principal at Covance Health Economics and Outcomes Services and has led a long career in government affairs. He has an advanced degree in health policy from the Johns Hopkins Bloomberg School of Public Health and an undergraduate degree from Colgate University.

Avania B.V.
10 Post Office Square, Suite 950
Boston Mass. 02109
USA

Tel: +1 240 486 6776
Email: stephen.hull@avaniaclinical.com
LinkedIn: www.linkedin.com/in/stephen-hull-483b6a230



Tarek Hamdan, PharmD, is a Senior Consultant in France and Middle Eastern markets providing strategic advisory support to a broad range of device, diagnostic, and pharmaceutical clients. He has supported numerous innovator firms launching in France and seeking to address evidence requirements across multiple EU geographies.
His expertise spans reimbursement and pricing, Health Technology Assessment (HTA), and Managed Entry Agreements (MEAs) for new innovations entering these target markets. He covers the full product lifecycle, from launch readiness and evidence generation to stakeholder engagement in key markets like France and the GCC. Previously, Tarek served as a Research Scientist at Ichnos Glenmark Innovation (IGI) in Lausanne, Switzerland, where he focused on oncology research. Tarek holds a Doctor of Pharmacy from the Université Claude Bernard Lyon 1 and a Master of Science from the Université Grenoble Alpes.

Avania B.V.
France

Email: tarek.hamdan@avaniaclinical.com
LinkedIn: www.linkedin.com/in/tarek-hamdan-pharmd



Kirstin Osthoff is a Sr. Consultant in Germany, having served as a consultant for medical device and diagnostic companies for 20 years, across a broad range of medical technologies. Kirstin has extensive experience in financial analysis and management, forecasting, company restructuring and M&A activities. She was formerly a manager of finance and controlling at Edwards Lifesciences, and previously served as a manager of finance and controlling at Baxter Ltd. in Germany and Spain. She also managed logistics and purchasing for Baxter Deutchland. Kirstin has completed academic work in economics and computer science and is fluent in German, English and Spanish.

Avania B.V.
Germany

Email: kirstin.osthoff@avaniaclinical.com
LinkedIn: www.linkedin.com/in/kirstin-osthoff-3b92414a



Dr. Eric Lam is Senior Vice President of Market Access and Reimbursement at Avania B.V., where he leads strategy and execution for diagnostics, medical devices, and emerging healthcare technologies. He brings more than 15 years of experience in the pharmaceutical and healthcare industries, with deep expertise in U.S. and global market access. Dr. Lam has successfully supported numerous technologies through complex coverage, coding, and payment pathways, supporting payer adoption, health economic value demonstration, and commercialisation across multiple markets. His experience includes designing and implementing integrated market access frameworks, evidence generation and publication strategies, and clear value communication to payers, providers, and policymakers. Dr. Lam earned his Ph.D. in Pharmacology from Case Western Reserve University and completed a NIH-sponsored postdoctoral fellowship in the Departments of Pharmacology and Medicine.

Avania B.V.
10 Post Office Square, Suite 950
Boston Mass. 02109
USA

Tel: +1 216 255 7115
Email: eric.lam@avaniaclinical.com
LinkedIn: www.linkedin.com/in/eric-lam-phd-7552641a5

Your Trusted MedTech Partner
When breakthrough medical technologies hold the promise of transforming patient care, the journey from concept to commercialisation demands more than traditional CRO services. It requires a partner who understands the distinct challenges of medtech innovation, one who combines deep expertise with collaborative commitment to your success. That partner is Avania.
As the only global CRO built for MedTech, Avania is purpose-designed to navigate the complexities of medical devices, diagnostics, and combination products. We offer comprehensive, flexible solutions that reduce risk and accelerate your product's path to market.

Medical device development involves challenges unlike any other sector: intricate regulatory pathways; demanding clinical trial designs; and specialised engineering considerations.

www.avaniaclinical.com

Avania
MedTech's Trusted Champion

Regulatory Strategy for Digital Therapeutics and Artificial Intelligence-Enabled Devices


Dr. Acacia Parks


Nick Butt


Sophia Farcas


Dr. Angela Johnson

Avania B.V.

Introduction

The term "digital therapeutics" (DTx) is defined by the International Organization for Standardization (ISO) as "health software intended to treat or alleviate a disease, disorder, condition, or injury by generating and delivering a medical intervention that has a demonstrable positive therapeutic impact on a patient's health" (ISO/TR 11147:2023). This definition distinguishes DTx from "wellness" applications, remote monitoring platforms, and clinical decision support systems through their requirement for rigorous clinical validation via randomised controlled trials and real-world evidence (RWE) generation (Digital Therapeutics Alliance, 2023).

Broadly speaking, DTx are considered Software as a Medical Device (SaMD) products and are often delivered via mobile applications, digital platforms, or connected devices. DTx cross therapeutic indications and align with three functional categories based on their primary therapeutic purpose: (1) treatment interventions that directly address disease pathology; (2) disease management tools that optimise ongoing care delivery; and (3) preventive applications that mitigate disease progression or occurrence (Digital Therapeutics Alliance, 2021).

DTx and, more recently, Artificial Intelligence (AI)-enabled devices, have the potential to rapidly change the patient care landscape. In 2016, Pear Therapeutics' reSET device became the landmark DTx product that kicked off the category with its successful De Novo, creating a new code for computerised behavioural therapy devices for psychiatric disorders (Pear Therapeutics, DEN 160018). Since then, the US Food and Drug Administration (FDA) has cleared 192 DTx products spanning mental health disorders, metabolic conditions, chronic pain management, and neurological conditions primarily via the De Novo and 510(k) pathways, while China's National Medical Products Administration has authorised 235 (Liang *et al.*, 2025). Per FDA's AI-enabled device list, 235 new AI-enabled devices were authorised in 2024, an all-time high. There have been 1,250+ AI-enabled devices approved (up from 950 in August 2024), a 32% increase in under a year (Bipartisan Policy Center).

Within the DTx landscape, AI-enabled DTx represent a more modern subset characterised by adaptive algorithms that leverage machine learning (ML) techniques to personalise therapeutic interventions, using software that can learn and modify its outputs based on parameters like patient-specific behavioural patterns, physiological responses, and engagement metrics (Hargreaves, 2023). These AI-enabled systems employ supervised, unsupervised, or semi-supervised learning methodologies to continuously refine treatment pathways, capabilities that necessitate specialised and rapidly evolving regulatory frameworks, including FDA's Predetermined Change Control Plans (PCCPs), to ensure safety and effectiveness throughout the total product lifecycle (FDA, 2024a). The integration of adaptive ML distinguishes AI-enabled DTx from static, rule-based therapeutic software by enabling new functionalities, such as real-time treatment optimisation, while simultaneously generating high-density patient datasets that inform iterative product improvements and development cycles (Hargreaves, 2023). The learning nature of AI-enabled software in the field requires new development and regulatory approaches.

Continues overleaf

Figure 1: Number of US FDA approvals for AI/ML-enabled medical devices over time

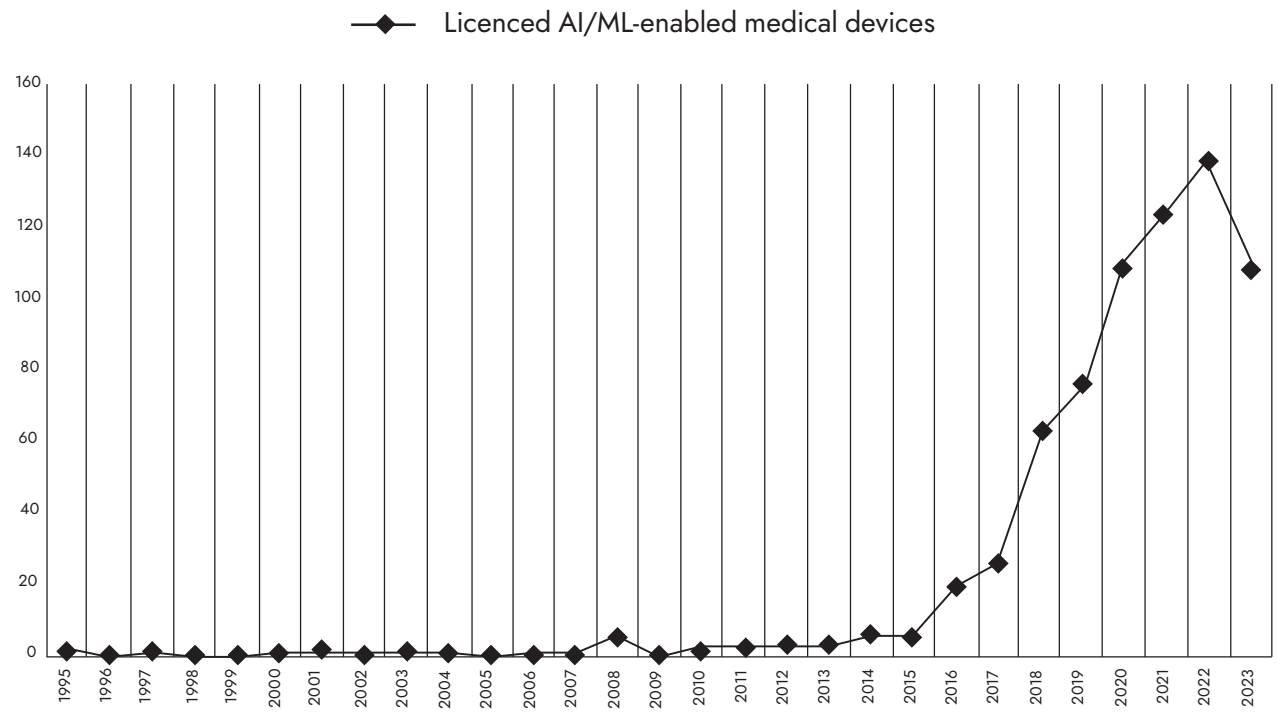
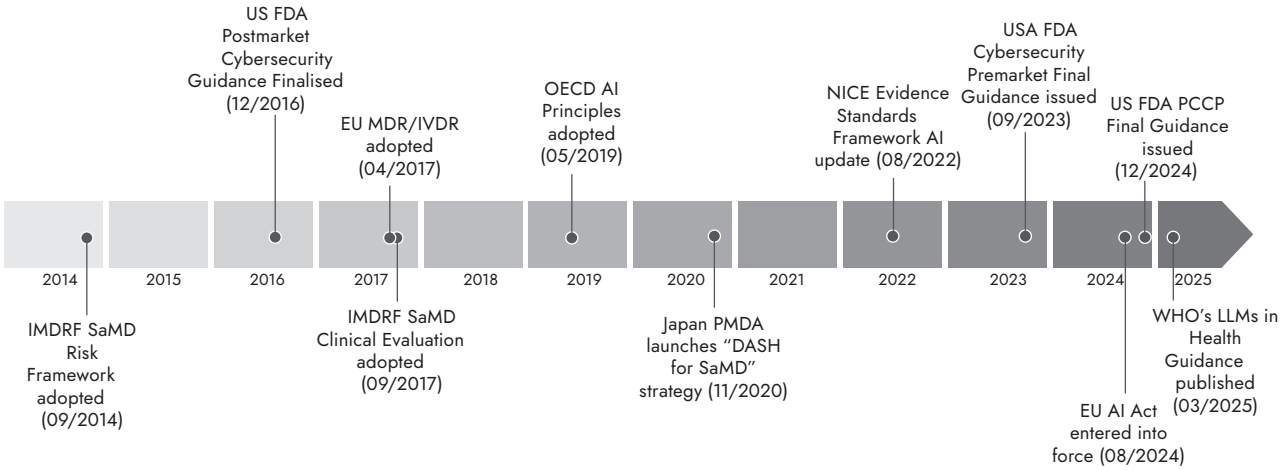


Figure adapted from Muralidharan, et al., 2024.

Regulatory Policy Landscape for DTx and AI-enabled Devices

FDA and global health authorities have made meaningful progress in defining pathways for digital health products. The regulatory frameworks governing AI-enabled technologies and advanced DTx remain in active development. This dynamic landscape means that device developers and regulatory reviewers cannot rely solely on precedent, and both must integrate policy and technological trends and adapt proactively to evolving device capabilities.

Figure 2: Timeline of Evolving DTx Regulations



IMDRF: International Medical Device Regulators Forum; LLM: Large Language Model; MDR/IVDR: EU Medical Device Regulation/In Vitro Diagnostic Regulation; NICE: National Institute for Health and Care Excellence; OECD: Organisation for Economic Co-operation and Development; PCCP: Predetermined Change Control Plan; SaMD: Software as a Medical Device; WHO: World Health Organization.

The regulatory architecture for DTx and AI-enabled medical devices remains fundamentally fragmented despite coordinated efforts toward international harmonisation. While the International Medical Device Regulators Forum (IMDRF) established foundational SaMD frameworks in 2014 (IMDRF, 2014), and subsequently refined risk categorisation principles (IMDRF, 2025), national authorities have implemented these concepts through distinctly divergent regulatory programmes that reflect underlying differences in risk tolerance, evidentiary expectations, and administrative culture.

Three critical strategic tensions define the current landscape (Table 1):

(1) the accelerated pace of technological development, resulting in a mismatch between algorithmic innovation cycles and traditional long and relatively static device modification pathways;
(2) the absence of mature, harmonised frameworks for continuously learning algorithms, though programmes like the FDA's pioneering PCCP guidance make meaningful progress (FDA, 2024a); and
(3) the tensions between sector-specific medical device regulations and horizontal AI governance frameworks like the EU AI Act, creating layered compliance obligations that fundamentally reshape go-to-market strategies across jurisdictions (Table 1).

DTx companies successfully scaling AI-enabled therapeutics treat regulatory architecture as competitive differentiation rather than compliance burden. Three distinct strategies are emerging: Innovation-First (US–UK primary markets with FDA PCCP and sandbox leverage, accepting regulatory debt for speed); Global-Ready (designing for Japan/EU stringency from inception to compress time-to-global-market); and Market-Specific (regional optimisation accepting delayed or foregone multi-market entry). The strategic choice fundamentally depends on capital availability, addressable market prioritisation, and risk tolerance for regulatory pivots if primary markets face reimbursement challenges.

FDA's risk-based pragmatism

FDA's approach permits RWE generation and adaptive clinical study designs, positioning the US as the preferred market for DTx innovation (FDA, 2024b). FDA's risk-based framework allows for different pathways with progressively more stringent requirements as the risk of the device increases. For example, the highest risk devices (Class III) go through a Premarket Approval process. The lowest risk devices (Class I) may only be required to register their establishment and list their device with FDA, with no formal review process, particularly if they can be classified alongside other common device types that are "510(k) exempt". All devices under FDA's oversight are subject to General Controls (e.g. proper labelling, registration, and quality system regulation), but 510(k)-exempt devices are *only* subject to General Controls. Another interesting low-risk category in digital health is known as "enforcement discretion", which comprises products that may or may not be devices and that are considered to be at a risk level that FDA chooses, at their discretion, not to exercise enforcement oversight. In between these two extremes are devices that require premarket review, which primarily includes all Class II devices and some non-exempt Class I devices. If a device is low risk (Class I or II) but is novel, and cannot be likened to any existing device in terms of technological characteristics or intended use, the De Novo pathway enables creation of new codes for novel products that then may be used as precedents for future 510(k)s. That regulation will contain Special Controls, or additional requirements for devices of that product type. These could include specific performance standards, labelling requirements, or post-market surveillance requirements, for example. If a device is low risk (Class I or II), but can be likened to an existing device, it may be subject to the 510(k) pathway; when a product is cleared via 510(k), it becomes attached to the same regulation as its predicate and is subject to the same Special Controls.

The FDA's PCCP framework, finalised in December 2024, represents the most sophisticated regulatory mechanism globally for managing AI-enabled device modifications while maintaining safety assurance (FDA, 2024a). Under the Federal Food, Drug, and Cosmetic Act §515C (enacted via the 2022 Food and Drug Omnibus Reform Act), manufacturers can pre-specify algorithmic modifications within approved boundaries, enabling continuous improvement without repeated premarket submissions, critical for ML devices.

The FDA also signalled a new risk-based framework for generative AI at the Agency's November 6, 2025, Digital Health Advisory Committee (DHAC) meeting examining "Generative Artificial Intelligence-Enabled Digital Mental Health Medical Devices". Despite its primary focus on mental health devices, the meeting represents a watershed moment in regulatory thinking for AI-enabled DTx more generally (FDA, 2025a). The Committee's nine-hour deliberation included presentations from non-device generative-AI mental health companies debating the boundary between regulated and non-regulated software functions, as well as discussion of a hypothetical prescription large language model (LLM) therapy chatbot for major depressive disorder, exploring scenarios across prescription *versus* Over-the-Counter pathways, adult *versus* adolescent populations, and single *versus* multiple mental health indications (Orrick, 2025).

Key regulatory signals emerging from public proceedings and manufacturer comments reveal the following Agency priorities:

(1) explicit risk stratification based on the degree of therapeutic autonomy and condition severity, an echo of FDA's overall risk-based approach;
(2) mandatory human escalation pathways and misuse detection mechanisms, consistent with FDA's general emphasis on humans-in-the-loop to critically evaluate AI output, see *Good Machine Learning Practice for Medical Device Development: Guiding Principles* (FDA and Health Canada, 2021);
(3) evidence requirements for equitable performance across demographic and linguistic populations, consistent with the value FDA consistently places on generalisability and bias reduction;
(4) continuous monitoring for model drift and safety signals, as well as misuse/overuse controls, and accessible explainability mechanisms, consistent with FDA guidance related to AI-enabled devices (FDA and Health Canada, 2021); and
(5) labelling transparency calibrated to the level of clinician involvement *versus* autonomous operation (FDA, 2025b; *Psychiatric Times*, 2025).

This meeting represents a critical inflection point in FDA's regulatory approach to LLM transformer-based AI therapeutic applications. Notably, for example, while FDA highlighted many ways that LLM-based DTx are held to similar standards as non-LLM-based DTx, the Committee acknowledged that generative AI's propensity to "confabulate, provide inappropriate or biased content, fail to relay important medical information, or decline in model accuracy" requires fundamentally different premarket evaluation compared to deterministic algorithms (*Psychiatric Times*, 2025).

Strategically, this meeting signals FDA's movement toward product-specific risk-assessment frameworks rather than categorical approval pathways for generative AI therapeutics. While the meeting topic was specific to devices addressing mental health indications, hearing FDA's thinking for this particular category of device is likely indicative of their thinking for similar devices in other indications. Sponsors developing AI-enabled mental health interventions should anticipate lifecycle regulatory approaches with heightened premarket scrutiny, real-world performance monitoring requirements, and potentially adaptive

labelling as evidence accumulates. The Agency's request for public comment, FDA-2025-N-2338 (FDA, 2025b), provides unprecedented transparency into regulatory decision-making and offers manufacturers a strategic opportunity to shape emerging guidance before it crystallises into binding policy.

It is also notable that, while current LLMs drive regulatory discussion at FDA, increasing sophistication of middleware orchestrating small language models (SLMs) and novel AI approaches like state space models (SSMs) are rapidly evolving. The focus on LLM regulation, while necessary, addresses one branch of a rapidly diverging evolutionary tree. Emerging architectures, SSMs with linear complexity, sparse mixture-of-experts (MoE) with selective activation, continuously adapting liquid networks, and graph neural networks (GNNs) for molecular reasoning each require fundamentally different validation paradigms. Regulatory frameworks optimised for transformer attention mechanisms may prove inadequate for architectures that do not share their failure modes, interpretability characteristics, or update dynamics.

EU's prescriptive dual-layer framework

The EU has taken a system-level approach to governing AI in healthcare, building on the strong foundations of its medical device framework. The EU Medical Device Regulation (MDR 2017/745) established a rigorous AI lifecycle model centred on clinical evidence, traceability, and post-market accountability. It requires structured Clinical Evaluation Reports, ongoing surveillance (Articles 83–92), and formal vigilance mechanisms, creating a substantially higher regulatory burden in the EU compared to US pathways (European Parliament and Council, 2017).

The EU AI Act (European Parliament and Council, 2024) extends this foundation into the algorithmic domain, positioning healthcare AI systems as high-risk technologies subject to conformity assessments, transparency documentation, and human oversight requirements. Together, the MDR and AI Act create an integrated "digital-by-design" framework that embeds ethical, clinical, and technical assurance across the product lifecycle. While this dual-oversight structure can lengthen approval timelines by an estimated 12–18 months compared to US pathways, it also delivers unparalleled visibility, accountability, and trust in the deployment of AI-driven medical technologies.

UK's agile framework

The UK Medicines and Healthcare products Regulatory Agency (MHRA) maintains EU MDR alignment principles while piloting agile AI oversight mechanisms, including regulatory sandboxes and accelerated pathways for software-based devices (MHRA, 2024). The UK's 2024 AI regulatory proposals outline a principles-based framework that prioritises safety, transparency, and fairness over rigid technical rules. This approach could give DTx developers an early advantage by allowing them to help shape guidance through active engagement with regulators.

Japan's evidence-intensive approach

Japan's Pharmaceuticals and Medical Devices Agency's (PMDA) and Ministry of Health, Labour and Welfare's SaMD/AI framework demands the highest evidentiary rigour globally, prioritising domestic clinical data, comprehensive algorithm transparency documentation, and mandatory post-market re-examination cycles extending 18–24 months beyond initial approval (PMDA, 2025). This approach generates robust real-world performance datasets and has established a strong safety track record for AI-enabled devices, making it one of the most stringent oversight frameworks internationally.

High-growth cluster in Asia-Pacific

The Asia-Pacific region is emerging as a high-growth cluster for AI-enabled medical devices and DTx, driven by rapid regulatory modernisation, targeted fast-track programmes and strong domestic innovation. Countries across the region are building targeted fast-track programmes that create early-access opportunities for device makers in this space:

- China's NMPA Special Review Procedures of Innovative Devices allow a fast-track evaluation for devices that demonstrate safety/performance advantage, and first-in-class or internationally advanced tech (China Center for Food and Drug International Exchange, 2025). NMPA has approved over 150 Class III AI medical devices, predominantly in pulmonary nodule detection and intracranial haemorrhage identification.
- Singapore's Health Sciences Authority (HSA) leads harmonisation among Southeast Asia through its 2024 guidance Change Management Program for ML-enabled SaMD, creating a regulatory proving ground for multinational DTx developers (HSA, 2024).
- South Korea's Digital Medical Products Act (effective January 2025) creates the world's first comprehensive legislation specifically for digital medical products, distinguishing it from software-agnostic frameworks. Korea approved 64 AI-enabled medical devices in 2023, with 85.9% domestically developed.
- India's AI regulatory landscape is accelerating under the Digital India Act and IndiaAI Mission, with the Central Drugs Standard Control Organization (CDSCO) developing early guidance for AI/ML-enabled medical devices and digital health tools (CDSCO, 2025).
- Taiwan's Food and Drug Administration's (TFDA) Priority Review Program for Medical Devices. TFDA implemented revised AI medical device technical guidelines in August 2025, targeting Class II and III AI/ML Computer-Aided Detection (CADe) and Computer-Aided Diagnosis (CADx) devices, with emphasis on independent performance evaluation and algorithm change management. Taiwan's Information and Communication Technology medical convergence strategy positions it as a high-precision manufacturing hub for AI-enabled medical devices, complementing established semiconductor leadership.

For Asia-Pacific entry, sponsors can benefit from starting in markets that provide accelerated regulatory pathways that can serve as springboards to the wider region. For example, sponsors can leverage Singapore's expedited approval pathways and Taiwan's Priority Review Program for Medical Devices to establish clinical performance data, then cascade approvals through other members of the Association of Southeast Asian Nations' (ASEAN) mutual-recognition agreements before tackling China's more intensive NMPA requirements or India's emerging frameworks.

Saudi Arabia leads the Middle East in AI frameworks

The Saudi Food and Drug Authority (SFDA) has pioneered binding AI/ML requirements through MDS-G010 Guidance

on Artificial Intelligence (AI) and Machine Learning (ML) technologies-based Medical Devices, incorporating adapted forms of non-AI guidelines into a cohesive AI-specific framework, positioning the Kingdom for Vision 2030 healthcare modernisation objectives (Solaiman, 2024).

It is also notable that Saudi Arabia's network-authentication rules and Singapore's four-tier Cybersecurity Labelling Scheme stand out as leading examples of emerging post-market cybersecurity requirements. Companies architecting cybersecurity-by-design during the development phase will achieve faster market access and premium positioning as these requirements cascade across Asia-Pacific and Middle East markets.

Brazil as Latin America's regulatory anchor

As Latin America's regulatory anchor, Brazil continues to shape regional standards, with ANVISA's 2024–2025 agenda focused on revising SaMD requirements and strengthening IMDRF harmonisation. Existing frameworks, including RDC 657/2022 and RDC 751/2022, already establish clear guidance for SaMD developers that is aligned with international standards, such as IMDRF.

Table 1: Global AI and DTx Comparative Framework Summary

Dimension	United States	European Union	United Kingdom	Japan	South Korea	China	Singapore	Saudi Arabia	Brazil	Taiwan
Core SaMD Regulation	FD&C Act; 21 CFR 800-898	MDR 2017/745 (Rule 11)	UK MDR (MDR-aligned)	Pharma-ceuticals and Medical Devices Act	Digital Medical Products Act (January 2025)	NMPA Class II/III pathways	HSA Medical Device Act	SFDA MDS-G010	ANVISA RDC 657/2022; RDC 751/2022	TFDA Medical Device Act
AI Gover-nance	PCCP (FD&C §515C); Good Machine Learning Practice for Medical Device Development principles; January 2025 lifecycle guidance	EU AI Act (high-risk category Annex III)	Transitional AI proposals (2024 consultation)	AI Promotion Act 2025; PMDA AI Guidelines	Digital products-specific framework (world's first)	NMPA AI device approval pathway	Change Manage-ment Program for ML-enabled SaMD	MDS-G010 binding AI/ML requirements	IMDRF-aligned SaMD framework	Class II/ III AI/ML CADe/CADx guidelines (August 2025)
Generative AI Readiness	November 2025 DHAC guidance expected	AI Act imple-mentation ongoing	Sandbox programmes piloting	Non-binding framework	Specialised digital legislation	Rapidly evolving	ASEAN harmonisa-tion leadership	Vision 2030 AI integration	Framework revision 2024–2025	ICT-medical convergence strategy
Cyber-security	FD&C §524B; FDA 2023 guidance	EU Cyber Resilience Act; International Electro-technical Commission (IEC) 62304	MHRA 2024 guidance	IEC 62304/ ISO 14971 alignment	Digital Products Act provisions	Emerging framework	IEC 62304 alignment	EU MDR/ IVDR-aligned	ISO 13485 alignment	IEC 62304 alignment
Post-Market Surveil-lance	Voluntary real-world monitoring; MDR/annual reports	Mandatory Post-Market Clinical Follow-up; Periodic Safety Update Reports; surveillance plans	MDR-aligned + agile pilots	Intensive re-examination; domestic data emphasis	Digital product-specific monitoring	Mandatory post-market	Perform-ance evaluation required	Vision 2030-aligned surveillance	Post-market vigilance require-ments	Algorithm change-management emphasis
Evidence Standards	Flexible (RWE permitted); <2% require Randomised Controlled Trials (RCTs)	Prescriptive Clinical Evaluation Reports	MDR-aligned	Highest rigour; domestic data preferred	Digital-specific validation	Domestic data emphasis	RWE acceptance	International standards-aligned	IMDRF-aligned evidence	Independent performance evaluation

Dimension	United States	European Union	United Kingdom	Japan	South Korea	China	Singapore	Saudi Arabia	Brazil	Taiwan
Approval Timeframe	Fastest (510(k) 90 days; De Novo 150 days)	Longest (MDR 1–2+ years)	Moderate (transitional)	Moderate-Long (re-examination adds years)	Moderate (new framework establishing)	Moderate-Fast (64 approvals/ 2023)	Fast (ASEAN efficiency leader)	Moderate (Vision 2030 acceleration)	Moderate (ANVISA modernisation)	Moderate (August 2025 guidelines new)

Developing Clinical Evidence for Regulators in DTx and AI-enabled Devices

The design of clinical evidence, including real-world data and clinical trials, is critical to bringing any DTx device or SaMD to market. DTx and AI-enabled medical devices represent an evolving class of software-based interventions that require rigorous clinical validation to demonstrate safety and effectiveness. Unlike traditional medical devices with established validation paradigms, DTx clinical trial design faces unique methodological challenges related to blinding, control selection, engagement measurement, and the integration of RWE into regulatory decision-making.

AI-enabled medical devices introduce additional complexity beyond traditional DTx, particularly for continuously learning algorithms that adapt based on new data inputs. The FDA's January 2025 draft guidance on "Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations" emphasises the need for novel trial designs that accommodate the total product lifecycle of AI systems, proposing recommendations for design, development, and implementation throughout the device lifecycle to support FDA's evaluation of safety and effectiveness (FDA, 2025c). Unlike locked algorithms whose decision logic remains fixed, continually learning systems perform lifelong learning where mathematical models update through new data while retaining previously learned knowledge – a technique that introduces unique validation challenges since traditional premarket testing may not adequately predict post-market performance as the algorithm evolves (Benjamens *et al.*, 2020). The current linear paradigm of AI deployment has largely failed to keep pace with technological development, particularly for interactive, adaptive, multi-agent AI systems that can substantially change behaviour through mechanisms like Reinforcement Learning from Human Feedback (RLHF) and in-context learning without necessarily updating model parameters (Wang *et al.*, 2025).

To address the critical question of when continuously learning AI/ML SaMD may require premarket submission for algorithm changes, FDA introduced the PCCP framework, which includes SaMD Pre-Specifications defining anticipated modifications to performance, inputs, or intended use, and Algorithm Change Protocols specifying the methodology to implement changes while managing patient risks (Benjamens *et al.*, 2020). The PCCP describes specific changes limited to modifications within the intended use of the original device, with methods and metrics that are scientifically and clinically justified in proportion to risk, along with evidence demonstrating benefits and risks before and after implementation (FDA, Health Canada, and MHRA, 2023). However, critical gaps remain in performance evaluation methods for frequently updated ML algorithms, particularly regarding two common scenarios: preventing performance decay over time due to shifts in clinical practice patterns or patient characteristics; and enabling rapid successive modifications without assembling new test datasets for each change (FDA, 2024c).

Novel trial designs for AI-enabled devices

Adaptive and Multi-Arm Multi-Stage (MAMS) designs

AI-enabled device trials increasingly employ adaptive designs that allow modification of trial parameters based on accumulating data (Khan *et al.*, 2025). Response-adaptive randomisation shifts allocation probabilities toward better-performing AI models during enrolment, while enrichment strategies allow patient selection criteria to evolve based on predictive biomarkers or algorithmic performance subgroups, and dose-finding approaches titrate the frequency, complexity, or personalisation depth of AI recommendations. MAMS designs enable efficient comparison of multiple AI algorithm variations against control conditions, incorporating futility stopping rules for underperforming approaches and seamless progression pathways for successful candidates, thereby maximising the information gained from each trial participant while minimising exposure to inferior interventions.

Observer performance studies

For AI diagnostic and decision support systems, observer performance studies compare clinician diagnostic accuracy or treatment selection with and without AI assistance, addressing the critical question of whether AI improves clinical decision-making in real-world practice (Song *et al.*, 2025). However, evidence demonstrating clinician improvement remains remarkably limited – as of 2024, analysis of FDA-cleared devices reveals that clinical performance studies were reported for only 55.9% of approved devices, with most using retrospective rather than prospective designs, and only 2.4% employing randomised clinical trials (Windecker *et al.*, 2025). Robust observer performance studies require reader study protocols with multiple clinicians interpreting cases with and without AI, crossover or parallel designs to control for case difficulty and individual reader variability, prespecified performance metrics including sensitivity, specificity, reading time, and inter-rater agreement, and real-world case mix reflecting actual clinical population diversity that ensures generalisability beyond curated research datasets.

Non-inferiority designs for AI substitution

When AI systems are intended to fully replace human decision-making (e.g., autonomous diabetic retinopathy screening), non-inferiority trials establish that AI performance meets acceptable thresholds compared to clinician standards. Of five non-inferiority DTx trials analysed, three successfully established equivalence between standalone AI and clinician decision-making (Abbasgholizadeh-Rahimi *et al.*, 2024).

Table 2: Trial Design Considerations: Comparative Analysis

Trial Design	Primary Use Cases	Key Advantages	Key Limitations	Recent Evidence
RCT – Standard-of-Care Control	DTx targeting conditions with established treatments; health economic evaluations	Gold standard for comparative effectiveness; regulatory acceptance well-established; enables reimbursement decision-making	Does not control for expectation effects; limited blinding achievable; may show smaller effect sizes *vs.* sham	67.5% of completed DTx trials use RCT design; remains regulatory preference for approval pathways
RCT with Sham Comparator	DTx with subjective endpoints (Patient-Reported Outcomes (PROs), behavioural symptoms); breakthrough device designation	Controls for placebo/expectation effects; enables blinding (participant-level); demonstrates specific DTx efficacy	Ethical concerns in chronic disease management; complex sham design for interactive DTx; may require larger sample sizes	Most rigorous comparator for subjective outcomes; required by FDA for certain De Novo pathways
RCT with Attention Control	Behavioural health DTx; interventions with significant engagement components	Controls for attention and engagement effects; provides active intervention to all participants; ethically acceptable alternative to sham	Does not fully control for expectation; credibility may differ from true sham; content development resource-intensive	Commonly used in mental health DTx trials; bridges gap between sham and standard of care
Waitlist Control/ Delayed Access	Prevention-focused DTx; conditions with no urgent treatment need	All participants eventually receive intervention; addresses ethical recruitment concerns; can assess sustained effects in crossover phase	Anticipation effects in waitlist group; limited follow-up duration; dropout rates higher in waitlist arm	Ethical alternative gaining adoption in prevention trials; 9.4% of DTx trials focus on prevention
Non-Inferiority Design	AI systems intended to replace clinician decision-making; autonomous diagnostic devices	Establishes AI as acceptable alternative; enables autonomous device approval; can demonstrate cost-effectiveness	Requires consensus on non-inferiority margin; regulatory acceptance varies by condition; may not capture all failure modes	Five of 86 AI RCTs employed non-inferiority; three successfully established equivalence to clinicians
Observer Performance Study	AI diagnostic support systems; clinical decision support DTx	Assesses real-world clinician improvement; captures AI–human collaboration dynamics; regulatory preference for Class III AI	Reader studies expensive and time-intensive; results highly protocol-dependent; limited generalisability	Only 7.77% of FDA-cleared AI devices included such studies as of 2024; FDA increasingly requiring
Adaptive/ MAMS Design	Multiple AI algorithm variants; dose-finding for DTx intensity	Efficient comparison of multiple interventions; enables mid-trial optimisation; reduces sample size requirements	Complex statistical analysis required; regulatory pathway less established; requires sophisticated trial infrastructure	Emerging in AI trials; particularly valuable for continuous-learning algorithms
Decentralised Clinical Trial (DCT)	DTx interventions requiring diverse populations; home-based usage assessment	40–50% faster recruitment; representative demographic sampling; real-world effectiveness data	Engagement dropout rates 30–50%; remote monitoring challenges; regulatory acceptance varies by geography	41 DTx DCTs reviewed in 2025; model particularly suited to DTx characteristics
Registry/RWE Study	Post-market surveillance; expanded population assessment; label expansion	Large-scale effectiveness data; heterogeneous population representation; cost-effective *vs.* traditional trials	Confounding and selection bias risks; missing data and inconsistent measurement; regulatory acceptance pathway evolving	FDA RWE framework enables DTx label expansion; AI reduces adverse event detection time from 90 days to 14 days
Pragmatic Trial	Effectiveness in routine clinical practice; health system implementation	High external validity; minimal eligibility restrictions; integration with clinical workflows	Reduced internal validity *vs.* explanatory trials; complex site coordination; limited mechanistic insights	Gaining traction for DTx integration studies; aligns with FDA effectiveness endpoints

Control arm selection

Like the requirement of a placebo arm in drug trials, devices often require the use of a sham comparator: a device that creates the expectation of improvement and allows a similar device experience for the patient without conferring a therapeutic benefit.

In non-AI based DTx, shams have taken one of two forms: either they provide a therapeutically inert version of the DTx itself in cases where the DTx is a computerised task like cognitive training, with the internal mechanics changed to eliminate clinical effect (e.g. Click Therapeutic's Mirai pivotal trial or Akili's pivotal trial featured true "sham devices" that otherwise resemble the true device in every way), or in the case of DTx designed to teach therapeutic skills via educational pathways, psychoeducational apps with similar amounts of

content have been used (e.g., Big Health's trial for Daylight features a strong attentional control that is an app, and creates expectation of improvement, but does not exactly resemble the true device). Designing the appropriate sham control group for an AI-enabled device is a challenge that FDA acknowledged during the 2025 DHAC meeting. The more interactive and adaptive a product is, the harder it is to give patients a similar experience without driving therapeutic benefit.

The US is unique in its requirement of a sham comparator for digital health products, but other jurisdictions require rigour in different ways. For example, in the EU, device manufacturers provide periodic reporting of clinical performance data after-market authorisation, while companies in the US do not, unless specifically required during the authorisation process. China, Japan, and India increasingly require domestic clinical data despite accepting foreign approvals for expedited pathways. Regulatory strategies for DTx must address the clinical evidence portfolio strategy, balancing pivotal US/EU trials with targeted emerging market studies to optimise global approval timelines.

Sham comparators

The use of sham comparators, interventions designed to control for expectation effects while providing no therapeutic benefit, has become increasingly sophisticated in DTx development. Sham controls are essential when primary endpoints are subjective (PROs, symptom scales), blinding is feasible through matched user interfaces and interaction patterns, expectation effects are substantial (behavioural health, pain management, cognitive training), or regulatory guidance requires placebo-controlled evidence (breakthrough designation, *de novo* pathways). During the DHAC meeting, FDA reinforced its expectation that AI-enabled therapeutic products use sham comparators, but noted significant design challenges: sham controls must be credible to patients who should not be able to discern they have received an inactive therapy. This requirement becomes particularly complex for AI-enabled DTx where creating convincing yet therapeutically inert experiences presents both a methodological challenge and a competitive advantage for companies that can establish validated sham protocols early, effectively setting industry standards.

Design strategies for DTx sham comparators employ several validated approaches. Matched interaction designs provide similar engagement patterns, notification frequency, and interaction time as the active DTx while eliminating specific therapeutic content or behavioural-change techniques, such as cognitive training tasks without progressive difficulty calibration, educational content delivery without evidence-based therapeutic frameworks (e.g., Cognitive Behavioural Therapy (CBT) restructuring, motivational interviewing), or gamification elements without behaviour change theory integration. Attention control designs deliver digital content matched for frequency and modality but lacking disease-specific therapeutic elements, thereby controlling for general attention and engagement effects, expectation of improvement from digital health participation, and time and effort invested in app interaction. Waitlist or delayed access controls, while not true shams and not acceptable to FDA as a substitute for a sham, allow all participants to eventually receive the intervention while maintaining a control period for comparison, addressing ethical concerns in chronic disease management but introducing potential bias from anticipation effects. These types of designs can be valuable for initial pilot studies, or, with a crossover component where all patients receive both the device and the sham, can provide a novel methodology for evaluating placebo effects without withholding treatment from control. While there is some precedent for crossover designs for FDA submissions, they are more novel and should be discussed with the Agency in advance, if utilised.

Standard-of-care and active controls

The selection of appropriate control arms in DTx trials depends critically on the therapeutic context, available treatment alternatives, and regulatory pathway. For DTx targeting conditions with established treatments, head-to-head comparisons against standard of care demonstrate incremental benefit and inform coverage decisions, as well as applications for Breakthrough Device Designation in the US. These types of active controls, in contrast, are particularly appropriate when established efficacy standards exist for the condition, denying treatment would be unethical, the DTx is intended to augment rather than replace existing care, or health economic analyses require direct cost-effectiveness comparisons. Active control designs dominated early DTx trials, with 52.5% focused on disease management and 38.1% on treatment, reflecting the practical reality that many DTx interventions are delivered alongside conventional therapies (Yao *et al.*, 2024). However, in recent years, FDA has very frequently required novel DTx interventions to first demonstrate superiority over a sham comparator (see below), in isolation or alongside standard of care (i.e., as an adjunct), with follow-on studies to demonstrate non-inferiority with or superiority over standard of care coming later.

Challenges in DTx blinding

Unlike pharmaceutical placebos, DTx interventions present unique blinding challenges that complicate traditional trial designs (Miao *et al.*, 2024; Scherer *et al.*, 2025). Users may recognise therapeutic content such as CBT modules or behavioural activation protocols even in modified forms, while true therapeutic DTx often require sustained engagement patterns that differ from control conditions. Community effects through online forums and social media discussions may reveal intervention details, and clinicians delivering concurrent care may be able to infer assignment based on patient reports. Recent analysis of 449 DTx trials revealed that traditional double-blind designs are rarely achievable, with most studies employing single-blind (participant) or open-label approaches (Miao *et al.*, 2024). FDA nevertheless expects double-blindness, reinforcing the necessity of discussing study designs with FDA in pre-submission meetings, before the research is conducted.

PCCPs

A significant regulatory innovation for AI devices at FDA is the PCCP framework, finalised in December 2024, which allows manufacturers to specify planned modifications to AI algorithms without requiring new premarket submissions. Pursuing this framework offers substantial strategic advantages for AI device manufacturers by reducing time-to-market for improvements and enabling more agile responses to gathered real-world performance data.

When manufacturers can apply their original verification and validation processes to a predefined list of new functionalities or modifications, the PCCP pathway is relatively straightforward. The manufacturer and FDA simply need to reach agreement on the scope of changes and the validation approach during the initial submission review. This predictability allows manufacturers to plan their product development roadmap with greater confidence, knowing that certain

categories of improvements can be implemented without the uncertainty and delay of traditional premarket review cycles.

The framework becomes more complex when companies propose novel validation methodologies that differ from their original premarket testing. For instance, if a manufacturer's original validation relied on clinical data but they later wish to use synthetic data or alternative testing paradigms for validating modifications, FDA must evaluate whether these new methods provide equivalent assurance of safety and effectiveness.

Leveraging the PCCP framework to its full potential requires strategic planning that extends beyond immediate product needs. Manufacturers should consider the full spectrum of potential algorithm modifications during initial submission, or as a 510(k) subsequent to their initial authorisation. While modifications that would affect the intended use of the device are generally not appropriate for a PCCP, there are many other modifications that can be included outside of the generic "retrain model with new data". Some examples include changes to performance thresholds, expansion to adjacent patient populations, and integration of new data modalities. Defining these modification categories broadly while still maintaining sufficient specificity for FDA review provides maximum flexibility for future development. Organisations that treat PCCP development as a strategic opportunity are better positioned to fully capitalise on the framework's potential to accelerate innovation while maintaining regulatory compliance.

Post-market Surveillance Requirements for AI-enabled Devices

Unlike static medical technologies, AI systems may experience performance degradation due to data drift, evolving clinical practice patterns, or shifts in patient populations over time (Finlayson *et al.*, 2021; Chen *et al.*, 2023). Establishing robust post-market performance monitoring is essential to ensure these devices maintain safety and effectiveness throughout their clinical lifecycle, particularly as many AI-enabled devices pursue PCCPs that enable continuous learning and adaptation (Hwang *et al.*, 2022).

The FDA currently lacks formal guidance on post-market surveillance of AI-enabled devices but recently released a Request for Comment docket titled "Measuring and Evaluating AI-enabled Medical Device Performance in the Real-World", signalling forthcoming regulatory expectations. Several recurring themes have emerged from stakeholder comments that will likely frame these regulations. First, manufacturers must establish predefined performance thresholds that trigger graduated safety responses when real-world performance declines below acceptable levels, ranging from output warnings to device suspension or algorithm retraining (Sendak *et al.*, 2020). Second, comprehensive monitoring programmes must evaluate multiple dimensions beyond algorithmic outputs alone, including patient population drift, user interaction patterns, automation bias among clinicians, and technical environment changes that could impact device performance (Wu *et al.*, 2021; Beede *et al.*, 2020). Third, there is growing consensus that manufacturers should publicly report monitored metrics and results at regular intervals to enable regulatory oversight and create accountability throughout the device lifecycle (Vasey *et al.*, 2022).

The appropriate balance between human oversight and automated evaluation in post-market monitoring remains contested. The Johner Institute proposes that humans should define performance metrics and evaluation methods while automation handles data gathering and enables scalable, reproducible assessments (Johner Institute, 2023). This balanced approach aligns with FDA's historical preference for human-centred oversight in safety-critical medical device applications.

Strategic Approaches to Regulatory Interactions

Clinical evidence development for DTx and AI-enabled devices demands methodological innovation that extends beyond traditional pharmaceutical trial paradigms, driven increasingly by evolving regulatory science initiatives across major health authorities. The FDA's finalisation of its PCCP guidance in December 2024 signals a fundamental shift toward lifecycle-based regulation that accommodates continuous algorithm improvement, while the EU's AI Act establishes the first comprehensive regulatory framework classifying certain medical AI systems as "high-risk", requiring conformity assessments that exceed traditional MDR requirements. Parallel initiatives from the UK's MHRA Software and AI Change Programme, Japan's PMDA "DASH for SaMD" accelerated review pathways, and Health Canada's emphasis on algorithmic transparency reflect both growing international harmonisation through the IMDRF Working Group on AI/ML and persistent regulatory divergence in post-market surveillance expectations, RWE acceptance criteria, and bias assessment requirements. As regulatory science capabilities mature globally, manufacturers must recognise that regulatory pathway-optimisation and evidence-generation strategies increasingly represent sources of competitive advantage rather than mere compliance obligations, the optimal clinical trial design for any DTx now depends not only on therapeutic mechanism and clinical context but also on sophisticated regulatory intelligence regarding which health authorities will accept decentralised methodologies, adaptive designs, RWE, and AI-enhanced trial operations as sufficient demonstration of safety and effectiveness in this rapidly transforming landscape.

Emerging trends and challenges in DTx clinical development

The FDA's Digital Health Center of Excellence has established increasingly rigorous standards for DTx evidence generation, emphasising that clinical trials must demonstrate not only statistical significance but also clinical meaningfulness through improvements in how patients feel, function, or survive (FDA, 2023). Contemporary guidance prioritises objective outcome measures such as validated performance tests, clinician-rated scales, and biomarkers over PROs alone (Kim *et al.*, 2024). Furthermore, regulatory expectations now emphasise function-based endpoints that reflect real-world patient benefit beyond symptom score improvements, durability of effect through extended follow-up periods that extend beyond the active intervention phase, and comprehensive safety monitoring appropriate to each product's risk profile, including mental health surveillance for behavioural health DTx (Mathews *et al.*, 2019; Nebeker *et al.*, 2023).

However, significant challenges remain in ensuring DTx evidence meets these evolving standards while addressing fundamental questions of algorithmic generalisability and bias. A comprehensive cross-sectional analysis of 903 FDA-approved AI-enabled medical devices as of August 2024 revealed substantial gaps in clinical validation: clinical

performance studies were reported for only 55.9% of approved devices; sex-specific performance data appeared in fewer than one-third of submissions; and age-related subgroup analyses were conducted in only one-quarter of evaluations (Windecker *et al.*, 2025). Perhaps most concerning, retrospective study designs dominated the evidence base at 38.2%, while randomised controlled trials accounted for merely 2.4% of submissions. These findings underscore an urgent need for prospective, diverse, and inclusive DTx trial designs that systematically assess performance across demographic subpopulations, socioeconomic contexts, and real-world clinical settings (Rajkomar *et al.*, 2018; Obermeyer *et al.*, 2019). The medtech industry must proactively address these evidence gaps to ensure that DTx deliver equitable health benefits across all patient populations rather than inadvertently perpetuating or amplifying existing healthcare disparities.

Optimising regulatory pathways across jurisdictions and engaging early

Early engagement with regulators is especially valuable in contexts where a device has a novel technology or usage. FDA's pre-submission meetings (through the Q-Submission process) prompt the Agency to consider scientific expert insights and interpretation of policy, regulation, and guidance documents for innovative products. Other regulatory agencies, such as Health Canada, Australia's Therapeutic Goods Administration, Japan's PMDA, and the UK's MHRA, also offer consultative meetings similar to FDA's pre-submission process. Additionally, FDA's innovation programmes, pilot programmes, and transparency initiatives, including public meetings, advance notice of draft guidance, and open-comment periods, create opportunities for manufacturers to engage with experts at FDA.

Multi-jurisdictional regulatory pathway optimisation enables companies to build a coordinated global strategy that sequences, bundles, and harmonises submissions across key markets to accelerate approval and reduce redundant evidence generation. For DTx and AI-enabled devices, this approach is essential for navigating divergent regulatory expectations while sustaining rapid iteration and global market momentum. By prioritising early "evidence-anchor" jurisdictions, sponsors can generate clinical and analytical performance data that can be leveraged through reliance, recognition, or abridged review pathways in subsequent markets. This creates cross-regional alignment in clinical evidence, AI/ML change-management, and post-market surveillance requirements, resulting in a more predictable and efficient commercialisation route.

Given the substantial differences in review timelines worldwide, strategic sequencing is critical. Sponsors often pursue US clearance first (frequently via a 510(k) with a PCCP) to enable rapid market entry and early real-world data generation. That evidence can then be used to support EU CE marking under MDR's clinical-evaluation obligations, followed by staged entry into the UK, Asia-Pacific, and other regions based on local data needs, reliance opportunities, and the developer's geographic footprint. This sequencing maximises regulatory leverage while minimising duplicative clinical-evidence requirements across global markets.

Regulation, strategy, and the future of AI-enabled SaMD devices

While LLMs are at the forefront of modern discourses and regulatory discussions, technology in both learning-enabling middleware software (i.e., memory systems and cognitive architectures) and alternative AI technologies is evolving rapidly. Sustained engagement with the evolving AI architecture landscape, beyond the quadratic-complexity attention mechanisms dominating current LLM regulatory conversations, will be essential for developing validation frameworks with lasting relevance to future AI technologies, including orchestrated deployment of SLMs, SSMs, liquid neural networks, GNNs, neuro-symbolic hybrids, and others.

Table 3: Regulatory Challenges for Current and Developing AI Technologies in MedTech

Architecture Type	Description	Medical/Therapeutic Relevance	Regulatory Challenge
LLMs	Transformer-based, quadratic-complexity attention, billions of parameters	Clinical documentation, diagnostic support, literature synthesis, patient communication	Current regulatory focus; PCCP addresses weight updates but assumes training-centric learning paradigm
SLMs/ Orchestrated Systems	Task-specific models coordinated via middleware, retrieval augmented generation (RAG), and agentic tooling	Modular clinical workflows, resource-constrained deployment, specialised diagnostic pipelines	Regulatory salience shifts to orchestration layer; system behaviour emerges from middleware logic, not model weights, and may be more difficult to regulate at scale
SSMs	Linear-complexity sequence modelling (i.e., Mamba)	Long-context patient records, continuous monitoring	Different failure modes than transformers, many risks are yet unknown
Receptance Weighted Key Value/ Extended Long Short-Term Memory	Recurrent architecture revival with linear scaling	Streaming physiological data, real-time monitoring	Temporal dependencies behave differently, observability faces new challenges
MoE	Sparse networks activating only relevant "experts"	Specialist routing for differential diagnosis	Which expert activated? Explainability challenges
Kolmogorov-Arnold Networks	Learnable activation functions	Potentially superior interpretability	Too new for any regulatory framework, but poses interesting challenges for the future

Architecture Type	Description	Medical/Therapeutic Relevance	Regulatory Challenge
Liquid Neural Networks	Continuous-time, adaptive	Wearables, adaptive dosing, implantables	Continuously changing weights, how do you validate?
GNNs	Relational/molecular structure reasoning	Drug discovery, protein interaction, molecular design, particle and wave modelling	Validation paradigms completely different from natural language processing
Diffusion Models	Iterative denoising/generation	Molecular generation, drug design, medical imaging	Generative validation *vs.* discriminative
Neuro-symbolic Hybrids	Neural + symbolic reasoning	Clinical decision support with explainable logic	Which component do you validate?
Spiking Neural Networks	Neuromorphic, event-driven	Edge/implantable devices, low-power medical AI	Timing-dependent behaviour, novel failure modes

Critically, regulatory frameworks must also address a fundamental misconception: that AI system behaviour is determined primarily by model training or fine-tuning, such as by RLHF. In commercially deployed systems, behavioural adaptation occurs predominantly through middleware orchestration, RAG indices, prompt engineering, and agentic tool-use configurations, none of which modify model weights, yet all of which substantively alter system outputs and risk profiles in medical use cases.

Regulatory science that anticipates architectural heterogeneity across recurrent, sparse, neuromorphic, and hybrid symbolic-connectionist paradigms, as well as compositional systems orchestrating task-specific SLMs through increasingly sophisticated middleware, rather than optimising for transformer-specific assumptions about weight stability, inference determinism, and gradient-based interpretability, is better positioned to accommodate the field's trajectory toward sub-quadratic alternatives, adaptive continuous-time systems, and multi-model agentic architectures. These evolving technologies in AI offer unprecedented opportunities and also will continue to challenge existing regulatory and development paradigms.

Concluding strategic summary

The most successful DTx regulatory strategies architect clinical-evidence generation around core regulatory questions that span jurisdictions, including algorithmic fairness across patient populations, real-world effectiveness in heterogeneous clinical settings, and safety signal detection sensitivity. Clinical study designs incorporating built-in RWE collection, diverse population recruitment, and long-term follow-up create regulatory assets reusable across multiple applications and jurisdictions.

The regulatory landscape for AI-enabled DTx will continue evolving rapidly, alongside the underlying technology. Medical device developers who view this as a strategic opportunity rather than compliance uncertainty, and who invest in sophisticated regulatory intelligence capabilities, will disproportionately capture market value as frameworks mature. While the current focus of AI development is on frontier LLM capabilities, we also note rapid evolution in both learning middleware software and other AI technologies that will challenge regulation and developers in the future.

We are at an inflection point for generative AI mental health devices. FDA guidance incorporating November 2025 DHAC recommendations will codify expectations around crisis escalation protocols, performance benchmarking to human therapist standards, and population-specific validation. Simultaneously, post-market requirements are intensifying – expect mandated continuous algorithm performance monitoring (FDA, 2025b), bias/equity surveillance across demographic subgroups, and safety signal detection for generative AI failure modes.

Additionally, evidence standards are rising sharply for reimbursement: the US Centers for Medicare & Medicaid Services and commercial payers increasingly require head-to-head comparisons to standard of care, outcomes-based risk-sharing contracts, and DTx formulary evaluations paralleling pharmaceutical pathways. Companies that craft their regulatory and clinical evidence strategies accordingly will achieve sustainable competitive advantage over those treating regulatory compliance as an afterthought.

References

Abbasgholizadeh-Rahimi S., Mendis S., Nouri R., *et al.*, (2024). Randomised controlled trials evaluating artificial intelligence in clinical practice: a scoping review. doi:10.1016/S2589-7500(24)00047-5

Beede, E., Baylor, E., Hersch, F., *et al.*, (2020). A Human-Centered Evaluation of a Deep Learning System Deployed in Clinics for the Detection of Diabetic Retinopathy. https://doi.org/10.1145/3313831.3376718

Benjamens, S., Dhunnoo, P., & Meskó, B. (2020). The state of artificial intelligence-based FDA-approved medical devices and algorithms: an online database. https://doi.org/10.1038/s41746-020-00324-0

Bipartisan Policy Center. (November 12, 2025). FDA Oversight: Understanding the Regulation of Health AI Tools. https://bipartisanpolicy.org/issue-brief/fda-oversight-understanding-the-regulation-of-health-ai-tools

Central Drugs Standard Control Organization. (October 21, 2025). Draft Guidance Document on conduct of Medical Device Software under MDR, 2017. https://cdsco.gov.in/opencms/resources/UploadCDSCOWeb/2018/UploadPublic_NoticesFiles/Draft%20guidance%20document%20on%20Medical%20Device%20Software%2021%2010%202025.pdf

Chen, I. Y., Pierson, E., Rose, S., *et al.*, (2023). Ethical Machine Learning in Healthcare. https://pubmed.ncbi.nlm.nih.gov/34396058

China Center for Food and Drug International Exchange. (July 2025). Announcement of the National Medical Products Administration on Issuing Measures to Optimize Whole Life-Cycle Regulation in Support of the Innovative Development of High-End Medical Devices (No. 63, 2025). https://www.ccfdie.org/en/gzdt/webinfo/2025/07/1753823853775950.htm

Digital Therapeutics Alliance. (2023). DTAs Adoption & Interpretation of ISOs DTx Definition. https://dtxalliance.org/wp-content/uploads/2023/06/DTA_FS_New-DTx-Definition.pdf

Digital Therapeutics Alliance. (2021). DTx Product Categories (Fact sheet). https://dtxalliance.org/wp-content/uploads/2021/01/DTA_FS_DTx-Product-Categories_010521.pdf

European Parliament and Council. (2017). Regulation (EU) 2017/745 on Medical Devices (MDR). Official Journal of the European Union, L 117/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745

European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act). Official Journal of the European Union, L 1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Finlayson, S. G., Subbaswamy, A., Singh, K., *et al.*, (2021). The Clinician and Dataset Shift in Artificial Intelligence. https://doi.org/10.1056/NEJMc2104626

Han, R., Acosta, J.N., Shakeri, Z., Ioannidis, J.P.A., Topol, E.J., & Rajpurkar, P. (2024). Randomised controlled trials evaluating artificial intelligence in clinical practice: a scoping review. doi:10.1016/S2589-7500(24)00047-5.

Hargreaves, B. (February 2023). AI is enabling the rise of sophisticated digital therapeutics. Pharmaphorum. https://pharmaphorum.com/digital/ai-enabling-rise-sophisticated-digital-therapeutics

Health Sciences Authority. (December 1, 2024). Guidance on Change Management Program (CMP) for SaMD, including machine-learning enabled SaMD. https://www.hsa.gov.sg/docs/default-source/hprg-mdb/guidance-documents-for-medical-devices/gn-37-r1-guidance-on-change-management-program-%28cmp%29-for-samd-including-machine-learning-enabled-samd.pdf?sfvrsn=143fb54a_1

Hwang, T. J., Kesselheim, A. S., & Vokinger, K. N. (2022). Lifecycle Regulation of Artificial Intelligence- and Machine Learning-Based Software Devices in Medicine. https://doi.org/10.1001/jama.2019.16842

International Organization for Standardization. (2023). ISO/TR 11147:2023 Health informatics—Personalized digital health—Digital therapeutics health software systems. https://www.iso.org/standard/83767.html

International Medical Device Regulators Forum (IMDRF). (2014). Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations (IMDRF/SaMD WG/N12 FINAL:2014). https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations

International Medical Device Regulators Forum (IMDRF). (2025). Characterization Considerations for Medical Device Software and Software-Specific Risk (IMDRF/SaMD WG/N81 FINAL:2025). https://www.imdrf.org/sites/default/files/2025-01/IMDRF_SaMD%20WG_Software-Specific%20Risk_N81%20Final_0.pdf

Johner Institute. (2023). Comment on FDA-2023-N-2177.

Khan, S. (2025). AI in clinical trials in 2025: the edge of tech. Clinical Trial Risk Tool.

Kim, M., Patrick, K., Nebeker, C., Godino, J., *et al.* (2024). The digital therapeutics real-world evidence framework: An approach for guiding evidence-based digital therapeutics design, development, testing, and monitoring. doi:10.2196/49208.

Koller, C., Blanchard, M., & Hugle, T. (2025). Assessment of digital therapeutics in decentralized clinical trials: A scoping review. doi:10.1371/journal.pdig.0000905.

Liang, J., Fang, Q., Jiao, X., Xiang, P., Ma, J., Zhang, Z., Liu, Y., He, Y., Li, Y., He, Z., … & Lei, J. (2025). Approved trends and product characteristics of digital therapeutics in four countries. npj Digital Medicine, 8, Article 308. https://doi.org/10.1038/s41746-025-01660-9

Mathews, S. C., McShea, M. J., Hanley, C. L., *et al.*, (2019). Digital health: A path to validation. https://doi.org/10.1038/s41746-019-0111-3

Medicines and Healthcare products Regulatory Agency (MHRA). (2024). Digital health technologies: qualification and classification. UK Department of Health and Social Care. https://www.gov.uk/government/publications/digital-mental-health-technology-qualification-and-classification

Miao, B. Y., Sushil, M., Xu, A., Wang, M., Arneson, D., Berkley, E., Subash, M., Vashisht, R., Rudrapatna, V., & Butte, A. J. (2024). Characterisation of digital therapeutic clinical trials: a systematic review with natural language processing. *The Lancet Digital Health, 6*(3), e222–e229. https://doi.org/10.1016/S2589-7500(23)00244-3

Nebeker, C., Torous, J., & Bartlett Ellis, R. J. (2023). Building the case for actionable ethics in digital health research supported by artificial intelligence. https://pubmed.ncbi.nlm.nih.gov/31311535/

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. https://doi.org/10.1126/science.aax2342

Orrick. (November 11, 2025). FDAs Digital Health Advisory Committee Considers Generative AI Therapy Chatbots for Depression (Client Alert). https://www.orrick.com/en/Insights/2025/11/FDAs-Digital-Health-Advisory-Committee-Considers-Generative-AI-Therapy-Chatbots-for-Depression

Pear Therapeutics (2016). DE NOVO CLASSIFICATION REQUEST FOR RESET. https://www.accessdata.fda.gov/cdrh_docs/reviews/DEN160018.pdf

Pharmaceuticals and Medical Devices Agency (PMDA). (2025). AI promotion act implementation guidance for medical devices. Ministry of Health, Labour and Welfare. https://www.pmda.go.jp

Psychiatric Times. (November 13, 2025). FDA Committee Meets on Generative AI Digital Mental Health Devices. https://www.psychiatrictimes.com/view/fda-committee-meets-on-generative-ai-digital-mental-health-devices

Rajkomar, A., Hardt, M., Howell, M. D., *et al.*, (2018). Ensuring Fairness in Machine Learning to Advance Health Equity. https://doi.org/10.7326/M18-1990

Scherer M., Amati F., Chapuis A., *et al.*, (2025). Assessment of digital therapeutics... doi:10.1371/journal.pdig.0000905.

Sendak, M. P., Gao, M., Brajer, N., & Balu, S. (2020). Presenting machine learning model information to clinical end users with model facts labels. https://doi.org/10.1038/s41746-020-0253-3

Solaiman, B. (2024). Regulating AI-Based Medical Devices in Saudi Arabia: New Legal Paradigms in an Evolving Global Legal Order. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11250741/

Song J., Zhang Y., Liu L., *et al.*, (2025). Advancements in clinical evaluation... doi:10.1016/j.heliyon.2024.e40808.

U.S. Food & Drug Administration and Health Canada (2021). Good Machine Learning Practice for Medical Device Development: Guiding Principles. https://www.fda.gov/media/153486/download

U.S. Food & Drug Administration. (2025a). Digital Health Advisory Committee meeting: Generative AI-enabled digital mental health devices (Public meeting). https://www.fda.gov/advisory-committees/advisory-committee-calendar/november-6-2025-digital-health-advisory-committee-meeting-announcement-11062025

U.S. Food & Drug Administration. (2025b). Digital Health Advisory Committee; Notice of Meeting; Establishment of a Public Docket; Request for Comments—Generative Artificial Intelligence-Enabled Digital Mental Health Medical Devices (Docket FDA-2025-N-2338). Federal Register, 90(177). https://www.federalregister.gov/documents/2025/09/12/2025-17651/digital-health-advisory-committee-notice-of-meeting

U.S. Food & Drug Administration. (2025c). Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing

Submission Recommendations. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/artificial-intelligence-enabled-device-software-functions-lifecycle-management-and-marketing

U.S. Food & Drug Administration. (2024a). Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions (Final guidance). https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence

U.S. Food & Drug Administration. (2024b). Clinical Decision Support Software: Guidance for Industry and Food and Drug Administration Staff (Final guidance). https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software

U.S. Food & Drug Administration. (2024c). Safe Algorithmic Change Protocols for Modifications to AI/ML-based Software as a Medical Device. https://www.fda.gov/science-research/advancing-regulatory-science/safe-algorithmic-change-protocols-modifications-aiml-based-software-medical-device

U.S. Food & Drug Administration. (2023). Digital Health Technologies for Remote Data Acquisition in Clinical Investigations. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/digital-health-technologies-remote-data-acquisition-clinical-investigations

U.S. Food & Drug Administration, Health Canada, and MHRA. (October 24, 2023). Predetermined Change Control Plans for Machine Learning-Enabled Medical Devices: Guiding Principles. https://www.fda.gov/medical-devices/software-medical-device-samd/predetermined-change-control-plans-machine-learning-enabled-medical-devices-guiding-principles

U.S. Food & Drug Administration. (2025). Artificial Intelligence-Enabled Medical Devices. https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-enabled-medical-devices

Vasey, B., Nagendran, M., Campbell, B., *et al.* (2022). Reporting guideline for the early stage clinical evaluation of decision support systems driven by artificial intelligence: DECIDE-AI. https://doi.org/10.1136/bmj-2022-070904

Wang, X., Chen, L., & Zhang, Y. (2025). A decade of review in global regulation and research of artificial intelligence medical devices (2015–2025). https://doi.org/10.3389/fmed.2025.1630408

Windecker, S., Baj, G., Shiri, I., Kazah, P.M., Kaesmacher, J., Grani, C., & Siontis, G.C.M. (2025). Generalizability of FDA-approved AI-enabled medical devices for clinical use. doi: 10.1001/jamanetworkopen.2025.8052.

Wu, E., Wu, K., Daneshjou, R., *et al.* (2021). How medical AI devices are evaluated: limitations and recommendations from an analysis of FDA approvals. https://doi.org/10.1038/s41591-021-01312-x

Yao H., Liao Z., Zhang X., *et al.*, (2024). A comprehensive survey of the clinical trial Landscape on digital therapeutics. https://pubmed.ncbi.nlm.nih.gov/39224386



Dr. Acacia Parks is a seasoned digital health executive and consultant with over 20 years of experience navigating the intersection of behavioural science, clinical rigour, and global regulatory strategy. Her career has centred on bridging the gap between innovative technology and validated clinical evidence, ensuring that digital health solutions – ranging from general wellness apps to high-risk medical devices – are both safe and effective. Currently serving as VP of Regulatory Compliance & Engineering Services at Avania, Acacia provides strategic leadership for global regulatory jurisdictions, product development, and quality management systems. Her expertise is particularly sought after for complex products involving Software as a Medical Device (SaMD), AI-enabled tools, and Digital Therapeutics (DTx).

Avania B.V.
100 Crowley Drive, Suite 216
Marlborough, MA 01752
USA

Tel: +1 978 493 6843
Email: acacia.parks@avaniaclinical.com
LinkedIn: www.linkedin.com/in/acacia-parks-phd-mba-rac-3088ba5



Nick Butt is a medical device consultant specialising in the development and regulatory support of software-driven medical technologies, including both Software as a Medical Device (SaMD) and Software in a Medical Device (SiMD), across a broad range of device types and therapeutic areas. He has supported multiple medical device manufacturers in achieving U.S. FDA 510(k) clearance by developing comprehensive cybersecurity documentation from the ground up in alignment with current FDA guidance and international best practices. Nick has authored Predetermined Change Control Plans (PCCPs) that enable manufacturers to responsibly deploy post-market updates to AI-enabled medical devices while maintaining regulatory compliance, including plans that have achieved regulatory acceptance without review deficiencies.

Avania B.V.
100 Crowley Drive, Suite 216
Marlborough, MA 01752
USA

Tel: +1 508 351 8632
Email: nick.butt@avaniaclinical.com
LinkedIn: www.linkedin.com/in/nicholas-butt-53aa7a256



Sophia Farcas is an advisory strategy and operations lead at Avania with more than a decade of academic and professional experience in regulatory and engineering. She coordinates overall solution strategy, connecting clinical trials, commercial market access and reimbursement, regulatory strategy, and engineering services for medical devices, including bespoke solutions for LLM orchestration, training, and observability and monitoring.

Avania B.V.
100 Crowley Drive, Suite 216
Marlborough, MA 01752
USA

Tel: +1 508 351 8632
Email: sophia.farcas@avaniaclinical.com
LinkedIn: www.linkedin.com/in/sophiafarcas



Dr. Angela Johnson, RAC, drives breakthrough medical technology commercialisation as Senior Vice President of Advisory Services at Avania, leveraging 25+ years of regulatory strategy expertise across FDA, EU MDR/IVDR, and Asia-Pacific markets. She has guided global teams at Cytiva (Danaher), GE Healthcare, and IQVIA, and led regulatory functions for multiple VC-backed companies through successful IPOs and strategic exits, with focus on combination products, digital health, cell and gene therapy, and AI-enabled devices. Her current work centres on the convergence of AI governance, cybersecurity, and medical device product development, including practical frameworks for deploying agentic AI systems within regulated industries per EU AI Act human oversight requirements and FDA's evolving SaMD guidance.

Avania B.V.
100 Crowley Drive, Suite 216
Marlborough, MA 01752
USA

Tel: +1 508 351 8632
Email: angela.johnson@avaniaclinical.com
LinkedIn: www.linkedin.com/in/ajohnsonresearch

Your Trusted MedTech Partner
When breakthrough medical technologies hold the promise of transforming patient care, the journey from concept to commercialisation demands more than traditional CRO services. It requires a partner who understands the distinct challenges of medtech innovation, one who combines deep expertise with collaborative commitment to your success. That partner is Avania.
As the only global CRO built for MedTech, Avania is purpose-designed to navigate the complexities of medical devices, diagnostics, and combination products. We offer comprehensive, flexible solutions that reduce risk and accelerate your product's path to market.

Medical device development involves challenges unlike any other sector: intricate regulatory pathways; demanding clinical trial designs; and specialised engineering considerations.

www.avaniaclinical.com

Avania
MedTech's Trusted Champion

Austria



Dr. Daniel Larcher



Dr. Mariella Rieder

ATLAS Attorneys at Law
Prewave GmbH

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

In Austria, there is no standalone legal or industry definition of "Digital Health" (DH) or "eHealth".

DH refers to the use of information and communication technologies, software, and data to prevent, diagnose, treat, and monitor disease, and to support health system management, including big data and AI. The term "eHealth" traditionally focuses on telematics and infrastructure.

As of 2026, the DH landscape is primarily shaped by the eHealth Strategy 2024–2030 and the planned integration of the European Health Data Space (EHDS). The eHealth Strategy Austria and the Digital Austria Act embed DH in the broader digital transformation of healthcare, covering electronic health records (ELGA), telemedicine, and DH applications.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

- Telemedicine and remote care (virtual consultations, telemonitoring and home monitoring).
- Electronic health records, eHealth infrastructure (ELGA, e-medication, electronic vaccination record) and applications for disease management.
- AI-supported diagnostics and clinical decision support (e.g. imaging, triage).
- Consumer health apps and wearables (health data collection, mental health and lifestyle).
- Health data platforms and analytics.
- Cybersecurity in healthcare.

1.3 What is the digital health market size for your jurisdiction?

The Austrian DH market has been growing steadily, with momentum boosted by post-COVID-19 infrastructure investments. Excluding digital fitness and well-being (around 55% of the broader DH market), it was estimated at about US$600 million in 2024 and roughly US$720 million in 2025.

Based on sector growth expectations (STATISTA) and European trends (where DH markets often grow at 18–22% annually), Austria's DH market could reach approximately US$790–860 million in 2026 if it grows at a conservative 15% per year from the 2024 base. These figures are indicative only and will depend on implementation success and the wider economic environment.

Public-sector DH initiatives (such as ELGA) are substantial in Austria but are often not fully reflected in commercial market estimates. Overall, the market is expected to continue expanding at double-digit annual rates (roughly 10–20% per year) at least through 2029, supported in particular by Austria's eHealth Strategy 2024–2030.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

No authoritative public ranking by revenue exists. Many market participants are subsidiaries of international groups (such as GE, Siemens, T-Systems, Oracle Cerner, Phillips) or privately held startups without published financials, and most do not disclose "digital health" revenue as a separate segment. In addition, a substantial part of the DH landscape is organised and funded by the Austrian state (e.g. ELGA and other e-health infrastructures).

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Official revenue growth rankings are not published for Austria. However, market observers point to fast-growing DH players in areas such as telemedicine, AI-based diagnostics, and remote monitoring, often including venture-backed startups and scale-ups that have recently raised significant funding.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

Generally, DH is subject to several regulatory regimes and therefore monitored by various authorities/agencies/entities:

- Federal Ministry of Social Affairs, Health, Care and Consumer Protection (BMSGPK).
- Federal Office for Safety in Health Care (BASG).
- Austrian Agency for Health and Food Safety (AGES).
- Austrian Umbrella Organisation of Social Insurance.
- Ethics committees.
- ELGA GmbH.
- Data Protection Authority (*Datenschutzbehörde* – DSB).

- Austrian Competition Authority (*Bundeswettbewerbsbehörde* – BWB).
- RTR/AI Service Desk.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The main legal regimes touching DH include:
- Medical Devices (MDs): EU Regulations (MDs and *in vitro* diagnostics (IVDs)), Austrian Medical Devices Act 2021 and adopted ordinances, industry codes.
- Data Protection and Health Telematics: GDPR, Austrian Data Protection Act, Austrian Health Telematics Act 2012, Telecommunications Act 2021.
- EU AI Act.
- Austrian Physicians Act (ÄrzteG).
- Product Liability and Safety laws.

Miscellaneous laws include drugs and hospitals regimes, trade licence law (e.g. for regulated MDs), advertising rules, reimbursement and social insurance law and cybersecurity/ICT security laws.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

(i) Key areas of enforcement:
- Classification of software under EU Medical Device Regulation (MDR)/*In Vitro* Diagnostics Regulation (IVDR) (Software as a Medical Device (SaMD), apps).
- Vigilance and reporting of "serious incidents" for medical software.
- Compliance with clinical evaluation and post-market surveillance requirements.
- GDPR enforcement concerning sensitive health data and secondary data use.
- Cybersecurity and data breach notification.
- Advertising and claims substantiation.

(ii) Emerging areas of enforcement:
- EU AI Act enforcement: AI transparency, bias mitigation, and explainability in clinical decision-support tools.
- Mandatory use of EUDAMED.
- NIS2 cybersecurity compliance for hospital/healthcare organisations (HCOs).
- Secondary use of health data for research and AI training.
- Cross-border DH services and telemedicine platforms.
- Interoperability and data governance obligations under EU health data initiatives.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Generally, software qualifying as SaMD is regulated under:
- MDR or IVDR.
- Austrian MD law (acts and ordinances).
- GDPR, Data Protection Act and Health Telematics Act (personal health data processing).

Competent authorities:
- BMSGPK/BASG/AGES (enforcing bodies).
- Notified bodies (conformity assessment for higher-risk software Class IIa, IIb, III).
- DSB.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

AI/ML-based digital solutions are generally treated as MD or IVD when they have a medical purpose. AI/ML-powered DH solutions are primarily regulated through:
- EU MDR/IVDR (medical safety and performance if the AI software has a medical purpose).
- EU AI Act classifying most medical AI systems as high-risk AI (data governance, transparency, human oversight).
- GDPR particularly automated decision-making and processing of health data.

Authorities:
- BASG/AGES – MD oversight.
- DSB – data protection and algorithmic processing.
- Future designated AI Act national supervisory authorities (AI Office).

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Austrian regulators appear to be gradually transitioning from a one-time approval model to a lifecycle management approach, with increased emphasis on post-market surveillance and lifecycle governance requirements (including change management, logging, and human oversight). In practice, many AI systems are currently approved in a relatively "locked" form, with updates treated as regulated modifications rather than as unconstrained continuous learning in the field.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data is central (make-or-break) to regulatory approval and enforcement under the MDR (Annex 14) and AI Act: Developers must demonstrate safety, clinical benefit, and performance/analytical validity relative to intended use. For AI systems, regulators increasingly expect:
- Training datasets are representative with population and bias-aware datasets (no algorithmic bias).
- Real-world performance evidence.
- Continuous validation through post-market clinical follow-up.

Under the AI Act, high-risk AI systems will also require robust validation datasets and documented risk mitigation measures. Insufficient or poorly designed validation data can lead to refusal or restriction of market access.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Austria operates under a centralised model that regulates DH primarily at the federal level. As a result, DH products are not subject to materially different regulatory approval regimes across the regions (*Länder*). The regional level is mainly responsible for ethics committees, healthcare service delivery, public procurement, and the administration of public hospitals.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Overall, while robust mechanisms exist (such as fines, reimbursement exclusions, system audits), DH enforcement in Austria is integrated into existing legal regimes without unique tailoring for DH. Austria has not recorded high-profile enforcement actions (fines, recalls, etc.) in the DH sector.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Medical advice: Medical advice and treatment may only be provided by licensed physicians (Sec. 3 ÄrzteG); in teleconsultations, the physician must decide case-by-case whether remote care is sufficient or whether a physical examination is required, and must refer the patient to in-person care if the information basis is insufficient.
  Teleradiology: Specific constraints exist for teleradiology (e.g. permitted in basic/special trauma care, dispersed outpatient facilities, and for maintaining night/weekend/holiday operations for urgent cases).
  Infrastructure: As of 2026, all private physicians are legally required to use ELGA, the e-card infrastructure, and the e-vaccination pass.
  Telematics and data transfer: Strict conditions for electronic transmissions of health and genetic data (e.g. GDPR; strong authentication of patients and providers; role-based access; confidentiality and integrity; state-of-the-art encryption and secure implementation).
- **Robotics**
  MD qualification: Robotic systems used for diagnosis, therapy or other medical purposes (e.g. surgical robots) qualify as MD and must undergo appropriate risk classification, conformity assessment and CE-marking.
  Medical advice: In case of robotic assistance in diagnosis or treatment, medical advice and final clinical decisions remain the responsibility of physicians and require supervision.
  Safety and cybersecurity: Manufacturers must address mechanical and software safety, cybersecurity, human-machine interface risks and post-market surveillance.
  Liability: Product liability applies to software and AI components, making manufacturers liable for defects.
  EUDAMED: As of May 28, 2026, robotics manufacturers must have their systems registered in the mandatory EUDAMED modules (Actor, UDI, and Certificates).
- **Wearables**
  Wearables marketed purely for wellness or lifestyle (e.g. step counters) are usually not MDs, unless the device is intended by the manufacturer for one or more medical purposes (monitoring vital parameters for diagnosis, therapy or risk stratification).
  Data Protection laws: Collection and processing of personal health data requires compliance with data protection laws.
  Interoperability/telematics: If integrated into Austrian e-health infrastructures or provider systems, health telematic laws and ELGA-related rules on secure health data exchange and access control become relevant.
- **Virtual Assistants (e.g. Alexa)**
  MD qualification: Virtual assistants are not MDs; however, if natural language processing or dialogue functions are specifically intended to be used for one or more medical purposes (e.g. symptom assessment leading to diagnostic output), MD laws apply.
  Medical advice: Reserved to physicians, consumer-directed virtual assistants must not be positioned as autonomously diagnosing or treating patients.
  Transparency rules: AI-generated content must be clearly identifiable.
  Data and e-privacy: The processing of personal or health data requires compliance with rules for health data, data minimisation, and security requirements.
- **Mobile Apps**
  MD qualification: Wellness-related apps are not MDs, but apps that perform diagnosis, recommend treatment, or control/monitor physiological processes for a medical purpose typically constitute MDs (Class IIa and higher) and must comply with risk classification, clinical evaluation, CE-marking and post-market surveillance.
  Consumer and advertising law: Misleading health claims can trigger unfair-competition and advertising-law issues.
  "App on Prescription": By late 2026, apps that prove positive care effects (medical benefit or structural improvement) can be prescribed and be reimbursed.
  App-specific data risks: Health apps process sensitive data; healthcare professionals (HCPs) or ELGA participants must observe health telematic laws on secure exchange.
- **Software as a Medical Device**
  MD classification and conformity: Software intended for diagnosis, prevention, monitoring, treatment or alleviation of disease is a MD (MDR Annex VIII notably Rule 11); diagnostic or therapeutic software will be class IIa or higher, requiring notified-body involvement.
  Clinical evaluation and lifecycle: SaMD requires appropriate clinical evaluation (including literature, clinical investigations or real-world data), risk management, usability engineering, cybersecurity and continuous post-market surveillance; significant updates may constitute substantial changes requiring reassessment.
  AI: Most SaMD falls into the High-Risk category of the AI Act requiring a quality management system that specifically includes data governance to prevent algorithmic bias.
  Data protection and telematics: Where SaMD processes personal health data.
  EU Product Liability Directive 2026 expands to standalone software.

- **Clinical Decision Support Software**
  MD qualification: CDSS that provides patient-specific assessments, diagnoses or treatment recommendations typically qualifies as SaMD; risk class depends on how directly it drives decisions with corresponding clinical evidence and notified-body requirements.
  Automated decision-making: When CDSS uses personal data to make or drive decisions, data rules on automated individual decision-making and profiling must be considered.
  Medical advice: CDSS must support, not replace, the physician's professional judgment; the physician remains responsible for interpreting outputs and deciding whether they are appropriate for the individual patient.
  Explainability, bias and accountability: For AI-enabled CDSS, regulators increasingly expect documentation of model performance, limitations, bias mitigation and human-oversight mechanisms (human in the loop).
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  MD and AI qualification: AI/ML systems intended for diagnosis, prevention, monitoring or treatment generally qualify as MD or IVD, triggering classification (at least class IIa), CE-marking, clinical evaluation and post-market surveillance.
  Algorithm dynamics and accountability: Changes in AI models can count as significant modifications under MDR, requiring updated documentation and possibly new conformity assessment.
  Data protection and telematics: Training and inference on health/genetic data require compliance.
  Austrian authorities currently apply a lifecycle-based compliance approach, relying on post-market surveillance rather than dynamic re-approval for software updates.
- **IoT (Internet of Things) and Connected Devices**
  MD status: Connected sensors and IoT platforms are MDs when intended for medical purposes (e.g. remote vital-sign monitoring, connected blood-pressure systems) and must comply with device safety, cybersecurity and interoperability requirements.
  Continuous data transfer of health parameters requires data protection (special-category data), health telematics compliance, and in some cases the observation of telecommunication/e-privacy rules; secure authentication, encryption and access control are essential.
  Liability analysis must cover hardware, embedded software, cloud components and interfaces to ELGA or hospital IT, in line with MDR post-market surveillance and EU product liability standards.
- **3D Printing/Bioprinting**
  Product classification: 3D-printed medical products may qualify as MD or, for tissue-engineered products (bioprintings), as advanced-therapy medicinal products (ATMPs), the latter requiring drug authorisation and drug quality requirements.
  Data and design files: Patient-specific printing involves processing imaging and other health data under data protection and health telematic rules; design files and printing parameters can raise IP and trade-secret issues.
  Bioprinting, especially of tissues or organs, raises ethical, safety issues, which must be addressed in clinical trials and ethics-committee approvals.
- **Digital Therapeutics**
  MD qualification: Digital therapeutics qualify as high-risk MDs.
  Evidence and reimbursement: Clinical evidence of therapeutic benefit is required for clinical evaluation and potential reimbursement (e.g. future Austrian DiGA/DiPA-type processes under the eHealth Strategy).
  Data and ELGA: Secure integration with ELGA as digital therapeutic solutions process detailed behavioural and health data, alongside clear information on adherence monitoring and secondary data use.
- **Digital Diagnostics**
  MD qualification: Software and connected tools that perform device-controlled diagnostic measures (including image analysis and lab result interpretation) are MDs or IVDs (class IIa or higher).
  Telematics: Diagnostic data are ELGA-relevant health data; their storage and exchange (e.g. lab reports, imaging results) must follow ELGA and health telematics rules on permitted data types, retention and access.
  The closer a diagnostic output is to an automated or decisive finding, the more regulators focus on validation, human oversight and compliance with data provisions on profiling and automated decision-making.
- **Electronic Medical Record Management Solutions**
  Data protection and telematics: Solutions must implement strong authentication, role-based access and logging; patients retain rights to access their data and may opt-out.
  ELGA framework: Regulates how long health data can be stored, and who may access it, as well as interoperability requirements, standardisation and secure connection. ELGA and integrated services (e-medication, e-lab, e-reports) are funded via the statutory health-insurance and public budgets. Patients do not pay separately for these services.
- **Big Data Analytics**
  GDPR compliance: Large-scale analytics on health data must comply especially with legal basis for processing special-category data, purpose limitations, and safeguards for research/secondary use exceptions.
  Data governance and sharing: The EU Data Governance Act and national laws aim to facilitate the sharing and re-use of protected data, including some health data, under controlled conditions; Austrian telematics regimes on health and genetic data apply.
  De-identification and re-identification risk: Pseudonymisation/anonymisation strategies must be robust, given high re-identification risk with health big data, and are central to data protection impact assessments and ethics approvals for analytics projects.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Data protection: Key regulatory challenges include data controllership reconciling, data subject rights, blockchain immutability (e.g. right to erasure or correction) and ensuring confidentiality and access control.
  Health telematics: Where health data is transmitted within healthcare systems.
- **Natural Language Processing**
  MD qualification: NLP technologies generally do not qualify as MDs (e.g. dictation or transcription software) unless where NLP is specifically intended for a medical purpose (e.g. symptom analysis, clinical decision support, or diagnostic assistance).
  Where personal or health data is processed, data protection rules apply, including transparency and security requirements.

Medical advice: NLP-based tools must not replace the physician in giving medical advice; their outputs must be framed as decision support and used under professional responsibility.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Providers must observe and navigate:

- Medical advice: only a treating physician, not the platform, must be presented as the medical service provider.
- Terms of use and user interfaces: should define responsibilities, professional independence of physicians and appropriate disclaimers.
- Prohibition of referral fees: platform business models must avoid per-patient referral fees, lead-based commissions or similar constructs; remuneration should be structured as neutral service fees (e.g. subscription/flat platform fees).
- Whether platform functionalities (e.g. decision support) could trigger MD requirements.
- GDPR and telematics: health data (special-category data) and state-of-the-art technical and organisational measures and roles (is controller, joint controller or processor).
- EU Digital Markets Act (Regulation (EU) 2022/1925): in case of gatekeeper-status, potential obligations on self-preferencing, data use and interoperability.
- Product liability, consumer protection and advertising restrictions.

Additionally, platforms intermediating between healthcare providers and patients may fall under the EU Platform-to-Business Regulation (Regulation (EU) 2019/1150), which requires transparent, fair terms and clear ranking and access rules for business users.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The use of personal health data is primarily governed by the GDPR and the Austrian Data Protection Act. According to Art. 9 GDPR, genetic data, biometric data and data concerning health are categorised as special categories of personal data, the use of which is generally prohibited. The processing of the foregoing data is only permitted if one of the conditions of Art. 9 Para. 2 GDPR is met (e.g. consent of the data subject or processing is required to protect vital interests). The Austrian Data Protection Act does not stipulate additional obligations.

In addition to the general data protection framework, the Austrian Health Telematics Act stipulates rules for the processing of health data by healthcare providers and is the central legal framework for electronic health record systems. With the EHDS new rules for sharing, accessing and using health data will be established.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Legal regulation of the use of personal health data is uniformly governed under national laws/European law.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

According to Art. 9 Para. 2 GDPR, the processing of health data is permitted under specific conditions. These conditions do not address specific entities, but determine which purposes are accepted. Albeit, within the purposes, some entities are considered (e.g. associations with a non-profit aim, public health entities, research entities). For medical professionals, the Health Telematics Act is applicable in addition.

With regard to the nature of the data, the main element is whether the data are personal, thus relating to an identified or identifiable natural person or anonymised (then GDPR does not apply).

4.4 How do the regulations define the scope of personal health data use?

As the processing of health data is generally prohibited under the GDPR, the permitted scope of use is explicitly set out in Art. 9 Para. 2. Also, the Austrian Health Telematics Act lays down in detail which data may be used for what purpose, e.g. in Sec. 14.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

A central aspect for contractual terms is the clear determination of the purpose of data processing and the roles of the different actors (data controller, data processor, data subject). Moreover, clarifying the retention of data, deletion of data, technical and organisational measures for secure processing, data transfers and data subjects' rights is essential.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

There are no regulations specifically addressing these aspects. However, the GDPR stipulates the principles of accuracy of data and the integrity of data, which also apply to health data. The Health Telematics Act additionally governs the integrity of electronic health data by stipulating the necessity of electronic signatures.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

There are various standards established by the Austrian Standards organisation, such as on health informatics.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The sharing of data is considered as a form of "processing"

such as the use of data. Therefore, for the sharing of data, the regulations of the GDPR and the Health Telematics Act apply. If data is shared for processing, the roles (controller and processor) and according obligations must be considered. If data is shared with a recipient that is located outside of the EU, this amounts to a transfer under the GDPR and must be in line with the strict requirements of Art. 44 *et seq.* GDPR. In addition, the EU Data Act must be considered.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The sharing of personal health data is uniformly governed under national laws/European law.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

See question 4.3.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

The GDPR stipulates strict rules for the sharing of data (as this is a form of processing and therefore requires a legal basis). In addition, the Health Telematics Act sets out in its Chapter 2 provisions specifically tailored to the electronic transfer of health data.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

In Austria, federated models of healthcare data (HD) sharing are most prominently embodied in ELGA, which is designed as a decentralised/federated system where health data remain stored at the level of the original healthcare providers and are made accessible through a shared infrastructure rather than being centrally pooled. ELGA is essentially governed by the Health Telematics Act and the GDPR.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under the Austrian Patent Act, an invention must be new, involve an inventive step, and be industrially applicable to be eligible for the awarding of a patent. Software as such is not patentable (explicitly excluded), unless it has a technical character or produces an additional technical effect. Hardware is patentable if it fulfils the requirements for a patent. Thus, DH technologies are patentable as hardware or as technical solutions, not as abstract data processing or medical decision-making alone.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The Austrian Copyright Act protects works that are original intellectual creations. It specifically governs the protection of computer software and databases, thus protecting the code, preparatory materials and databases. However, only works created by natural persons (not, e.g., AI) are protected.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

The Austrian Act against Unfair Competition protects information that is secret, has commercial value due to its secrecy, and is subject to reasonable confidentiality measures, as a trade secret. This can be crucial if other intellectual property (IP) rights do not apply. However, the characteristics of a trade secret must be upheld to be protected.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

The Austrian University Act stipulates that employed researchers must report inventions to the university, which can subsequently acquire patent rights to these inventions. With regards to copyrights, only the natural person generating the work is regarded as the originator and protected by copyrights, but rights of use can be granted to other parties such as academic institutions.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

The protection for SaMD depends on the qualifications of the components. For hardware and software with technical contribution, patent law can apply. For source codes and databases, copyrights can apply. Information can be protected as a trade secret.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No. Only natural persons can be inventors.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

There is no specialised statutory regime in Austria that provides for an automatic transfer of IP rights to the state on the basis of funding. The allocation of these rights must be governed by contracts. It is common practice to grant certain rights or obligations on dissemination or open access.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

IP rights are mainly shaped by the legal framework and less by precedential cases. A significant decision to mention was 4 Ob 119/20h issued by the Austrian Supreme Court on the aspects of "technicity" for protection under patent law.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

When structuring collaborations in DH, parties should:

- Define IP and ownership: clear contractual allocation of ownership to pre-existing and emerging IP, usage and commercialisation rights, licensing scope, exclusivity, and sublicensing rights.
- Allocate regulatory and liability responsibilities: Contractually assign MDR/IVDR roles and responsibilities for CE-marking, vigilance, post-market surveillance and telematics compliance, clarify liabilities, insurance and corrective measure responsibility.
- Define governance and exit: regulate decision-making processes, joint steering, audits, governance structures, information sharing, exit scenarios, and the handling of regulatory-driven changes to ensure long-term scalability and compliance.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

- Compliance and roles under MDR/GDPR.
- Ensure business transparency and written documentation.
- Ensure healthcare compliance with ABC rules (MD laws, criminal law), professional conduct rules and industry codes (for MDs and drugs).

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

- Address roles (controller, joint controller, processor).
- Regulate security, data minimisation, governance and confidentiality.
- Assess whether data can be anonymised, as this limits the data protection requirements and allows re-use and commercialisation.
- Address IP ownership in trained models, restrictions on downstream use, and regulatory compliance (e.g. MDR, AI Act).
- Regulate liability allocation and audit rights.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

- Ensure AI Act compliance (e.g. AI literacy, prohibited practices, transparency, high-risk AI).
- Ensure MDR alignment (risk classification, conformity assessment, technical documentation, risk management, transparency).
- Clarify who may use and own AI-generated code, text, images or clinical content, and whether and how such output may be reused, commercialised or used for further training.
- Identify and address third-party IP risks and allocate warranties, indemnities and due-diligence obligations accordingly.
- Prohibit or tightly control input of identifiable patient data into general-purpose AI systems unless a solid GDPR legal basis, telematic compliance and appropriate DPAs are in place (including location of processing and sub-processor chains).
- Define confidentiality, security and data-use limits for providers of foundation models (e.g. patient/customer data training).
- Regulate product liability and transparency (human supervision).

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Austria has not yet established a centralised regulatory body for AI/ML frameworks enforcement. Consequently, competences are distributed among various authorities, such as: the AI Service Desk at the RTR; the governmental AI Advisory Board; DSB; and AGES.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

The primary regulatory framework is the EU AI Act. At present, there is no supplementary national legislation in Austria dedicated to AI. However, the deployment of such technologies remains subject to existing cross-sectoral regimes, specifically the GDPR and the Health Telematics Act for the secure electronic processing of health data.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under Austrian law, rights are only granted to human originators. Improvements generated autonomously by AI either remain unprotected or are attributed to the human who designed the system, depending on circumstances.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

As HD is a special category of personal data (Art. 9 GDPR), HD licensing is significantly more restricted and compliance-heavy than general AI data licensing.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Currently, only the AI Act itself differentiates: if an AI system serves to generate text, images etc., transparency obligations apply (e.g. the output must be marked as generated by AI). In addition, there are specific rules for general purpose AI (GPAI), i.e. an AI model trained with a large amount of data using self-supervision, capable of performing a wide range of distinct tasks. Providers of GPAI must comply with stricter requirements (e.g. notification of the EC, technical documentation, copyright protection policy).

When health data is used in AI applications, high-risk AI rules apply, as Annex I of the AI Act classifies MDs as high-risk AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Generative AI and GPAI are subject to a more stringent regulatory regime under the EU AI Act due to the risks associated with synthetic outputs that are indistinguishable from human-generated content and the possibility of using these applications for various purposes.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In Austria, the issue of AI/ML models trained on data without appropriate rights is addressed through a combination of copyright rules, GDPR and the EU AI Act. The central legal mechanism is the Text-and-Data-Mining exception, which stipulates that models may be trained on data, if the holder of the according rights has not explicitly refused. With regard to personal data, the processing must comply with the GDPR.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Austria regulates DH liability through general liability rules rather than a sector-specific regime. For AI/ML, the same basic rules apply, but forthcoming EU product-liability and AI rules will increase expectations on risk management, transparency and documentation.

- Contractual and tort liability (for damages caused culpably and unlawfully in the healthcare context, including pain and suffering, but excluding punitive damages).
- Strict Product liability (2026 will bring liability rules for standalone apps and AI models as well as presumptions of defect and document disclosure obligation).
- Regulatory, criminal and professional consequences (for instance fines or recalls).

9.2 What cross-border considerations are there?

- Applicable law and jurisdiction mainly follow EU rules, unless contractually agreed upon.
- Physicians outside Austria providing telemedical services to patients located in Austria must comply with Austrian professional licensing requirements unless the freedom to provide services applies (if services are provided on a temporary and occasional basis, Sec. 37 ÄrzteG).
- Consumer protection rules may also be relevant, as healthcare services are typically provided on the basis of contracts concluded by patients acting as consumers.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Such risks can be mitigated through a combination of legal, technical, and organisational measures, namely a robust regulatory and quality compliance, allocation of responsibility and governance.

- Ensure AI/ML-enabled solutions comply with MD/IVD laws (risk management, clinical evaluation, post-market surveillance, etc.), with clear allocation of roles.
- Implement documented quality-management and risk-management systems that explicitly address AI/ML lifecycle risks.
- Ensure clear allocation of responsibilities (vendor, integrators, providers, deployers) and governance around models and updates.
- Ensure data protection, security and transparency.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

- GDPR: A misuse of HD constitutes a breach of GDPR, which allows the data subject to exercise its rights and claim damages under tort law or contract law. In addition, administrative fines can be awarded.
- Manufacturer and vendor liability: AI/ML developers and vendors can be liable under contract and tort principles, and/or product liability (e.g., security defects, model leaks).

In practice, managing the liability risk requires careful allocation and documentation of roles (controller/processor, manufacturer/user), lawful data sourcing and training, strong technical and organisational safeguards, and clear internal policies on how AI/ML outputs are used in clinical and commercial workflows.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

- Data protection and telematics compliance (strong encryption, access controls, logging and secure transmission; location of processing and transfer to third countries, especially regarding ELGA/eHealth infrastructure integration).
- MD qualification and shared responsibility (manufacturer, cloud provider and healthcare role, e.g. regarding configuration and update responsibilities, incident response).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

- Regulatory perimeter and business-model fit: Check if the solution is a MD/IVD, whether activities/services fall under medical services (reserved for physicians) or engage in prohibited patient referrals and/or comply with health data rules.
- Reimbursement: Assessed whether reimbursement is legally possible to avoid market entry barriers.
- Healthcare compliance (ABC) rules *vis-à-vis* HCPs/HCOs and implement compliance culture/structures.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

- Perform in-depth regulatory, healthcare law and data-protection due diligence.
- Ensure EU-wide regulatory scalability.
- For AI/ML-based products regarding compliance with model development, training data, update processes and documentation rules and EU AI/product-liability requirements.
- Check reimbursement status and eHealth pathways (ELGA integration, possible future DiGA/DiPA-type schemes, individual contracts with payors) and dependence on specific HCPs/HCOs for assessing scale potential.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

- Medical advice is reserved to licensed physicians thereby limiting task-shifting and automation or direct-to-patient models.
- Infrastructure constraints: Fragmented IT infrastructure and varying digital maturity across providers and regions can slow down integration of new tools with hospital information systems and ELGA.
- Literacy gaps: digital literacy of the ageing patient population and/or HCPs.
- *Ad hoc* reimbursement: currently no structured framework, but a standardised process is to be established in 2026.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Adoption and processes are primarily governed by regulatory frameworks rather than by independent certification bodies.

Consultations on these matters typically involve the Austrian Medical Chamber, the Umbrella Association of Social Insurances or special health associations. Endorsements or guidelines from such professional associations and scientific societies can be influential in clinical practice and may be consulted in legislative, court or policy processes, especially for defining "state-of-the-art" care.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

A standardised national reimbursement process will be codified by 2026/2027 – DiGAs will be reimbursable if clinical evidence of positive care effects is provided.

Presently, for digital tools, reimbursement, on an occasional basis, requires the solution to be classified as a medical aid or reimbursement is specifically agreed upon by the developer with social insurance carriers. Still, formal evaluation and registration requirements are expected to increase as Austria develops a framework for evidence-based digital therapeutic applications under the Digital Austria agenda.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence gaps often arise from the complex framework, namely the intersection of regulatory, data protection, and technical issues. Legal, technical, and clinical aspects are frequently analysed in isolation but require a multidisciplinary approach. Also, interoperability with eHealth systems and data fragmentation and insufficient documentation or validation can be an issue.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

- Trade licences and facility permits.
- The 2026 alignment of ELGA with the EHDS regarding cross-border portability and secondary use data (data altruism).
- DiGAs: standardised national reimbursement process planned.
- High-risk AI: AI Regulatory Sandbox, allowing DH startups to test AI-driven solutions in a "safe harbour" environment with regulatory guidance from the BASG.
- Mandatory digitalisation for physicians (medical data storage).
- Stricter product liability (AI/software defects, evidence standards).



Dr. Daniel Larcher is a Partner at ATLAS Attorneys at Law and was admitted to the Bar in 2010. He specialises in commercial law and public commercial law with a focus on healthcare, regulatory and contracts. Daniel is the author of numerous publications in his areas of expertise and gives lectures, workshops, and training courses on these topics.

ATLAS Attorneys at Law
Nibelungengasse 13/1
1010 Vienna
Austria

Tel: +43 1 925 97 66
Email: d.larcher@atlas-law.at
LinkedIn: www.linkedin.com/in/daniel-larcher-43808698



Dr. Mariella Rieder, LL.M., is a Senior Legal Counsel at Prewave GmbH, an Austrian company providing AI-driven software for supply-chain monitoring. Mariella has passed the Austrian Bar exam, worked for an international law firm, the European Commission, as well as the Austrian Ministry of Justices, and currently specialises in AI Law, Data Protection Law and IT Law.

Prewave GmbH
Rothschildplatz 4 / Austria Campus 4, 3rd Floor
1020 Vienna
Austria

Tel: +43 1 30 50 743
Email: mariella.rieder@prewave.ai
LinkedIn: www.linkedin.com/in/mariella-rieder

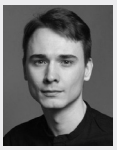
ATLAS Attorneys at Law is a business law firm based in Vienna, Austria. The ATLAS team advises and represents national and international businesses as well as public corporations. The focus areas are corporate and business law as well as public commercial law.

www.atlas-law.at

ATLAS
ATTORNEYS AT LAW

Belarus


Kirill Laptev


Vladislav Zhavnerchik


Anastasiya Pyshnaya-Muryna


Anna Zhdanovich

Anischenko Laptev

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

The new approach to digital health in general and its definition is reflected in the draft Code "On Healthcare" (**Draft Code**), which is planned to be introduced into Parliament by December 2026. Digital health (or electronic healthcare) is defined as a system of state, public, and medical measures aimed at preserving and strengthening public health, preventing and treating diseases through the use of information and communication technologies, as well as through the establishment and operation of online pharmacies and other services designed to organise and ensure accessible medical care for the population, including through the development of the Centralized Healthcare Information System (**CHIS**), the use of robotics solutions, and other technological innovations.

Previously, the Belarus Concept for the Development of Digital Health in the Republic of Belarus for the period up to 2022, adopted by the Ministry of Healthcare of the Republic of Belarus (**Ministry of Healthcare**), defined digital health as a set of information systems and resources, and information and communication technologies, functioning in the healthcare sector based on common principles and rules, to provide information interaction between organisations and citizens, and to serve their information needs. Since 2024, the practical implementation of digital health has been carried out through the establishment of the CHIS.

While the Model Law "On Digital Health" adopted by the Interparliamentary Assembly of Member States of the Commonwealth of Independent States (**CIS**) also reflects a comprehensive understanding of digital health, it does not have legally binding effect in Belarus and to date its definition of "digital health" is not reflected in Belarus laws. In turn, regulations on the level of the Eurasian Economic Union (**EAEU**) can apply, for instance, under the Protocol approved in December 2025 amending the Agreement on Uniform Principles and Rules for the Circulation of Medical Devices within the EAEU of 23 December 2014; the transition period allowing registration of medical devices under either national law or EAEU law has been extended until 31 December 2027, enabling Belarus to gradually move to a unified EAEU registration system while ensuring uninterrupted market circulation, including for digital health products qualifying as medical devices.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The Belarusian telemedicine regulatory regime, introduced by the Law "On Healthcare" (**Law on Healthcare**) and elaborated by the Resolution of the Ministry of Healthcare No. 65 of 28 May 2021, establishes a framework for the delivery of medical care via telemedicine. These telemedicine services are part of broader digitalisation efforts, including the CHIS.

The digital health landscape is rapidly evolving around the deployment of the CHIS, an integrated information system designed to centralise storage and the processing of medical information and provide authorised users with access thereto. The Government Activity Programme for 2025–2029 requires all healthcare organisations, both public and private, to be integrated into the CHIS by 2026. The Draft Code also provides for the regulation of telemedicine, including its integration with the CHIS or medical information systems.

Key services of the CHIS include:

- A unified electronic medical record (**EMR**) accessible to all healthcare providers.
- A personal patient portal for appointment booking, access to test results, electronic prescriptions, medical certificates, sick leave and vaccination information, available via web and mobile applications.
- A centralised system for recording laboratory tests across public and private healthcare providers.
- A national archive for digital medical images, including CT and MRI scans.
- A patient queue-management system for surgeries and other planned medical procedures.

1.3 What is the digital health market size for your jurisdiction?

No official sources on the digital health market size in Belarus are publicly available.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

No official sources on the largest (by revenue) digital health companies in Belarus are publicly available. Most digital health innovation currently ties into national initiatives, public systems or pharmacy/delivery platforms. The regulator, the Ministry of Healthcare, and its supervised state-owned organisations are dominating in digital healthcare, in particular, by introducing and operating the CHIS.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

No official sources on the fastest growing (by revenue) digital health companies in Belarus are publicly available. Please refer to question 1.4 for details.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The principal regulatory authority in the healthcare sector in Belarus, including the digital heath sphere, is the Ministry of Healthcare. Scope of its enforcement powers extends across legal issues within the healthcare regulatory framework and, *inter alia*, encompasses ensuring the functioning and development of the CHIS by:

- coordinating the interaction between the operator and users of the CHIS;
- carrying out organisational and methodological support for the functioning and development of the CHIS; and
- ensuring the improvement of the normative legal framework in the field of digital healthcare.

The Ministry of Healthcare is accompanied by its subordinated authorities and state organisations in enforcing regulations in digital health. In particular, the State Institution "Republican Scientific and Practical Center for Medical Technologies, Government, Governance and Economics" has been designated as the operator of the CHIS, whose responsibilities include the phased implementation, reliable operation and progressive development of the CHIS in accordance with the digital agenda of the Ministry of Healthcare.

According to the Draft Code, the Council of Ministers of the Republic of Belarus (**Council of Ministers**) shall also closely regulate this sphere, *e.g.*, by determining the procedure for the functioning and use of the CHIS.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Overall regulation of healthcare in Belarus, including digital health, is covered by the Law on Healthcare.

There are also acts of the government and sectoral authorities that regulate digital health, such as: the Resolution of the Council of Ministers "On the Functioning and Use of the CHIS"; the Resolution of the Council of Ministers "On the State Programme 'Health of the Nation' for 2026–2030"; the Resolution of the Ministry of Healthcare "On Approval of the Regulation on the Specifics of Providing Medical Care Using Telemedicine Technologies"; the Order of the Ministry of Healthcare "On Certain Issues of Telemedicine Consulting in the Republic of Belarus"; etc.

Furthermore, the legislation on product safety, personal data (**PD**) protection and cybersecurity apply to digital health. In addition, general regulations on competition and consumer protection law must be kept in mind.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

(i) The key areas of enforcement relating to digital health encompass compliance with general requirements in traditional healthcare, as well as regulatory compliance for telemedicine, medical devices, data protection, information security and systems compliance, medical secrecy regime, consumer protection and liability for harm, and intellectual property matters.

(ii) The emerging areas relate to anticipated legislative development, *e.g.*, by the Draft Code adoption (including those concerning artificial intelligence (**AI**), virtual reality, and 3D printing) and further acts to be introduced in its implementation. Additionally, new regulations and expected amendments in tech and data spheres may be of relevance, for instance, regulations of AI-based technologies and amendments to PD protection laws.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Belarus legislation does not contain special legal regulation of SaMD, *i.e.*, one must comply with general regulation on the circulation of medical products (devices), notably with the Law on Healthcare.

The aforementioned law defines medical devices as any instruments, apparatus, devices, equipment, materials and other items that are used for medical purposes separately or in combination with each other, as well as *with accessories necessary for the intended use of medical devices* (including *special software*), intended by the manufacturer to provide medical care, including monitoring of the human body, conducting medical research, recovery and other uses. The Draft Code contains a similar definition, clarifying that such software may be developed utilising AI technologies. Hence, software may be identified as an accessory necessary for the use of a medical device, rather than as a medical device itself.

The regulatory bodies in Belarus responsible for medical device matters are the Ministry of Healthcare and the Republican Unitary Enterprise "Centre for Expertise and Testing in Healthcare".

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Belarus has no regulations specifically addressing AI or machine learning (**ML**)-powered digital health devices or software solutions, while the Draft Code addresses their further implementation in healthcare. To the extent that such devices may fall within the definition of medical devices (as discussed in question 2.4), they may be subject to medical device regulations.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Pursuant to the Draft Code, the development and deployment of solutions founded on AI technologies and other innovative approaches and solutions shall be implemented, *e.g.*, within the CHIS.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

There are no regulations that apply to clinical validation data regarding regulatory considerations for AI/ML-based digital health solutions.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Digital health regulation in Belarus is centralised at the national level, so all the regulatory authorities should adhere to the unified policy.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

No special regulations apply to enforcement actions devoted to digital health products and solutions in Belarus, so general enforcement actions are relevant.

State supervision over the circulation of medical devices is carried out by the State Institution "*Gospharmnadzor*" in accordance with the legislation on control (supervisory) activities. Other state authorities within their competence may conduct respective control and supervision as well.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Telemedicine in Belarus is defined as information technologies that enable remote interaction between healthcare professionals, patients or authorised persons for, *inter alia*, consultations, medical opinions, monitoring after in-person visits, and medical examinations (please see question 1.2 above).
  Core issues from a legal and regulatory standpoint include:
  - Patient Identification and Authentication: Healthcare providers must ensure proper identification and authentication of patients and medical personnel.
  - Patient Information: Providers must inform patients about the scope of services, the telemedicine system operator, the consulting physician, procedures and consent for data processing.
  - Data Protection and Medical Secrecy: Telemedicine providers must comply with PD protection and maintain medical secrecy.
  - Licensing and Professional Requirements: Only healthcare organisations and professionals holding the appropriate medical licences may provide telemedicine services. No separate telemedicine licence is required beyond standard medical licensing.
  - Limits on Remote Diagnosis: Remote treatment adjustments can only be conducted after an initial in-person examination by a treating physician.
  - Documentation: All telemedicine interactions, including consultations, treatment adjustments, and prescriptions, must be recorded in the patient's EMR maintained by the healthcare provider and signed using the healthcare professional's electronic digital signature.
- **Robotics**
  As of the time of writing, Belarus has no dedicated legal framework specifically regulating use of robotics in healthcare. Meanwhile, general rules may apply for use of robotics in digital health depending on its qualification, like for medical device use, PD protection, cybersecurity and medical secrecy, liability for harm and malfunction, and product safety requirements. For instance, the Ministry of Healthcare, by its Order No. 32 of 16 January 2025, approved the testing of an innovative "pharmacy robot", supporting the integration of robotics into pharmaceutical services. In particular, the pilot operation of the pharmacy robot shall ensure proper placement, effective functioning, 24/7 pharmaceutical consultation, compliance with drug storage and shelf-life rules, adherence to Good Pharmacy and Storage Practices, consumer protection, data privacy, and payment and reporting requirements under Belarus law. Evolving technical standardisation regulations may also be of relevance, as well as potential rules for AI-based systems, which are under discussion.
- **Wearables**
  As of the time of writing, Belarus has no dedicated legal framework specifically regulating the use of wearables in healthcare. Though the Draft Code mentions wearables, no special rules are stipulated. Same as for robotics, general rules are to be considered. In addition, the use of wearables for medical reasons (*e.g.*, blood glucose monitoring) for children in educational institutions (schools) is permitted as an exception from the general prohibition introduced in 2025.
- **Virtual Assistants (*e.g.*, Alexa)**
  Belarus laws do not specifically regulate virtual assistants in healthcare. Same as for robotics, general rules are to be considered.
- **Mobile Apps**
  Belarus laws do not specifically regulate mobile apps in healthcare. Same as for robotics, general rules are to be considered. The Draft Code mentions introducing mobile apps into the daily practice of medical workers as part of information support in the healthcare sector without other specifically devoted rules. In addition, use of mobile phones for medical reasons (*e.g.*, when heart rhythm monitoring is recorded using a mobile application) for children in the educational (study) process is permitted as an exception.
- **Software as a Medical Device**
  Belarus laws do not specifically regulate SaMD in healthcare. Same as for robotics, general rules are to be considered.
- **Clinical Decision Support Software**
  Belarus laws do not specifically regulate clinical decision support software in healthcare. Same as for robotics, general rules are to be considered, as well as medical ethics. The Draft Code mentions development of clinical decision support systems and predictive analytics as part of information support in the healthcare sector without other specifically devoted rules.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Belarus laws do not specifically regulate AI/ML-powered digital health solutions. Same as for robotics, general

rules are to be considered, as well as ethics and standardisation in the sphere of AI systems. Please see questions 8.1–8.7.

- **IoT (Internet of Things) and Connected Devices**
  Belarus laws do not specifically regulate IoT and connected devices in healthcare. Same as for robotics, general rules are to be considered. Technical standardisation regulations may be also of relevance, for instance, STB 2623–2023 "Internet of Things. Terms and Definitions".
- **3D Printing/Bioprinting**
  Belarus laws do not specifically regulate 3D printing/bioprinting in healthcare. Same as for robotics, general rules are to be considered. Though the Draft Code mentions 3D printing, no special rules are stipulated. Technical standardisation regulations may also be of relevance, for instance, the introduction of national standard "Additive Manufacturing in Medicine. Data. Optimized Medical Imaging Data", planned for 2029 according to the Programme of Advanced Standardization in Priority Sectors of the National Economy for 2025–2029, approved by the Order No. 222 of the Chairman of the State Committee for Standardization of the Republic of Belarus on 22 December 2025.
- **Digital Therapeutics**
  There are no specific healthcare regulations for digital therapeutics in Belarus. Same as for robotics, general rules are to be considered, including related to licensing, professional liability and ethics.
- **Digital Diagnostics**
  The same applies for digital diagnostics. Under the Draft Code, when addressing issues related to diagnosis, treatment prescription, determination of the scope of medical care, and other matters of telemedicine, healthcare professionals are guided by clinical protocols and the directives of the Ministry of Healthcare.
- **Electronic Medical Record Management Solutions**
  EMR management solutions are actively developing in Belarus as part of the CHIS introduction in 2026 (unified EMR to be used by both medical organisations and patients and their personal electronic accounts). Medical secrecy and PD protection, as well as compliance with regulatory requirements for connection to the CHIS by medical information systems, play the role of core legal (regulatory) issues.
- **Big Data Analytics**
  There are no specific healthcare regulations for big data analytics in Belarus. One of the key objectives in the digital development of healthcare, according to the Draft Code, is the accumulation of big medical data to train AI, without another special legal framework provided. General requirements for information processing and PD protection, as well as medical secrecy, are of relevance.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Belarus laws do not specifically regulate blockchain-based healthcare data sharing solutions.
- **Natural Language Processing**
  There are no specific healthcare regulations for natural language processing in Belarus.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Digital platform providers in the digital health space face issues in compliance with general legal and regulatory requirements in traditional healthcare and other areas, like data protection and use of information systems (resources). Meanwhile, the regulatory landscape is also evolving, including rules for telemedicine, introduction of the CHIS and the Draft Code to be considered by the Parliament in 2026.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The key regulatory issues stem from its dual qualification as a special category of PD under the general data protection regime and as medical secrecy under sector-specific legislation.

The primary legislative act establishing key requirements for the processing of PD is the Law of the Republic of Belarus No. 99-Z of 7 May 2021 (**Belarusian Data Protection Act**), which:

- categorises "information about health" alongside genetic and biometric data as special PD, thereby triggering stricter processing requirements; and
- establishes a clear rule of precedence: if another legislative act provides a specific regime for processing PD that constitutes a legally protected secret, that special regime prevails. For health data, this is the medical secrecy regime defined by the Law on Healthcare. It covers not only the patient's diagnosis and health status but also the fact of seeking medical assistance, details of proposed treatment, associated risks, and any other personal information obtained during care provision.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Belarus has no federal or regional differentiation in the legal regulation. However, a *de facto* two-tier regulatory and supervisory model exists, characterised by functional specialisation rather than territorial jurisdiction.

The National Personal Data Protection Centre of the Republic of Belarus (**NPDPC**) is an independent public authority responsible for supervising the application of the Belarusian Data Protection Act to protect the rights of data subjects. Its competence extends to all operators (similar to "controllers" under the GDPR) and authorised persons (similar to "processors" under the GDPR), including those operating in the healthcare sector.

Sector-specific regulation and supervision in healthcare is carried out by the Ministry of Healthcare, which is responsible for regulating the processing of personal health data within the framework of the medical secrecy regime. The Ministry develops and approves mandatory sector-specific rules, for example: the forms and procedure for obtaining a patient's consent for the inclusion and processing of their PD in electronic healthcare information systems (*e.g.*, Order of the Ministry of Healthcare No. 74 of 7 June 2021 (**Order No. 74**)).

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

Regulatory obligations in Belarus differ depending on the status of the processing entity and the categories of PD involved.

The Belarusian Data Protection Act's territorial scope is limited: foreign organisations without a legal presence in Belarus are not directly subject to its provisions. That said, the requirements of the Belarusian Data Protection Act may apply indirectly.

Personal health data are classified as special PD under the Belarusian Data Protection Act, which subjects their processing to stricter rules. Unlike general PD, the processing of special categories (including health data) cannot be based on the performance of a contract.

Differences also arise depending on the type of organisation within the healthcare sector, reflecting the fact that sectoral regulatory development is still evolving and lacks full uniformity: public healthcare institutions must follow mandatory procedures, including the use of standardised consent forms; private medical organisations, by contrast, are not bound by these standard templates. Entities that process biometric or genetic data are subject to enhanced obligations. These include mandatory registration of their information systems with the State Register of PD Operators and implementation of enhanced technical and cryptographic protection measures for PD in accordance with the requirements of the Operations and Analysis Center under the President of the Republic of Belarus.

4.4 How do the regulations define the scope of personal health data use?

The regulatory framework in Belarus defines the scope of permissible personal health data use primarily through the principle of purpose limitation, which is anchored in both general data protection law and healthcare legislation. The scope is not established by a single exhaustive list of permitted uses but is instead constructed from lawful purposes and legal bases set forth in the Belarusian Data Protection Act.

The fundamental legal basis for processing personal health data is "for the purpose of organising the provision of medical care", provided that such data are processed by a medical, pharmaceutical, or other healthcare worker who is under a statutory obligation to ensure the protection of PD and is bound by the duty of medical secrecy (Article 8(2), paragraph 5, of the Belarusian Data Protection Act). This encompasses all activities necessary for diagnosis, treatment, medical rehabilitation, and maintaining patient records, as governed by healthcare legislation.

For processing that extends beyond the immediate context of direct care (particularly for inclusion in electronic information systems, registers, or databases of a specific operator), the primary mechanism defining the scope is the explicit and informed consent of the data subject.

The scope of use may also be defined by direct statutory authorisation, including, but not limited to:

- protecting the life, health, or other vital interests of the data subject or other persons where obtaining consent is objectively impossible;
- fulfilling duties or exercising powers expressly provided for by legislative acts (*e.g.*, social security, public health reporting, or forensic medical examinations); and
- conducting administrative or criminal proceedings or carrying out operational investigative activities.

Any use of personal health data for purposes incompatible with the original purpose of collection (such as marketing or commercial analytics) is prohibited unless a new, specific legal ground is established.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

In Belarus, any engagement of an authorised person to process personal health data on behalf of an operator must be governed by a written data processing agreement (**DPA**).

Key contractual terms include:

(i) Clear specification of the methods and purpose of processing: The agreement must define the exact scope of permitted operations (*e.g.*, storage, analysis, transmission) and link them to a valid legal basis. Generic or open-ended formulations are unacceptable.

(ii) Obligation of confidentiality and medical secrecy: The authorised person (processor) must be bound by a duty of confidentiality that aligns with the standards of medical secrecy under healthcare law.

(iii) Security measures (including legal, organisational, and technical):
- Legal measures, such as the publication of documents defining the data processing policy.
- Organisational measures, such as appointing a Data Protection Officer, training employees, and establishing access procedures.
- Technical measures, such as implementing technical and cryptographic protection of PD in accordance with the requirements of the Operations and Analysis Center under the President of the Republic of Belarus.

Furthermore, in accordance with the NPDPC Recommendations on the Relationship between Operators and Authorised Persons in PD Processing, the DPA must include the following provisions:

(i) Sub-processing restrictions: Any further delegation of processing tasks requires the prior authorisation of the operator and must be subject to the same level of protection.

(ii) Assistance with data subject rights: The authorised person must support the operator in fulfilling statutory obligations toward data subjects, including requests for access, rectification, erasure, or information about processing.

(iii) Data return or secure deletion: Upon termination of the agreement, all PD must either be returned to the operator or securely destroyed, with written confirmation provided.

It is important to note that, as outlined in the same NPDPC Recommendations, if the authorised person is a non-resident of Belarus and therefore cannot implement specific mandatory protection measures prescribed by Belarus law (*e.g.*, certain organisational requirements under Article 17), an assessment must be made of the equivalent measures it has taken under its home country's legislation. Particular attention must be paid to ensuring data protection when instructing processors resident in states not deemed to provide an adequate level of protection.

The circle of countries recognised as ensuring an adequate level of protection of data subjects' rights is defined by Order No. 14 of the Director of the NPDPC dated 15 November 2021 "On Cross-Border Transfer of PD". These include foreign states that are parties to the Convention for the Protection of Individuals with regard to Automatic Processing of PD, as well as foreign states that are members of the EAEU. As their

data-subject rights standards may be lower, the operator must exercise heightened diligence.

Regardless of the authorised person's residence, the operator retains the ultimate obligation to ensure compliance with data subject rights and bears full responsibility for the authorised person's actions.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Belarus law addresses data inaccuracy primarily through the principle of accuracy, which obliges operators to ensure that PD (including health data) are accurate and, where necessary, kept up to date. Complementing this, Article 11(4) grants data subjects the right to request correction of incomplete, outdated, or inaccurate data, provided they submit supporting documentary evidence. Operators must review such requests and either make the correction or provide a reasoned refusal.

The legal framework does not contain specific provisions addressing algorithmic bias, automated decision-making, or systemic discrimination in the processing of PD – including health data. There is no statutory right to human review of automated decisions, nor are there sector-specific anti-discrimination safeguards tied to health data analytics, AI-driven diagnostics, or risk-scoring models. That said, according to available information and statements by representatives of the NPDPC, the issue of introducing provisions on automated decision-making may be addressed in the forthcoming revision of the Belarusian Data Protection Act, which is scheduled for 2026 pursuant to Decree of the President of the Republic of Belarus No. 400 of 18 November 2025 "On the Plan for the Preparation of Draft Legislative Acts for 2026".

That said, Article 4(2) of the Belarusian Data Protection Act requires that processing be proportionate and ensure a "fair balance of interests", which may, in theory, serve as a basis for challenging discriminatory outcomes.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Belarus employs a multi-layered regulatory framework to establish standards for the use and collection of personal health data, combining general data protection rules with sector-specific healthcare regulations (please see question 4.1). Further procedural detail is provided by secondary regulations, such as Order No. 74. This Order establishes the specific standard for obtaining a patient's consent for the inclusion and processing of their data in electronic healthcare information systems within state institutions, mandating the required form and process.

Major national initiatives also act as *de facto* standard-setters. The CHIS, established by Decree of the Council of Ministers No. 267 of 13 May 2021, is a flagship programme aiming to create a unified national digital health infrastructure. Its development inherently creates technical and organisational standards for data collection, storage, and exchange across the healthcare system.

In the Code there was no explicit requirement for written consent to include PD in an organisation's information systems. This signals a potential legislative shift that could simplify and standardise data collection procedures, aligning them more closely with the integrated digital ecosystem being built.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

When sharing personal health data in Belarus, the key considerations involve navigating the intersection of general data protection law and the specific, stringent regime of medical (professional) secrecy under the Law on Healthcare.

For special-category data like health information, the primary bases are a specific statutory exception (*e.g.*, necessity for the provision of healthcare) or the data subject's consent. The information shared typically constitutes a medical secret, which fundamentally restricts disclosure. The patient has the right to determine to whom information about their health may be disclosed or to prohibit disclosure altogether. For minors, this right belongs to their legal representatives – parents, adoptive parents, guardians, or custodians. If the patient is unable to make decisions due to health reasons, disclosure may be made to their spouse or close relatives (including parents, adult children, siblings, grandchildren, and grandparents) who are entitled to receive medical extracts and health certificates in accordance with established procedures. Sharing without such authorisation is permissible only in legally defined exceptions, such as disclosures to certain public authorities for statutory purposes.

If sharing involves transferring data outside Belarus, the requirements of Article 9 of the Belarusian Data Protection Act and NPDPC Order No. 14 of 15 November 2021 apply. Transfers are permitted to jurisdictions deemed to provide an adequate level of protection – for example, parties to Convention 108 and Member States of the EAEU. Transfers to other countries are prohibited unless one of the exceptions under Article 9(1) of the Belarusian Data Protection Act applies, including:

- the data subject's informed consent after being advised of the risks associated with the absence of an adequate level of protection;
- transfer necessary for the performance of a contract with the data subject;
- necessity to protect the life, health, or other vital interests of the data subject or other persons where consent cannot be obtained; or
- prior authorisation granted by the NPDPC.

The data controller must also ensure that adequate legal, organisational, and technical measures under Article 17 are implemented to protect the data.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The sharing of personal health data (including information protected by medical secrecy) is regulated uniformly at the national level. There are no regional variations, waivers, or divergent regulatory regimes.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The regulatory approach to sharing personal health data varies

on the status of the processing entity and the sensitivity of the data, as detailed in the response to question 4.3.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

The standards for sharing healthcare data are established by the same legislative acts that govern its processing (see the answer to question 4.7).

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

There is no specific regulatory framework in Belarus addressing federated models of healthcare data sharing, where data are analysed in a decentralised manner without centralising the datasets.

In the absence of bespoke rules, any model for processing medical data must comply with the general, stringent regulatory landscape for processing and sharing personal health data. The key issues and applicable laws to consider are therefore those outlined throughout sections 4 and 5.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Digital health technologies can be subject to patent protection based on the Law of the Republic of Belarus "On Patents for Inventions, Useful Models, Industrial Designs".

Digital health technologies may be patentable as inventions in Belarus if they constitute a technical solution (product, device, method or its specific medical use) and meet the standard patentability criteria: novelty; level of invention; and industrial applicability.

Only a natural person can be recognised as the author of an invention.

Standalone software without a technical effect by general rule is not patentable, but software integrated with medical devices or methods may qualify.

The patent term for an invention is 20 years from the date of application. In some cases, this period may be extended, but not for more than five years. Additionally, useful models (10 years) and industrial designs can be patented for digital health devices and interfaces.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

In Belarus, copyright protection extends to original works of science, literature, and art, including computer programs (software) and databases, that are the result of creative effort and expressed in a tangible (material or digital) form. Under the Law of the Republic of Belarus "On Copyright and Related Rights", authors-natural persons are granted exclusive rights to reproduce, distribute, modify, publicly perform, and make available their works, including software code and structured databases. The Law also provides for derivative works, collective authorship and work-for-hire regimes for copyright objects. While an author's moral rights are protected indefinitely, protection for exclusive (proprietary) rights is granted for the author's life plus 70 years.

A computer program is protected as a literary work regardless of its functionality. Software may also constitute a complex object of copyright, including databases, images, etc. Copyright in Belarus arises automatically upon creation and does not require formal registration, but there is a procedure for voluntary registration (deposition) with the National Center of Intellectual Property (**NCIP**), which can serve as evidence of authorship and date of creation in case of disputes.

In the context of digital health, this means that the developers of medical software, AI algorithms, and health data platforms enjoy exclusive rights over their code, interface designs, and curated datasets, although these rights do not extend to ideas, methods, or functional principles underlying the software or database.

Copyright objects may include, for example, software, databases, audio and video demonstrations of medical operations, scientific articles or reports, monographs, dissertations and abstracts, including authors' translations of such works, etc.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

In Belarus, the Law "On Commercial Secrecy" protects information that has commercial value due to being unknown to third parties and is subject to a confidentiality regime, but it does not cover state secrets and objects of intellectual property rights such as patents or copyright, except for know-how that is protected within a commercial (trade) secret regime. For digital health technologies, this may include proprietary methods, algorithms, software implementation techniques, or organisational processes, provided the owner implements and enforces a trade secret regime.

Such a regime must include:

- limiting and controlling access to confidential information;
- record-keeping of persons with access;
- employee obligations, including employment contracts and additional non-disclosure agreements;
- contractual obligations for counterparties; and
- designation of responsible personnel to maintain confidentiality.

Protection continues as long as the information remains secret and the trade secret measures are effectively maintained.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

The regulation of academic technology transfer is not detailed in Belarus law as of January 2026.

In Belarus, academic or scientific technology can be created as a work-for-hire within employment or under specific agreements for scientific, research, development, or experimental works.

Work-for-hire within employment: If an employee develops an invention, software, or other intellectual output in the course of performing their official duties (instructions from an employer, using its experience of funds) by general rule the result is considered a work-for-hire. The employee retains moral rights (recognition as author), while the employer by default holds the proprietary rights, including the right to

obtain a patent. In certain cases, obtaining proprietary rights obliges the employer to pay remuneration, with a minimum established by law.

Under scientific agreements: Intellectual property created under research, development, or experimental technology agreements funded by public or private entities is considered part of the results of scientific activity. In these cases, the contractual terms govern ownership, proprietary rights, and obligations to commercialise, while the author retains moral rights. Publicly funded results are subject to mandatory commercialisation requirements, ensuring their use and exploitation in line with the purpose of funding. Please see question 6.7 for more details.

This framework allows both employees of academic institutions and contracted researchers to contribute to digital health technologies, while clearly defining the allocation of moral and proprietary rights and the obligations for commercialisation.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Protection for SaMD is not specifically provided by Belarus law.

Software, as well as databases, is eligible for copyright protection (please see question 6.2). As for medical devices consisting of different components, including software, patent protection may apply (please see question 6.1).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No, an AI device cannot serve as an inventor of a patent in Belarus – only an individual can be the invention creator. The results of AI activities may require indication of an individual as an author to be recognised as patentable.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

In accordance with the Edict of the President of the Republic of Belarus "On Commercialisation of Results of Scientific and Scientific-Technical Activities Created at the Expense of Public Funds", results of such activities created entirely or partially at the expense of public (state) funds shall be subject to mandatory commercialisation in the manner and time provided for by the Edict.

The commercialisation of scientific and technical results, generated through research programmes and innovative projects, is achieved, for example, in the following ways:

- Selling goods created using the results of scientific and technical activities, or using these results for personal needs; granting other parties the right to use the results of scientific and technical activities on a reimbursable basis.
- Full transfer of property rights to the results of scientific and technical activities to other parties on a reimbursable basis.
- Gratuitous transfer of property rights to the results of scientific and technical activities or granting the right to use these results, which are subject to their subsequent commercialisation by the acquirer of these rights, etc.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

No court precedents affecting intellectual property rights protection of digital health innovations are publicly available in Belarus.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

When engaging in collaborative improvements, parties should clearly establish comprehensive contractual set up, especially distribution of rights to intellectual property arising from the collaboration. This includes respective registration formalities, *e.g.*, for patentable objects. Collaborations in digital health often involve the exchange of sensitive information (both business-related and PD or medical secrecy); thus, proper confidentiality regime as well as PD protection compliance shall be ensured. We also recommend to stipulate allocation of liability.

For cross-border collaborations involving a Belarusian resident, it is important to consider regulatory requirements, like currency control and taxation. For medical device or digital health solution improvements that trigger re-registration or new regulatory approvals, the agreement should assign responsibility for regulatory submissions.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

The healthcare sector in Belarus is highly regulated, with healthcare organisations required to operate in full compliance with detailed statutory and regulatory frameworks, including licensing, medical practice, data protection, and digital health requirements. When engaging in collaborations or joint projects, it is therefore essential to draw on the experience of established healthcare organisations to design business and contractual models that support efficient integration and cooperation. Clear allocation of responsibilities is particularly important to ensure compliance with healthcare, regulatory and digital health obligations in Belarus.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Belarus laws do not specifically address federated learning.

Federated learning healthcare data-sharing agreements must comply with general rules for data protection and healthcare data processing to mitigate regulatory risks. Explicit contractual mechanisms to address sufficient legal ground for data processing (like patient consent) and complexities arising from multi-institutional secondary uses of data are recommended. For instance, parties may need to clarify, *inter alia*: (i) which institution obtains initial patient consent and whether additional consent is required from patients treated at secondary participating sites; (ii) how consent is documented

and enforced across the federation; and (iii) how patients exercise data subject rights in a distributed setting. Information security and risks (liability) allocation are also of importance.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Generative AI systems in healthcare create distributed liability complexity absent from traditional software: responsibility for errors may implicate the AI vendor, the healthcare provider deploying the system, the medical specialist relying on the AI output, and potentially the healthcare institution as the employer. Parties should establish explicit liability allocation provisions. There is no well-established practice in Belarus in this regard as of the time of writing.

Nonetheless, parties must consider the general principles governing PD collection and processing, as well as intellectual property rights protection (see sections 4, 5, 6 and 8 for further guidance).

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

As of early 2026, the Republic of Belarus lacks a dedicated regulatory framework or a single principal authority with exclusive enforcement powers over AI and ML.

The Model Law on AI Technologies was adopted by the Interparliamentary Assembly of the CIS in April 2025. In 2025, a cross-ministerial working group was established under the National Academy of Sciences of Belarus's leadership to draft the country's first Law on AI – the development of the draft is expected to be completed in 2026. The institute is also spearheading the creation of a national technical committee for AI standardisation.

The Ministry of Communications and Informatisation acts as the responsible state customer for the overarching State Programme "Digital Belarus" for 2026–2030, which designates digital technologies and AI as a top priority. The Ministry coordinates the implementation of strategic AI initiatives, such as the "Data Economy" subprogramme, ensuring alignment with national industrial policy.

The State Committee for Science and Technology and the Ministry of Economy contribute to the strategic and financial framework for AI development. They support the prioritisation of AI within state research and innovation programmes, as outlined in Presidential Decree No. 135 of 1 April 2025 "On the approval of the priority avenues of scientific, scientific-technical and innovative work in the country for the period of 2026–2030", and manage funding allocation for relevant scientific and technological projects.

The State Standardization Committee is responsible for technical regulation, developing AI standards (*e.g.*, for unmanned vehicles and management systems), and will oversee the newly established national and interstate technical committees on AI standardisation (ITC 566).

The NCIP is actively working to define the legal framework for intellectual property rights related to objects created with the use of AI; the State Committee for Science and Technology also addresses the issue.

In the absence of AI-specific rules, the NPDPC retains authority over AI/ML systems that process PD, enforcing compliance with the Belarusian Data Protection Act, particularly regarding lawful bases, data minimisation, and security.

A comprehensive enforcement mandate for a designated AI regulator may appear in case of development and adoption of the AI law, which is currently under discussion.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

In the absence of AI-specific rules, the most significant applicable horizontal legislation is the Belarusian Data Protection Act. Any AI/ML system processing PD must comply with its core principles as well as the requirements for a legal basis for processing and the mandatory security measures stipulated in Article 17. For healthcare AI, this is critically important, as health data constitute a special category of data and are simultaneously subject to the regime of medical (professional) secrecy under the Law on Healthcare.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Only a natural person can be recognised as the author of a copyright-protected work, including computer programs.

Algorithms themselves (regardless of whether they are developed or refined by humans or AI systems) are not protected by copyright. Established legal interpretation holds that copyright does not extend to methods, processes, systems, or functional elements, even when expressed in a protected work such as software.

Therefore, where an algorithm is improved autonomously by an AI/ML system without active human creative input, no new intellectual property rights arise in favour of the AI system (which is not a legal subject), and no human authorship is established in the absence of personal creative contribution. The resulting output may be used by the operator or developer as a functional tool, but it does not constitute a protectable copyright work.

The NCIP is currently working to clarify intellectual property issues related to AI-generated outputs, with its findings expected to inform the forthcoming Law on AI.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Any dataset containing PD must be processed on a valid legal basis under the Belarusian Data Protection Act and in compliance with the general data processing principles.

Importantly, the sale of PD is fundamentally restricted. According to the official Commentary to the Belarusian Data Protection Act, PD cannot be treated as a "standalone product" or "commodity". Their commercialisation (*i.e.*, buying or selling PD for profit) is considered incompatible with the fundamental legal, ethical, and social principles of privacy and human dignity. Consequently, licensing arrangements must be framed as part of a legitimate service or processing relationship, not as a sale of data.

When licensing healthcare data, such data are classified as special PD and are simultaneously protected as medical secrets under the Law on Healthcare. Use beyond direct medical care generally requires explicit patient consent. Even de-identified health data may be subject to heightened scrutiny if re-identification risks exist, as de-identified data remain within the scope of the Belarusian Data Protection Act.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

The existing and emerging regulatory framework – including strategic documents and the CIS Model Law on AI Technologies – employs a broad, unified definition of AI (as a complex of technological solutions mimicking cognitive functions). The focus of ongoing legislative work is on foundational concepts, institutional setup, and horizontal issues such as safety, certification, and intellectual property, rather than on categorising or creating distinct rules for specific AI subtypes like generative AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

The unique legal issues posed by generative AI in Belarus are not yet addressed by specific regulations and fall under the general application of existing laws. There are no dedicated initiatives solely for regulating generative AI. Its development is being addressed within the broader, ongoing process of creating a comprehensive national AI framework.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Belarus law does not contain data disgorgement provisions or specific rules on AI models trained on unlawfully obtained data. The Belarusian Data Protection Act requires that all processing – including data collection for training AI – be based on a valid legal ground and comply with the general processing principles. If PD were processed without a lawful basis, the operator must cease processing and delete or block the PD. No dedicated legal mechanisms exist to compel the deletion of model weights or to mandate model retraining.

Civil, administrative or criminal liability may apply for unlawful processing. Furthermore, the NPDPC may order the suspension of data processing for up to six months, which could effectively halt an AI service reliant on such data until violations are remedied.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

There are no specific liability rules or theories tailored exclusively to digital health technologies as of the time of writing. Liability for adverse outcomes involving digital health solutions is governed by general civil, administrative and criminal liability frameworks, as well as special orders from responsible state authorities within their powers under Belarus law.

Civil liability may arise for damage caused by negligent performance of medical services or harm from defective digital health products, including compensation for material damage and moral harm to patients, including within the consumer protection regime.

Administrative liability applies for violations of medical practice and information protection or information system compliance (*e.g.*, breach of the medical secrecy regime). For example, unlawful disclosure of medical information, including digital health data, is prohibited and punishable under administrative norms; in addition, administrative sanctions for violations of the PD protection regime include fines for non-compliance with data protection requirements. The NPDPC can also order to suspend PD processing within an information system (resource) in case violations are revealed.

Criminal liability may apply in more serious cases, such as unlawful processing or dissemination of PD without consent that results in significant consequences, or negligence causing serious harm or death. Criminal liability applies only to individuals.

9.2 What cross-border considerations are there?

Extraterritorial effect and special rules for cross-border operations shall be considered. For instance, product safety for import of goods, currency control rules, data protection and information systems compliance (cross-border transfer restrictions for PD and localisation requirements), advertisement and antitrust rules, and counter-sanctions measures (see question 10.3). Practically, the main liability risk lies with the Belarusian counterparty.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

The best practice assumes sufficient legal grounds for data processing, including PD and medical secrecy, introducing comprehensive data protection measures, especially under the Belarusian Data Protection Act, as well as ongoing compliance monitoring and audits, including of data protection measures by engaged third parties and contractual liability allocation, following changes in the legislation and practice, including a sector-specific approach.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

There are currently no theories or measures of accountability in the field of AI/ML models. General liability to misuse of healthcare data may apply.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Information systems (resources) compliance, cybersecurity

and PD protection constitute the primary legal and regulatory considerations in the context of cloud-based services used for digital health purposes. In this regard, reference should be made to the considerations outlined in sections 4 and 5 above.

Entities involved in the processing of data may be subject to certain data localisation requirements under Belarus law. In particular, pursuant to Edict of the President of the Republic of Belarus No. 60 dated 1 February 2010, activities involving the sale of goods, performance of works or provision of services within the territory of Belarus through information networks connected to the Internet must be carried out by Belarusian legal entities or individual entrepreneurs using information systems and resources located and duly registered in Belarus. This rule may affect local providers of cloud-based services within Belarus, as well as local customers using foreign cloud-based services as part of their sales, works or services in Belarus.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

As described above, digital health products and services are subject to strict regulations and under a high level of control. The regulation of the digital healthcare market in Belarus is evolving, having now many areas of uncertainty. To enter the digital healthcare market, companies must review and ensure comprehensive compliance, including to meet the various regulatory, data protection and healthcare compliance requirements.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Investors are advised to carry out thorough regulatory due diligence prior to investing in digital healthcare ventures in Belarus.

Belarus has also introduced "special restrictive measures", *i.e.*, special economic measures and other countermeasures aimed at eliminating (or minimising) the negative effects of foreign states committing so-called unfriendly actions against Belarus. Persons from countries that are undertaking "unfriendly" actions against Belarus are subject to certain restrictions, for instance, in profit distribution or disposal (sale) of shares in Belarusian companies without special permits.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

One of the key barriers to the widespread clinical adoption of digital health solutions in Belarus is the absence of digital health-specific regulations allowing use of such solutions, as well as strict data protection rules. Introducing the Draft Code and its implementation may help with further adoption of digital health technologies, as well as wide use of the CHIS starting from 2026.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Belarus, there are no independent clinician certification or professional accreditation bodies comparable to those operating in certain other jurisdictions that would formally influence the clinical adoption of digital health solutions. Decisions relating to the implementation and use of digital health technologies in clinical practice are predominantly taken at the state level, primarily through coordination between the government and the Ministry of Healthcare.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

The Belarusian legal framework does not currently provide for specific reimbursement models tailored to digital health solutions; it does not establish dedicated certification, registration or approval procedures as a prerequisite for reimbursement by public or private healthcare payors. In the absence of such sector-specific regulation, general legal principles governing reimbursement and liability for harm caused to patients' health apply.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

The regulatory environment governing AI/ML-based solutions in the healthcare sector remains under development. This regulatory immaturity and the absence of detailed, sector-specific guidance may result in uncertainties when assessing compliance requirements for data-driven digital health products. At present, in the absence of dedicated regulation (see section 8), such solutions are subject to general principles and provisions from intellectual property law, data protection and privacy legislation.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

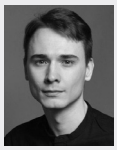
Belarus is in the process of developing and launching a centralised software platform for the CHIS, with the aim of its subsequent implementation. Please refer to questions 1.2 and 3.1 for details. We also recommend following developments relevant to digital healthcare regulations on an EAEU level.



Kirill Laptev is a partner and co-founder of Anischenko Laptev, previously a partner and head of the TMT group in Belarus at an international law firm. He is highly experienced in corporate, commercial and regulatory-related projects, advising, among others, well-known multinational pharma producers and healthcare companies on local matters and distribution models. Kirill has been mentioned by international directories such as *The Legal 500* in Commercial, Corporate and M&A, as well as IP and Dispute Resolution.
Kirill's profile covers: expansion of well-known global pharmaceutical producers to the Belarus market; legal review of local counterparties; developing new viable and efficient set-up for carrying out their business operations in the Eurasian Economic Union, from a Belarus law perspective; and localisation of foreign clients' contractual documents under Belarus laws for launching a new implanted device and respective monitoring software system, including in terms of a contractual model with clinics in Belarus.

Anischenko Laptev
ul Internatsionalnaya 36-1
220030 Minsk
Belarus

Tel: +375 29 339 4590
Email: laptev@al.legal
LinkedIn: www.linkedin.com/in/kirill-laptev



Vladislav Zhavnerchik is counsel and head of Digitalisation and Data Protection at Anischenko Laptev. Prior to joining the team, he has extensive experience in regulatory matters, having served as DPO and lead counsel at one of the largest Belarusian infrastructure providers. Vladislav has provided strategic legal guidance to private healthcare providers navigating stringent data protection requirements under Belarus law. Notably, he led a rapid-response engagement for a private medical clinic facing an enforcement inquiry from the national data protection authority. His team successfully negotiated an extension of the compliance deadline from one month to five – providing the clinic with sufficient time to implement necessary structural and procedural changes without disrupting its core operations.

Anischenko Laptev
ul Internatsionalnaya 36-1
220030 Minsk
Belarus

Tel: +375 44 559 9267
Email: v.zhavnerchik@al.legal
LinkedIn: www.linkedin.com/in/zhaunerchyk



Anastasiya Pyshnaya-Muryna is an associate at Anischenko Laptev; her practice focuses on corporate, commercial, antitrust and regulatory issues, specialising in the Healthcare and Pharmaceuticals sector. Her experience includes assisting globally recognised companies on corporate, competition and licensing issues, *e.g.*, in entering contracts with potential suppliers and potential violations of competition law. She also specialised in compliance for international companies with Belarus regulations, as well as guiding international pharmaceutical companies on market entry and licensing agreement execution. She is passionate about ESG providing guidance on compliance.

Anischenko Laptev
ul Internatsionalnaya 36-1
220030 Minsk
Belarus

Tel: +375 33 314 9358
Email: a.pyshnaya-muryna@al.legal
LinkedIn: www.linkedin.com/in/a-pyshnayamuryna



Anna Zhdanovich is an associate at Anischenko Laptev with considerable experience in contract, corporate and labour law. Her experience encompasses organising and conducting legal due diligence with subsequent preparation of reports for well-known foreign and local companies, particularly on intellectual property matters. She has also participated in projects involving the provision of legal advice on complex corporate matters, as well as the establishment of corporate presence and drafting transactional documentation.
Prior to joining the team, Anna developed substantial practical experience at another Belarusian leading law firm. Her experience includes drafting and reviewing diverse contractual arrangements with international counterparties, including from Europe, the United States and China. Anna also provided legal guidance to representatives of foreign pharmaceutical companies on the activities of the botex plant.

Anischenko Laptev
ul Internatsionalnaya 36-1
220030 Minsk
Belarus

Tel: +375 25 673 0789
Email: a.zhdanovich@al.legal
LinkedIn: www.linkedin.com/in/anna-zhdanovich-al

Anischenko Laptev (AL Legal LLC) is a leading Belarusian full-service business law firm, founded by two partners following a friendly separation from the international law firm Sorainen, which exited the Belarusian market. Based in Minsk, Anischenko Laptev combines deep local insight with extensive international expertise, offering a comprehensive suite of legal services to both Belarusian businesses and foreign clients operating in or entering Belarus.
With the team's significant experience in the Belarusian legal market, the firm is recognised for its strong foundations in corporate, transactional and regulatory law, coupled with a forward-looking approach to ESG responsibility, technology-enabled service delivery, and global business trends.

www.al.legal

ANISCHENKO LAPTEV

Belgium

Quinz


Olivier Van Obberghen


Pieter Wyckmans


Amber Cockx


Chaline Sempels

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

While more than one definition exists, digital health or e-health is generally described as "the use of information and communication technologies within healthcare to optimise patient care".

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Belgium's digital health subsectors continue to diversify across the life sciences value chain and into the patient journey with a focus on remote, personalised, precision and preventative care. While patient-facing health and wellness apps have been around for a while now, we observe a growing number of provider-focused digital health tools, including AI-driven clinical decision support and remote patient monitoring tools.

1.3 What is the digital health market size for your jurisdiction?

There are currently no official statistics available that provide a clear overview of the size of the Belgian digital health market due to the broadness of the concept of digital health and the difficulty of delineating its boundaries. According to Agoria, Belgium's largest industry federation for technology companies (including its dedicated HealthTech Cluster), over 450 companies develop health technology solutions in Belgium, generating more than EUR 3 billion in value added to the Belgian economy.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

In line with question 1.3, no definite statistics on Belgium's largest digital health companies exist. Belgium's digital health landscape is populated by multinational (tech) corporations headquartered abroad, biotech and pharmaceutical companies venturing into digital branches and a large number of MedTech companies and fast-growing start-ups, scale-ups and spin-offs. BeMedTech is the Belgian federation representing the medical technology industry, encompassing nearly 200 companies that account for 80% of the market in Belgium. Their website features a list of prominent digital health companies. A key ecosystem accelerator is Imec, Belgium's world-leading semiconductor R&D hub, whose sensor chips and low-power edge-AI hardware underpin many next-generation medical devices and secure on-device AI applications.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

See our response to question 1.4.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

First, the Belgian National Institute for Health and Disability Insurance (NIHDI) is responsible for establishing reimbursement schemes for healthcare services, health products and medicines. Further, the Federal Agency for Medicines and Health Products (FAMHP), in cooperation with the European Medicines Agency (EMA), supervises the quality, safety and efficacy of medicines and health products and enforces the legislation applicable thereto. The Institute for Public Health (Sciensano) monitors public health and diseases and evaluates the effectiveness and safety of vaccines, medicines and health products and was therefore of paramount importance during the COVID-19 pandemic. Additionally, professional associations such as the Order of Physicians and the Order of Pharmacists regulate the deontological aspects of healthcare professions, while the self-regulatory organisations Pharma.be and BeMedTech provide industry guidance. The Belgian Data Protection Authority (DPA) enforces compliance with data protection legislation and the recently established Health Data Authority oversees the sharing and use of healthcare data. Authorities overseeing recent digital health and data legislation include FPS BOSA, acting as Belgium's single information point for the implementation of the EU Data Governance Act, and the Health Data Authority, which now coordinates governance and oversight of electronic health data access and secure data sharing frameworks.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

- Act on the Performance of the Healthcare Professions of 10 May 2015.
- Act on Hospitals and Other Care Facilities of 10 July 2008.
- Health Care Quality of Practice Act of 22 April 2019.
- Patients' Rights Act of 22 August 2002.
- Law on Medicines of 25 March 1964.
- EU Regulation 2017/745 on Medical Devices (MDR); Medical Devices Act of 22 December 2020; EU Regulation 2017/746 on *In Vitro* Diagnostic Medical Devices (IVDMDR) of 5 April 2017; and *In Vitro* Diagnostic Medical Devices Act of 15 June 2022.
- Law on Experiments with Humans of 7 May 2004; EU Regulation 536/2014 on clinical trials on medicinal products for human use of 16 April 2014.

Additionally, Belgium is now in the first full supervisory cycle of key EU digital and data legislation, which applies cumulatively where digital health solutions involve software, AI or health data processing, including the Digital Services Act, the AI Act (AIA), the Data Governance Act, the Data Act and the European Health Data Space Regulation.

Furthermore, horizontal Belgian and EU regulatory frameworks continue to apply to digital health and healthcare IT, including personal data protection law, e-commerce and consumer protection, competition law, and unfair commercial practices, product safety and cybersecurity requirements.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The DPA and the Market Court in Brussels are responsible for investigating and enforcing penalties for data protection infringements. In addition, the FAMHP can take administrative sanctions and restrict the placing of medicines and health products on the market. The EU Commission and the Belgian Competition Authority implement the competition policy on the Belgian market, while the public prosecutor's office investigates, prosecutes and brings to judgment offences that are criminally curbed. The AIA is expected to become an emerging area of enforcement, with potential fines reaching up to EUR 35 million or 7% of the consolidated annual turnover.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

If software is considered a medical device (for more information on this classification, see question 3.1) or an accessory to a medical device, the Medical Devices Act of 22 December 2020, the MDR and/or the IVDMDR will apply, depending on the type of medical device. The Belgian national regulatory framework was brought in line with the MDR and IVDMDR by the Acts of 22 December 2020 and 15 June 2022 and a Royal Decree of 13 September 2022. Prior to being placed on the market, medical devices must undergo a clinical evaluation and conformity assessment to review the safety and performance of the device. Demonstrating conformity is in the first instance the responsibility of the device manufacturer. For most medical devices (except for class I medical devices), the conformity then needs to be confirmed by a "notified body" designated by the Belgian (or another EU Member State's) government. In addition, medical devices need to be traceable throughout the supply chain up until the end-user. The FAMHP is responsible for post-market surveillance of (software as a) medical device. On 16 December 2025, the European Commission published a proposal to amend the MDR/IVDR aimed at simplifying and reducing the regulatory burden. If adopted, it may affect SaMD, for instance, by adjusting software classification rules, easing clinical evidence concepts and progressing towards risk-based periodic reviews.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Software that is powered by AI/Machine Learning (ML) is first of all governed by the same regime as other software (see question 2.4).

If AI/ML-powered digital health devices or software solutions fall within the scope of the MDR or the IVMDR, they must thus be CE-marked (after having completed a successful conformity assessment) before being placed on the market. In addition, where such functionalities meet the criteria for high-risk AI systems under the AIA, which entered into force on 1 August 2024 with substantive high-risk obligations phasing in throughout 2026, manufacturers must prepare to satisfy overlapping AIA requirements alongside their MDR/IVDMDR obligations. Belgian authorities have also issued specific guidance on in-house medical device software under the MDR, clarifying compliance obligations for healthcare institutions developing their own medical software.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Please see question 10.7 regarding the dynamic nature of AI/ML-based digital health solutions. Belgian authorities are increasingly seeking to adapt static approval and reimbursement frameworks to better accommodate digital health innovation. In this context, the 2025 federal coalition agreement expressly calls for the exploration of a temporary reimbursement mechanism for digital health applications (notably at level 3 of the mHealthBelgium validation pyramid), allowing further real-world data collection prior to permanent reimbursement where sufficient clinical added value is demonstrated. Although the mHealthBelgium validation pyramid has been slightly revised in recent years, the limited number of fully reimbursed applications highlights persistent shortcomings. Reimbursement remains largely pilot- or project-based (for example, certain applications for the telemonitoring of chronic heart failure are reimbursed where hospitals conclude specific agreements with the NIHDI), rather than embedded in a systematic framework. At EU level, regulatory evolution is reinforced by initiatives such as the EMA/Heads of Medicines Agencies Data and AI workplan to 2028, which promotes the structured use of data and AI (including real-world evidence) in regulatory decision-making.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

As noted above, the MDR and IVDMDR require clinical evidence (i.e. demonstrating safety, efficacy and clinical benefit) for medical devices before such devices can be placed on the market. If classified as a medical device (see question 3.1), an AI/ML-based digital health solution will generally fall into a higher risk class, requiring a more stringent clinical assessment. Clinical validation requirements for AI/ML-based digital health solutions will increasingly be assessed in parallel with obligations under the AIA, once applicable, including expectations around data quality, performance monitoring, bias mitigation and post-market surveillance.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Belgium has a complex healthcare landscape with fragmented political competences and sometimes divergent approaches. The Belgian federal government is responsible for laying out Belgium's general healthcare policy, supervises the (placing on the market of) medicines and healthcare products, and oversees the regulation and financing of compulsory health insurance, as well as the funding of hospital services. On the other hand, the Communities (the Flemish Community, the French Community and the German-speaking Community) are responsible for health promotion and prevention, and for the recognition and quality assurance of healthcare providers (HCPs) and healthcare institutions. In other words, the approval and post-market surveillance of digital health products and solutions are primarily a federal responsibility, whereas the use of such solutions in clinical practice is overseen by the Communities. The creation of a Belgian Integrated Health Record (BIHR) should improve cooperation between the various government bodies involved (see below).

A dedicated chapter of the Flemish Government's coalition agreement 2024–2029 focuses on the digitisation of healthcare, highlighting the importance of empowering patients to manage their health without needing to visit doctors or hospitals. The Flemish Government intends to promote the use of digital health applications and technologies to alleviate the burden on HCPs and enhance the quality of care. A similar sentiment is ushered in the Federal Coalition agreement of 2025.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

As stated above (see question 2.3), the main areas of enforcement in digital health concern data protection infringements, violations of rules governing the marketing and sale of medical devices, and competition considerations. The DPA's governance plan of 2025 indicates that its litigation chamber wishes to focus on a limited number of high-impact cases arising in the context of the European digital package.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Belgium does not have an all-encompassing framework on telemedicine yet and there has been long-term opposition against consultations at a distance where a diagnosis of the patient is made, especially by the National Council of the Order of Physicians (NCOP). Concerns mainly related to the quality and credibility of online HCPs, and the privacy and security of patient data. There has, however, been a switch in mindset. As from 2022, teleconsultations – complementary to face-to-face patient care – are acceptable under certain conditions. In particular, amongst other requirements: (i) the duration and circumstances of the teleconsultation must be sufficient to guarantee the quality of care; (ii) the physician needs to be able to verify whether there is consent of the patient and there is an adequate therapeutic relationship between the patient and the physician established; (iii) the continuity of care must be warranted (e.g. by completing the patient's electronic patient record); and (iv) any prescriptions must be made through the official system for electronic prescriptions, Recip-e. Importantly, due to budgetary constraints, the reimbursement of tele-consultations has been temporarily halted by the NIHDI (although certain video-consultations are still reimbursed).
- **Robotics**
  Although the traditional rules regarding (contractual, extracontractual, medical and product) liability apply (see question 9.1 below), it may be difficult for a patient suffering damage due to robot-assisted surgery to assess the most suitable remedy for their claim and the current EU and national liability framework may prove to be inadequate.
- **Wearables**
  Wearables are subject to considerably different regulatory frameworks based on their classification as a medical device or not. The decisive criteria to determine whether a wearable constitutes a medical device is to establish whether the instrument, appliance or software is intended to be used for one of the medical purposes in art. 2(1) of the MDR (e.g. for the diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of a disease or disability). The medical devices framework is relatively burdensome, giving manufacturers an incentive to indicate that their health product is not intended to be used for one of these medical purposes in order to avoid having to comply with the MDR. On the other hand, reimbursement for wearables is currently limited to CE-certified medical devices (see further under "Mobile Apps").
- **Virtual Assistants (e.g. Alexa)**
  Virtual (voice) assistants (VVAs) have ample applications in healthcare settings. They can aid in clinical notetaking, in assisting an ageing population or patients suffering from mobility issues, in medication management and in health information-seeking activities. However, data protection and privacy concerns have been raised by (amongst others) the European Data Protection Board (EDPB) in its Guidelines 02/2021 on VVAs. Careful consideration must be given to the legal

basis of the processing of personal data by virtual assistants under art. 6 of the GDPR and the requirements of art. 5(3) of the Directive 2002/58/EC on privacy and electronic communications (which long-awaited revision has been withdrawn on EU level), as transposed into Belgian law by the Electronic Communications Act of 13 June 2005. Since VVAs require processing of biometric data for user identification, an exemption under art. 9 of the GDPR must also be sought. Other data protection challenges have also been raised, for example regarding the data minimisation principle and the accidental collection of personal data or the collection of background noise or other individuals' voices besides the user. The European Commission has also voiced antitrust concerns about virtual assistants in light of its consumer Internet of Things (IoT) inquiry. These concerns included the high entry and expansion barriers of the technology, certain exclusivity and tying issues, the lack of interoperability, the large amounts of data feeding into the technology and VVAs functioning as intermediaries between the user and smart devices or IoT services. The Digital Markets Act is relevant for virtual assistant services because they fall within the definition of "core platform services" and are often provided by large platforms that have been designated as gatekeepers.

- **Mobile Apps**
  Since January 2021, mobile apps that meet all the criteria of the mHealth Belgium validation pyramid can be reimbursed. In the first instance, they need to be CE-certified as a medical device and meet the requirements of the GDPR. Secondly, they need to pass certain interoperability and connectivity criteria. Lastly, a socio-economic benefit must be demonstrated in order to receive reimbursement by the NIHDI. Up until now, the success of the validation pyramid has been limited, as proving the socio-economic importance of apps remains difficult (see also question 2.6 above). Note that mobile apps can also be financed by other payers such as hospitals, healthcare professionals or health insurance companies. Nonetheless, some other issues concerning mobile apps remain. For example, if mobile health apps are used in healthcare and prescribed by a healthcare professional, patients that do not have access to the Internet may be discriminated and the patients' rights under the Patients' Rights Act need to be respected, such as the right to quality healthcare. With regard to the GDPR, the Belgian DPA has issued guidelines specifically tailored for mobile health apps. Mobile apps may be classified as a medical device if intended to be used for medical purposes and may consequently have to comply with the MDR/IVDMDR framework, while other apps may be considered a wellness or lifestyle device. While such wellness devices are not primarily regulated as medical devices, the collection and processing of any personal data through these apps must comply with the GDPR. In addition, the European Health Data Space and, where applicable, the Data Act may impose additional obligations concerning the governance, access and sharing of data generated by such devices.
- **Software as a Medical Device**
  The classification of Software as a Medical Device (SaMD) suffers from the same shortcomings as the ones for wearables and mobile apps. Software will be considered a medical device if: (i) it is intended by its manufacturer to have a medical purpose or if the software meets the definition of an "accessory" for a medical device; (ii) it performs an action on data that goes beyond storage, archival, communication or simple search; and (iii) it is for the benefit of individual patients. As said, classification as a medical device has consequences for the regulatory framework that applies to software.
- **Clinical Decision Support Software**
  Besides the undeniable ethical challenges, clinical decision support software (CDSS) raises a number of legal issues. It is, for example, uncertain which party will be responsible in the event of a medical accident as a result of a decision made on the basis of CDSS. In addition, there are data protection and medical confidentiality concerns, for instance if the patient data that is submitted to the CDSS is used, not only to render a medical decision concerning the relevant patient, but also to improve the CDSS or for other business purposes of the CDSS manufacturer. Where CDSS qualifies as AI-based software, it may also fall within the scope of the AIA as a high-risk AI system, triggering additional obligations on risk management, data governance, human oversight and post-market monitoring. As further set out below, due to the requirements of the GDPR in relation to automatic decision-making, human intervention by a healthcare professional before making a final medical decision is in any case advised.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  A key barrier in the widespread implementation of AI/ML-powered solutions in healthcare concerns the massive amounts of special-category personal data that are often needed for the optimal functioning of these devices and the accompanying data protection aspects, for example in relation to automated decision-making by AI/ML-powered solutions. The exercise by the data subject of certain rights, such as the right to access and erase personal data might (technically) also be notably difficult. Besides data protection, the interplay of the AIA and the MDR results in stringent requirements for AI-powered medical devices. Any AI-powered medical device that must undergo a conformity assessment procedure by a notified body is considered as a high-risk AI system within the meaning of the AIA (art. 6 and Annex III of the AIA), subject to strict monitoring obligations. Since most SaMD will be classified as Class IIA or higher and must therefore undergo a conformity assessment, the majority of AI/ML-powered medical devices will be deemed to be high risk under the AIA.
- **IoT (Internet of Things) and Connected Devices**
  While IoT and connected devices offer significant advantages for patients (e.g. assisted living), physicians (e.g. telemonitoring) and hospitals (e.g. stock management and patient identification), they raise important privacy, data protection and cybersecurity concerns. In addition, the EU's recent digital legislative package, including the Data Act and European Health Data Space introduces new obligations relating to data access and sharing, interoperability and risk management, which are particularly relevant for connected medical and health-related devices.
- **3D Printing/Bioprinting**
  Legal considerations on bioprinting include IP questions (copyright, patentability and design rights of techniques and materials), the classification of the bioprinted product (as medical device or (advanced therapy) medicinal product) and the liability of the variety of actors involved.

- **Digital Therapeutics**
  DTx have great potential in shifting healthcare to be more personalised, preventative and patient-centred. The downside, however, includes major concerns relating to cybersecurity, data protection and privacy. By using digital implements such as mobile devices, sensors and IoT, DTx transfers enormous amounts of personal information over the Internet and hence, risks of unauthorised access and manipulation of these products and underlying data (e.g. further use of real-world evidence) could compromise both trust in the product and patient care. Since some of the key therapeutic areas of DTx include cognitive behavioural therapy and lifestyle management (e.g. for patients with chronic conditions), it may be especially difficult to distinguish whether a DTx solution is a medical device or not. Unless it concerns a mobile app or a medical device, the financing for DTx is also uncertain.
- **Digital Diagnostics**
  Digital diagnostics are tools used in the diagnosis of medical conditions or for measurement of health parameters (e.g. digital biomarkers). Such tools will often qualify as a medical device or an *in vitro* diagnostic medical device, depending on the intended use and functionalities of the product. The classification of a medical device and *in vitro* diagnostic medical device determines the regulatory requirements associated with the product and the conformity assessment which the product must undergo prior to being placed on the market. Many digital diagnostic tools now embed AI components, giving rise to additional regulatory considerations, as set out above.
- **Electronic Medical Record Management Solutions**
  Belgium is among the frontrunners in Europe in the digitalisation of patient records, with the storage of patient information in an electronic medical record being mandatory pursuant to Article 34 of the Belgian Health Care Quality of Practice Act. The patient's right to privacy and to a carefully kept patient record (arts 9 and 10 of the Act of 22 August 2002 on Patients' Rights and arts 33–40 of the Health Care Quality of Practice Act of 22 September 2019) needs to be taken into account when processing, storing and accessing patient health information via electronic medical records. The Belgian National Commission of Representatives of Physicians and Health insurance funds has also issued a list of acceptable electronic medical record software providers to avoid interconnectivity or security issues. Furthermore, the Regulation establishing the European Health Data Space includes technical requirements for electronic health record systems to ensure the security of such systems and their interoperability across the EU, facilitating the exchange of health data between systems from different manufacturers.
- **Big Data Analytics**
  ML and AI systems are trained on large amounts of data, which are examined to identify trends, patterns and correlations. The insights resulting from such advanced analytical process allow the system (or its user) to make data-informed decisions in the future. As already explained above (see Artificial Intelligence/Machine Learning-Powered Digital Health Solutions), ensuring compliance with data protection legislation can be challenging. When data collected in a specific (medical) context are being used to develop and/or improve a system or for other business objectives, the legal basis providing the justification for the initial data collection and processing might not cover such secondary use. The interplay between GDPR and the AIA brings about additional complexities.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain technology enables secure decentralised data sharing, while providing the possibility to monitor, trace and revoke data exchanges. This enhances security, data privacy and efficiency in the storage and management of the large amounts of data involved in IoT devices. In February of 2023, the European Commission introduced the "European Blockchain Regulatory Sandbox for innovative use cases involving Distributed Ledger Technologies", establishing a pan-European framework for cross-border dialogue between regulators and supervisors on the one hand, and (private or public) developers of blockchain use cases on the other hand. Data solutions are now also increasingly assessed alongside horizontal EU data frameworks, including the GDPR, the European Health Data Space and the Data Act.
- **Natural Language Processing**
  Natural language processing (NLP) technology raises data protection and confidentiality concerns similar to those associated with virtual assistants (see above), particularly where large volumes of free-text patient data are processed. In healthcare settings, NLP is increasingly used to extract, structure and analyse unstructured clinical data (such as medical notes, discharge summaries and clinical correspondence). Healthcare professionals may nevertheless encounter interoperability challenges, as well as risks of language-based bias or discrimination. NLP also raises broader ethical and legal issues relating to transparency, explainability, fairness and accountability. Where NLP solutions are AI-driven, compliance with the AIA must also be taken into account, in addition to applicable data protection requirements.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The EU Digital Services Act imposes extensive transparency obligations on intermediary service providers (including providers of digital platform services) and requires them to designate a single point of contact for communications with authorities and users. In addition, to avoid liability, if the provider gains knowledge of an infringement committed through its services, it needs to act expeditiously to remove or to disable access to the illegal activity or illegal content concerned and it needs to inform the public prosecutor of such infringement. Even more obligations are imposed on online platforms (a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public) and very large online platforms (platforms with over 45 million active users monthly), which have to put in place measures to actively counter the spreading of illegal goods, services or content online, such as mechanisms to identify sellers of goods and buttons for users to flag illegal content.

Digital platforms offering remote consultations with doctors need to take into account the quality standards set by the Health Care Quality of Practice Act, as well as the conditions listed in question 3.1 under "Telemedicine". For example, consultations organised through a digital platform will not always be eligible for reimbursement, as one of the conditions for reimbursement holds that the doctor and patient have an existing treatment relationship (i.e. the doctor is the patient's

primary care physician, the patient physically visited the doctor at least once in the past calendar year or the patient was referred to the doctor-specialist by another doctor).

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

As in most jurisdictions, the use and processing of personal data in healthcare in Belgium has drastically changed over the last decades. In the past, a patient's medical records were usually stored by their treating physician in a paper version and were solely used for the purposes of treatment. With the introduction of e-health, other actors have entered the process, resulting in greater risks of privacy and/or data protection breaches. Under the GDPR and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data, data related to health are considered as "sensitive personal data" or a "special category of personal data". In principle, such data cannot be processed unless a valid legal basis can be found and an exception applies, e.g. informed consent, medical diagnosis by someone under the obligation of professional secrecy, reasons of public interest in the area of public health, etc. (arts 6 and 9 of the GDPR). The right to privacy (art. 8 of the European Convention of Human Rights, art. 7 of the Charter of the EU and art. 22 of the Constitution) and the right to data protection (art. 8 of the Charter of the EU, art. 16 of the Treaty on the Functioning of the EU and art. 10 of the Act on Patients' Rights) of a patient need to be reconciled with the advantages of the processing and sharing of certain medical data. On an individual basis, electronic health records and the automatic processing of personal data may facilitate long-term follow-up by several different HCPs. On a larger scale, (big) data analyses of personal data may increase the quality and efficiency of healthcare, offer predictive therapeutic models and allow for the personalised care of patients. In January 2024, the Data Act came into effect, aiming to set clearer rules for individuals and businesses on the use of both personal and non-personal data generated by connected objects, also known as the "Internet of Things" and applying, amongst others, to medical and health devices. Furthermore, the European Health Data Space, which will be phased in over the next few years, establishes a dedicated framework for the primary and secondary use of electronic health data.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The implementation and enforcement of the GDPR in Belgium is primarily governed at the federal level by the Belgian DPA and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data. In addition, sector-specific health data governance is increasingly coordinated at the federal level through the Health Data Agency and the BIHR project, a national framework to ensure interoperability and secure access and use of health data.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

As a consequence of the introduction of e-health, the personal data of patients are no longer solely processed by physicians and other HCPs, who are bound by professional secrecy under the penalty of criminal sanctions in accordance with art. 458 of the Criminal Code (art. 25 of the Code of Medical Ethics of the NCOP). Employees of the medical devices industry or health app providers may be in direct contact with patients and process their personal data. Under the GDPR, one may only process personal health-related data when one of the grounds of art. 9.2 applies. Personal data may be processed for purposes of preventive or occupational medicine, medical diagnosis or the provision of health or social care treatment, but this may only be done under the responsibility of a professional subject to the obligation of professional secrecy (arts 9.2(h) and 9.3 of the GDPR). Accordingly, health app providers cannot benefit from this provision and will have to rely on any of the other exceptions in art. 9 (e.g. freely given, specific and informed consent (art. 9.2(a)), where processing is necessary for reasons of public interest in the area of public health (art. 9.2(i)) or where processing is necessary for scientific research purposes (art. 9.2(j)).

4.4 How do the regulations define the scope of personal health data use?

The GDPR and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data adopt a definition of "processing", which includes nearly any action or operation related to personal data: "'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (Art. 4.2 of the GDPR and arts 5 and 26.2 of the Law on the Protection of Natural Persons with regard to the Processing of Personal Data.) Personal information related to health, as well as genetic and biometric data used for identification purposes, is classified as sensitive personal data or special category data under arts 9 of the GDPR and 10 of the Law on the Protection of Natural Persons with regard to the Processing of Personal Data. The processing of such data is generally prohibited unless a valid justification is provided. Consequently, health-related personal data can only be processed in exceptional circumstances.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

When more than one party is involved in the processing of (health-related) personal information, both territorial aspects and the relationship between the parties need to be considered. On the one hand, compliance with the GDPR and national implementing laws is required when the controller or processor of personal data is established in the EU, as well as when the processing of personal data concerns data subjects

who are located in the EU (if related to the offering of goods and services or the monitoring of behaviour of data subjects within the EU). If personal data that is subject to the GDPR is transferred to a controller or processor outside the EEA (not normally subject to the GDPR), a transfer mechanism (such as the (updated) standard contractual clauses) needs to be implemented and a transfer impact assessment may be necessary. On the other hand, it is essential to allocate the rights and responsibilities of each actor involved in the processing. Whenever a processor processes data on behalf of a controller, a data processing agreement must be concluded (art. 28.3 of the GDPR). This is the case if a physician makes use of a medical device for the diagnosis of their patients and personal data will be processed by the medical device provider for such healthcare purposes. If such provider also processes personal data for its own purposes and means (e.g. to improve its products and services), such provider may – in addition – be considered a controller, for which the GDPR does not require a specific agreement. Further, if the physician and medical device provider jointly determine the purposes and means of the processing and thus relate to each other as joint controllers, the parties must conclude a transparency agreement (art. 26 of the GDPR). Furthermore, in B2B relations, the Data Act bans unfair contractual terms related to data access or usage. It also provides a list of clauses that are always deemed unfair and another list of clauses that are presumed to be unfair.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The principle of data accuracy and the right to rectification (art. 5(1)(d) of the GDPR) of incorrect personal data (art. 16 of the GDPR) about oneself are closely connected. The Knowledge Centre for Data and Society considers that the more important the data is for training an AI system, the greater the effort must be to verify that it is correct or needs to be adjusted. The datasets used to train or "feed" AI systems must be sufficiently reviewed to ensure they do not incorporate bias or prejudice that may reinforce discrimination and socio-economic injustice. Issues arise also in relation to the data subject's right not to be subject to a decision made solely by automated means, especially if the decision has a considerable impact on the data subject. As a consequence, decision-making by AI must be transparent and verifiable (there must be an "explainability" of decisions made by AI systems, AI systems must be auditable or at least suitable for *post-hoc* interpretability). If this review does not happen on a regular basis, the use of an AI system could lead, for example, to discrimination based on historical data patterns contrary to the Gender Act, the Anti-Racism Act and the Anti-Discrimination Act.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The GDPR maintains high data protection standards, including a purpose limitation principle, meaning that personal data that is collected for a certain purpose cannot be used for a new and incompatible purpose (art. 5.1(b) of the GDPR). It is thus important to establish all purposes for which the personal data will be used at the time of collection. This is particularly relevant in the context of clinical trials. All too often, personal data collected in the course of a clinical trial (first use) may become of interest for the use in other research, independent of this clinical trial (further use). The purpose limitation principle prohibits further processing of personal data incompatible with the initial purpose; however, further processing in accordance with art. 89(1) of the GDPR for scientific research purposes shall not be considered incompatible with the initial purpose. Nonetheless, if the legal basis for the further processing of personal data (secondary use) is consent under art. 6.1(a) of the GDPR, this may pose certain problems. Consent must be freely given, specific, informed and unambiguous. However, often at the beginning of the clinical trial (first use) when consent of the data subject is sought, it is not yet entirely clear for which further research purposes the personal data may also be used (further use). Fortunately, recital 33 of the GDPR allows for some flexibility in this regard and notes that data subjects should be permitted to give their consent for the further use of their personal data for scientific research on a more general level. Ensuring that data subjects give their consent at the time of collection for all purposes for which one intends to use the personal data is good practice and avoids the situation where one would have to go back to the data subject to ask for consent for additional purposes.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In order to assure confidence of a patient in the healthcare industry and protect an individual's data and privacy, adequate safeguards must be provided to ensure personal data is not shared with third parties without a patient's knowledge and/or without their consent (if the legal basis for the processing of personal data is consent). In an information society, the obligation to professional secrecy no longer suffices to protect a patient's medical data. In this context, it is highly recommended to enter into a data sharing agreement addressing what data can be shared, who has the authority to access the data and which security measures are required, especially when there is a large number of parties involved in the processing of personal data. These considerations are also at the forefront of the European Health Data Space project, intended to facilitate the use and sharing of European health records to boost the availability of qualitative health data in the EU, both for the purpose of providing healthcare services and for "secondary purposes" such as research and policy-making.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As mentioned above, the GDPR is implemented and enforced on a national level. The Belgian Health Data Agency is specifically tasked with the governance of health data sharing.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Data protection laws must ensure that the personal data collected by a physician, a medical device or a health app is, on

the one hand, not shared with, for example, insurance companies but, on the other hand, can be consulted by a physician administering emergency care. The Data Act outlines the conditions under which public sector bodies and specific EU institutions, like the European Commission, can request data holders to provide access to data necessary for fulfilling their statutory duties in the public interest.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Since 2008, a national e-Health platform has been established, where HCPs upload electronic health records of a patient to allow all other HCPs having a therapeutic relationship with that same patient to access and review such records in a secure way. One of the common themes in the Belgian eHealth Action Plan 2025–2027 is the development of a BIHR, a more advanced model of data exchange via a central digital platform that should allow for closer collaboration between all actors in health to ensure a seamless continuum of care for the patient. One of the objectives is to make the "real-world data" from the BIHR available as "routinely collected data" and increase the documentation, findability, accessibility, quality and reusability of the data. In relation thereto, a Belgian Health Data Agency has been established to supervise secondary use of health data and, more generally, play a facilitating role in the exchange of health data for research purposes.

The EU Data Governance Act aims to facilitate the sharing of data that are in the possession of government agencies and are not to be made publicly available, for commercial and non-commercial reuse. Under the Data Governance Act, each government should establish an easily accessible central location where all relevant information is available and through which requests for data access or reuse can be submitted. For the Belgian federal government, the FPS Policy and Support (BOSA) is designated as the central information point. A Royal Decree of December 2024 restricts access to patient health data to healthcare professionals acting with a therapeutic purpose and introduces stricter informed-consent requirements for data sharing between HCPs.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Federated learning avoids the exchange of raw data between the parties. Instead, the models trained on each local dataset are shared and aggregated. While this form of collaborative model training offers clear benefits in terms of data minimisation and quality of training, data leakage and security concerns are still present. Other issues relate to data processing roles and responsibilities and secondary data use, as further discussed below (see question 7.3).

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Since there are no specific intellectual property (IP) regimes for digital health technologies, the scope of protection is defined by applicable traditional regimes. Inventions, in all fields of technology, are patentable if they are new (in other words, they are not part of the state of the art), if they are the result of the inventiveness or resourcefulness of the inventor, if they are capable of industrial application, and lawful (Title 1 of Book XI of the Code of Economic Law (CEL) and Part II of the European Patent Convention). Software and mathematical methods are specifically exempt from patent protection; however, only to the extent that a patent application relates solely to software or mathematical method as such. One can apply for patent protection for "mixed inventions", for instance, for a new product of a technical nature that incorporates a software program. Similarly, methods for diagnosis are not patentable under European law, but medical devices used to carry out the diagnostic method are.

The European Patent Office (EPO) classifies AI- and ML-related applications as mathematical methods in its guidance. From 2023, inventions in the EU can be protected by a European patent with unitary effect (the "unitary patent"), providing uniform patent protection across participating EU Member States and being subject to the jurisdiction of the Unified Patent Court.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protects literary or artistic works in a broad sense (Title 5 of Book XI of the CEL). A work is eligible for copyright protection provided that it represents the author's own intellectual creation (the "originality" requirement). The author of a work that fulfils these conditions is granted copyright protection without any formality, up until 70 years after their death. Copyright includes both transferable property rights and inalienable moral rights. However, the originality requirement seems to be problematic in relation to digital health technologies. While the expression of software (i.e. the code and preparatory design work) and the structure of a database (i.e. the selection and arrangement of the data) can be protected by copyright, the ideas and principles underlying the technology (such as algorithms and functionalities) are not copyrightable, nor is the content of a database. The latter could be protected by the *sui generis* database right, provided that the acquisition, verification and presentation thereof constitute a substantial investment by the author (art. XI.306 of the CEL). Interestingly, there seems to be a legislative trend to limit the scope of copyright protection in order to facilitate the development of digital technologies and the sharing of data. The EU Directive 2019/790 on Copyright and Related Rights in the Digital Single Market (the Copyright Directive), which has been transposed into Belgian law by the Act of 19 June 2022, has introduced exceptions to copyright for text and data mining (i.e. the automated analysis of large bodies of data in order to generate knowledge on patterns, trends and correlations). This will allow developers of AI systems to extract data from a database without having to obtain the prior authorisation of its owner. Art. 43 of the Data Act provides that the *sui generis* database right does not apply to databases containing data obtained from or generated by a connected (IoT) product or related service.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Information is considered a trade secret if the information is secret, not publicly known or easily accessible, if the information has commercial value due to its confidentiality, and if the information was made subject to reasonable measures

to protect its confidentiality (Title 8/1 of Book XI of the CEL). As such, trade secrets can protect raw or processed data and databases, methods, algorithms, codes, processes, parameters, etc. Trade secrets are not protected by an IP right and do not require registration, but the wrongful acquisition of such information is prohibited and may be enforced in court by means of a claim for injunctive relief and damages. It should be noted that independent discovery or creation of the same information remains lawful.

Digital health technology companies may rely on trade secrets for the protection of the data used to train their AI models, provided they can prove the commercial value thereof. This will be easier when it comes to a combined dataset rather than with respect to any part of the data in isolation. However, as part of the data sharing obligations introduced by the Data Act, the trade secret holder may be required to disclose its trade secrets to the user of a connected device or even a third party (subject to the user of a connected device or third party taking adequate technical and organisational measures to preserve the confidentiality of the trade secret).

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Higher education is a competition of the Communities in Belgium. For the Flemish Community, the Codex Higher Education stipulates that any property rights to inventions made by salaried staff as part of their research duties shall belong exclusively to the university or the university college. The Codex further lays down rules for the participation of universities or university colleges in spin-off companies and for scientific services performed by universities and university colleges. Most academic technology or knowledge transfers are handled by the tech transfer offices of the universities or university colleges and take the form of licence or other types of collaboration agreements or participation in spin offs.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

As said above, software may be protected by a patent if incorporated in technology, such as a medical device. In addition, the expression of software enjoys copyright protection if it is original in the sense that it is the author's own intellectual creation (Title 6 of Book XI of the CEL). In this respect, copyright can also protect the appearance (i.e. graphics and multimedia elements) of a digital health application.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

The EPO has confirmed on multiple occasions that AI (devices) cannot be named as inventors on patent applications, as the European Patent Convention stipulates that the inventor must be a person with legal capacity.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The core rules and laws applicable to government-funded inventions in Belgium are noted down in the CEL, Book XI, Title 1, Chapter 2. Irrespective of any governmental funding, the inventor is considered the person who developed the invention.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

In the *Eva-Maria Painer* case, the CJEU ruled that copyright applies only to works that reflect the author's personality and result from their free and creative choices. Based on this reasoning, AI-generated outputs may not qualify for copyright protection, meaning individuals using AI to create content would not hold any copyright over those works.

On 27 February 2025, the CJEU issued a judgment on a request for a preliminary ruling from the Administrative Court of Vienna to the CJEU, stating that a data subject's right to receive meaningful information about the logic involved in automated decision-making (art. 15(1)(h) of the GDPR) should be balanced against the (IP) interests of the controller, such as the protection of its trade secrets. It is up to the supervisory authority or court involved to, based on the actual information and the facts of the case, determine the extent of the right of access that must be granted to the data subject.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

The allocation of IP rights must be carefully assessed before concluding collaborative agreements. Both the ownership of results and the IP that arises from such results as potential licence rights and the limits to such licence rights must be considered before R&D commences.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

In any collaboration in the healthcare industry, one must be wary of anti-competitive agreements. The (health) tech and pharmaceutical landscape is often characterised by major players, so caution needs to be exerted when contracting. In addition, the healthcare industry is one of the highest regulated sectors. The healthcare company must take the lead in assuring that the non-healthcare company understands and abides by healthcare regulations whenever it applies to the latter.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

As discussed above (see question 5.5), federated learning can help to overcome data protection-related obstacles to collaborative big data projects, amongst others, by reducing the amount of personal data processed by third parties (data minimisation) and by avoiding the need to transfer data to

other jurisdictions (with potentially inadequate data protection and privacy laws). However, it does not solve the typical uncertainties relating to data processing roles and responsibilities. Indeed, a party can be considered a data controller in relation to certain data without actually receiving such data in raw form. (Consortium) partners need to take into account that having their respective roles and responsibilities clearly defined is imperative to avoid ambiguity for data subjects. This can cause considerable delays in the negotiation of partnership agreements. Another important consideration is whether the partners have the right to process existing research data for secondary use in a federated learning project, especially when the data subject's consent is used as the legal basis for the original collection and processing. The GDPR and the European Commission's guidelines offer some flexibility when it comes to obtaining consent for a broader area of research rather than for one research project (see Recital 33 of the GDPR).

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

As already discussed above, several challenges need to be overcome when using generative AI in the field of healthcare, including regarding the allocation of liability, clinical responsibility and human oversight, data access and reuse (including training data), transparency and explainability commitments, and post-market monitoring. Agreements should anticipate evolving obligations under the GDPR, MDR and AIA.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Under the AIA, each Member State should designate at least one notifying authority and at least one market surveillance authority as national competent authorities for the purpose of supervising the application and implementation of the Act. These authorities are still to be appointed in Belgium (although the official deadline for designation has passed).

The notifying authority will be responsible for setting up and carrying out the necessary procedures for the assessment, designation, notification and monitoring of conformity assessment bodies (i.e. third-party bodies which, once notified, are responsible for verifying conformity of high-risk AI systems before their placement on the market). For Belgium, it is anticipated that the existing notifying authorities under current EU legislation will be designated as the notifying authorities for the AIA within their respective areas of competence. In the case of digital health products, this role is expected to be assigned to the FAMHP.

It is further expected that the Belgian DPA will be appointed as the market surveillance authority responsible for enforcing compliance with the AIA. A key argument in favour of having data protection authorities at the forefront of AI regulation is that this would allow for a centralised (cross-product) approach to market surveillance. The DPA's decisions would apply to all types of products incorporating AI/ML systems, which reduces the risk of having conflicting interpretations of the AIA by different authorities regulating different types of products. The Belgian DPA has already offered guidance on how the GDPR interacts with the AIA.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

As stated above (see question 2.2), the AIA has recently entered into force. The AIA's obligations are implemented in phases. Both the provisions related to prohibited AI systems and AI literacy specific obligations for general-purpose AI models have become applicable in the meantime. Most other obligations under the AIA, including those for high-risk AI systems and systems with specific transparency requirements, will take effect on 2 August 2026. The remaining provisions will become applicable on 2 August 2027. Consequently, several procedures are still ongoing regarding the designation of the competent authorities and the further implementation of the regulation.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

According to the case law of the Court of Justice, copyright protection is merely possible if the author has been able to express his creative abilities by creating free and creative choices that give a personal touch to the work. A work, made or improved by AI or ML, cannot be protected by copyright if it is created without creative human involvement and does not meet the requirement of originality. With regard to patents, according to the EPO and art. XI. 4 of the CEL, algorithms are *per se* of an abstract mathematical nature and normally exempt from patent protection. If not exempt from patentability, for example, when incorporated in technology, other problems occur. When AI is merely used as a tool to aid a researcher in the development of an invention, the researcher shall still be the inventor. It becomes more complicated if human involvement is limited or non-existent. Problems may arise with the condition of inventiveness if the human intervention in the creation of an invention did not require any originality, creativity or intellectual contribution from the researcher. Under current patent law, an inventor can only be a person, and AI cannot be seen as the inventor. The question arises in such cases whether it is more adequate to allocate the patent to the developers of the AI technology or to the owners of the AI technology, rather than to the person who "notices" the invention developed by the AI (the researcher).

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

The quality of the data used in ML is essential for the quality of the results it presents. Therefore, companies developing AI technology are interested in (exclusive) licences on quality datasets with the least restrictions possible. Data ownership and control, scope of the permitted use (e.g. training, validation, inference), and whether the licence permits reuse, sublicensing or model retraining are all important negotiation points. The impact of evolving regulation, such as the GDPR's principle of data minimisation and purpose limitation, and the European Health Data Space and Data also impact how

healthcare data may be accessed, shared and commercially exploited within the EU market.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Generative AI differs from standard AI as it is not limited to rule-based predictive tasks but instead uses ML to analyse data, recognise patterns and generate new content that mimics human creativity. Both generative and standard AI fall within the AIA framework. The AIA recitals classify generative AI models as "general-purpose AI models", given their ability to generate diverse content such as text, audio, images and video for various tasks. These models are subject to a distinct regulatory framework under the AIA. While most AIA provisions apply to both generative and standard AI systems, additional transparency obligations apply to generative AI providers and deployers, including the requirement to clearly indicate when content has been artificially generated or manipulated.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Most of the risks associated with AI in general are enhanced when dealing with generative AI technologies. First of all, generative AI can contribute tremendously to the spreading of misinformation and the distribution of harmful content online. The additional transparency obligations imposed by the AIA on generative AI systems should (somewhat) alleviate concerns in that respect (see question 8.5). Further, generative AI poses additional challenges with respect to copyright infringements. The development and training of generative AI models require access to vast amounts of text, images, videos and other data. Text and data mining techniques may be used extensively in this context for the retrieval and analysis of such content, which may be protected by copyright and related rights. When generative AI tools are trained on copyrighted material, the copies of the input data created by these tools may be considered "reproductions" of the original content. If these copies are made without the prior authorisation of the rights holder, such use could constitute copyright infringement. The AIA addresses the interaction between AI technologies and copyright protection. Providers of general-purpose AI models must implement a policy to comply with EU laws on copyright and related rights, in particular to identify and respect the rights of copyright holders. They must also provide a detailed summary of the content used for training the general-purpose AI model so that rights holders can enforce their rights. Finally, ensuring compliance with GDPR and determining liability for damage caused by the output system are also complicated by the specific nature of generative AI.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Data protection authorities are stressing the importance of compliance with the GDPR in the development of AI systems. The Belgian DPA has recently released guidelines on AI and the GDPR, highlighting the critical need to follow data protection principles to ensure AI systems operate ethically. The guidelines discuss the main data protection principles that are relevant to AI systems, such as lawfulness, purpose limitation and data minimisation, storage limitation, etc. However, the guidelines do not address the deletion of (unlawfully processed) personal data embedded within AI models. Even if personal data was processed lawfully in the development of the AI model, the GDPR requires the erasure of personal data without undue delay upon request of the data subject. For AI model developers, this may technically not be feasible.

On 18 December 2024, the EDPB adopted an opinion on the use of personal data for the development and deployment of AI models. In this opinion, the EDPB states that when an AI model was developed with unlawfully processed personal data, this could render the subsequent operation of the AI model unlawful, unless the AI model has been duly anonymised (meaning that it is very unlikely to directly or indirectly identify individuals whose data was used to create the model, or to extract such personal data from the model through queries). However, the extent to which the lack of legal basis for the initial processing activity impacts the lawfulness of the subsequent processing should be assessed on a case-by-case basis, depending on the context of the case. If the AI model is developed and deployed by different controllers, the controller deploying the AI model should in any case conduct an appropriate assessment to demonstrate compliance with GDPR as part of its accountability obligations.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Besides the general regimes of contractual and extra-contractual liability, the regimes of product liability and medical liability must be considered. A two-track system exists for medical liability in Belgium. On the one hand, the patient can invoke the medical liability of its physician or the hospital. On the other hand, a fund has been established to compensate severe damage caused by "medical accidents without liability". Furthermore, product liability is based on strict liability. A party claiming damages must only demonstrate a defect in the product, the damage and the causal relationship between the defect and the damage. The fault of the manufacturer need not be established. A product is defective if it does not provide the safety one is entitled to expect from that product. Any person in the production chain, the EU importer and the supplier may be held liable. As such, a physician or hospital may take the role of manufacturer or supplier of a defective product. The EU has recently made efforts to modernise the product liability regime to be more resilient for the current digital age, by means of the (slightly) updated liability framework of the Digital Services Act and the new Product Liability Directive (which entered into force on 8 December 2024 and should be transposed into national law by 9 December 2026). These instruments aim for a more equal sharing of the burden of proof for complex digital solutions between the claimant and manufacturer, ensuring better protection for victims. A Proposal for a Directive on adapting non-contractual civil liability rules to AI (AI Liability Directive) was, however, withdrawn, due to a lack of consensus.

9.2 What cross-border considerations are there?

Within the EU, product liability is more or less harmonised and a patient suffering damages from a defective product such as a medical device will be granted similar protection in all Member States. The EU importer can also be held liable in the same manner as a foreign manufacturer can be. This ensures there is always an EU-based liable party from whom a victim can claim compensation, even when the manufacturer itself is not based in the EU. However, as for medical liability, the Law on Medical Accidents of 31 March 2010, providing compensation for medical accidents without liability, only applies to healthcare provided on Belgian territory (regardless of the patient's nationality). Several other countries do not have a regime for faultless medical liability; accordingly, a Belgian patient may not enjoy equal protection when receiving healthcare services abroad. Lastly, the EU Directive on the Application of Patients' Rights in Cross-Border Healthcare is taking its first steps in ensuring proper professional liability insurance in cross-border healthcare within the EU.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

In addition to the aforementioned considerations relating to cybersecurity and data protection, companies developing and marketing AI-driven digital health solutions should be aware of the stringent regulatory and compliance framework under which the healthcare sector operates, which entails corresponding rigorous duties and liabilities. It is therefore important to seek (local) expert advice and guidance on the requirements associated with entering the healthcare market in general.

To minimise the risk of medical errors caused by the use of AI-driven devices, it should be kept in mind that AI may work well in efficiently processing large amounts of data to suggest and verify conclusions (perhaps correcting human mistakes), but should not be deployed without human intervention and oversight. From a data protection perspective, data subjects (e.g. patients) have the right not to be subject to a decision based solely on automated processing (art. 22 of the GDPR). It is therefore important that every diagnosis or treatment decision made by or on the basis of AI-driven technology is carefully reviewed by a natural person (i.e. the HCP). This can be challenging as it may not always be clear how the software has reached a certain conclusion. The new EU Product Liability Directive provides for strict (product) liability. The AI Liability Directive proposal introduced a fault-based liability regime for AI technologies, with a (rebuttable) presumption of a causal link between the provider's or user's fault and the output produced by the AI system, as well as disclosure requirements to aid victims in providing the evidence to support their claim; however, this proposal has now been withdrawn. Attention should also be given to consistency with the roles of data controller and data processor in agreements (between providers, manufacturers, importers, distributors and users).

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

GDPR enforcement consists of a combination of public enforcement (by supervisory authorities imposing administrative sanctions as well as through the criminal justice system) and private enforcement (civil liability).

There are several legal grounds on which a data subject can file a complaint with the Belgian DPA to initiate public enforcement. The dispute chamber can impose various sanctions, including fines, but it does not have the authority to award compensation to the data subject. Consequently, the proceeds from financial sanctions will not benefit the complainant.

To receive compensation for the damage suffered due to misuse of healthcare data in the training of AI models, the injured party can rely on art. 82 of the GDPR. Similar to the general regimes of contractual and extra-contractual liability in Belgian law, which are also available to the injured party in this instance, the claimant must provide proof of a violation of the GDPR, material or immaterial damage and a causal link between the violation and the damage. It should be noted, however, that a claim for compensation based on art. 82 of the GDPR can only be brought against data controllers and data processors.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Caution should be exercised when making use of Cloud-based services, as this is an area particularly sensitive to data breaches, cybersecurity issues and other data protection hazards. If a (digital) health company/healthcare organisation makes use of the services of a Cloud service provider, such service provider will generally be considered the processor, which processes personal data on behalf of the company or organisation (controller) and which may be working with multiple sub-processors. Consequently, a sound data-processing agreement must be concluded, including extensive audit rights for the controller and a liability clause that sufficiently protects the controller in the event of claims by data subjects or a data protection authority as a result of infringements by the processor. Furthermore, the healthcare industry is notably vulnerable to cyber-attacks, as Belgian hospitals have experienced first-hand over the years. Therefore, it is of utmost importance to ensure that Cloud service providers offering services to the (digital) health industry have taken adequate organisational and technical measures to safeguard any personal data and confidential documents stored. In this regard, the Directive (EU) 2022/2555 (NIS 2) extends the scope of entities to which the NIS requirements apply to also cover hospitals and other HCPs. Finally, Cloud service providers are also included as intermediary service providers in the Digital Services Act. Cloud service providers are under an obligation to implement appropriate "notice and take action" mechanisms and need to be transparent if content is taken down.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Entering the healthcare industry means entering a highly regulated context, in which innovating might be challenging. Market strategies shall have to be adapted to the specific regulatory framework governing health products and services. For instance, the promotion of medical devices has been severely restricted. Further, the company shall have to be prepared to

invest heavily in compliance, e.g. data protection laws, medical device regulation, product safety, etc. Lastly, the company will have to bear in mind that it will have to represent the interests, not only of the end-user, but also of doctors, hospitals, health insurance providers and the NIHDI.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Belgium has seen important investment activity into health tech and digital health, although assessing the growth potential and the relative strength of a digital healthcare venture amongst its competitors is not without its challenges. For instance, it is important to evaluate the IP protection the venture has obtained (or can likely obtain in the near future) for its product, whether the product shall classify as a medical device or not and whether reimbursement has been obtained or is foreseeable to be obtained in the near future. The safety of the product and potential risks for liability claims need to be determined and one needs to ensure that there is a market for the health product, consisting not only of end-users, but also physicians and hospitals willing to prescribe or use the product in their provision of healthcare services.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The lack of reimbursement for a great number of digital health solutions is one of the major deficiencies in the Belgian (regulatory) landscape. In addition, uncertainty regarding the interpretation of existing legal frameworks on new health technology hinders swift adoption. Although the primary responsibility for healthcare remains with the Member States, a more harmonised approach at EU level may benefit the cross-border offering of digital healthcare services and products, a situation that might improve once the EU's Digital Strategy is fully implemented. Finally, it needs to be noted that, although the government has already initiated certain financial incentives for health practitioners to implement electronic health records, such incentives may need to be extended to other digital health applications.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The NIHDI is responsible for the accreditation of physicians and pharmacists, while organisations such as the Joint Commission International accredits hospitals in Belgium. As the NIHDI is also the institution responsible for reimbursement decisions (see question 10.6), naturally, its endorsement of digital health solutions is essential to steer clinical adoption. In addition to the NIHDI, the guidance and advice of the deontological body of physicians, the NCOP, are crucial in the long road ahead to better patient care through digital health.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

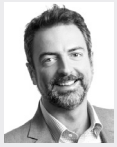
Digital health solutions that are medical devices can be reimbursed by the NIHDI if they fulfil the reimbursement criteria (see question 3.1 above). However, other digital health solutions and telehealth services are currently not part of the nomenclature of the NIHDI and therefore are not currently reimbursed.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

There are several gaps in the regulatory framework for the assessment of digital health solutions, particularly those incorporating AI and ML. One key challenge involves the evaluation of the safety and efficacy characteristics of SaMD and AI/ML-powered solutions. For instance, under the MDR, a medical device needs to undergo a new conformity assessment if it undergoes modifications before being placed on the market. While this approach is well-suited for traditional, static medical devices, it poses challenges for dynamic technologies that frequently require updates, security patches and algorithm refinements on the basis of new data. The AIA does not fully resolve this issue of continuous learning AI models, with algorithms evolving based on real-world data.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The current geopolitical climate, macroeconomic uncertainty and evolving global supply chains will undoubtedly continue to have an impact on the digital health landscape. Payers will have to find new and inventive ways of funding health solutions to accommodate constrained healthcare budgets and fragmented reimbursement schemes, for example by exploring value-based payment schemes. On the other hand, consumers and patients may find difficulty in affording innovative, health-targeted consumer devices or medical devices due to the relatively higher cost of living. Shortages in, for example, the chip industry have important consequences for the costs and availability of medical devices. Finally, (venture capital) investment in healthcare companies leveraging (generative) AI has exponentially increased and will likely continue to do so.



Olivier Van Obberghen works exclusively for clients in the life sciences and innovative technologies sectors. He co-heads the Life Sciences department of Quinz together with Pieter Wyckmans.

Quinz
Medialaan 28B, B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: olivier.vanobberghen@quinz.be
LinkedIn: www.linkedin.com/in/olivier-van-obberghen-5906a4



Pieter Wyckmans provides expert advice to companies and organisations active in the (bio-) pharmaceutical, biotech and smart devices sectors. Pieter co-heads the Life Sciences department of Quinz together with Olivier Van Obberghen.

Quinz
Medialaan 28B, B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: pieter.wyckmans@quinz.be
LinkedIn: www.linkedin.com/in/pieter-wyckmans-39499b8



Amber Cockx is a Life Sciences lawyer with a main focus on R&D, technology and data protection matters. Amber provides transactional and regulatory support to clients active in the pharmaceutical and medical devices sector. Her main areas of expertise comprise transactional and regulatory assistance throughout the entire product life cycle, from negotiating and drafting contracts, coordination of international R&D collaborations, through clinical phases, early access, marketing authorisations, advertising and promotion, pricing and reimbursement, and interactions with healthcare professionals and healthcare organisations.

Quinz
Medialaan 28B, B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: amber.cockx@quinz.be
LinkedIn: www.linkedin.com/in/amber-cockx-520914170



Chaline Sempels is a lawyer focusing on the life sciences industry, including digital health. She supports clients ranging from innovative start-up ventures to multinational corporations in (strategic) transactions and European regulatory affairs, throughout the entire product life cycle. In this context, her main areas of expertise include negotiating and drafting (supply chain and distribution) agreements, co-ordination of international R&D collaborations (the Horizon 2020 funding programme, the Innovative Medicines Initiative (IMI2) programme), medical devices, software applications and emerging technologies, and interactions with healthcare professionals and organisations.

Quinz
Medialaan 28B, B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: chaline.sempels@quinz.be
LinkedIn: www.linkedin.com/in/chaline-sempels-387605179

Quinz is a Brussels-based law firm with a strong focus on Life Sciences. Quinz assists the global, regional (EMEA, LATAM, APAC) and local (Belgium, Luxembourg and the Netherlands) legal departments of pharmaceutical companies on a broad array of (strategic, operational, licensing and M&A) transactions throughout the life cycle of a life sciences product. Quinz has also developed a sound expertise in regional and local regulatory work (including pricing and reimbursement, clinical trials, data transparency, marketing authorisation procedures, cGMP) and compliance matters (including transfers of value, promotion of life sciences products, antitrust compliance questions, patient-directed programmes, GDPR). Its Life Sciences department is headed by Pieter Wyckmans and Olivier Van Obberghen.

www.quinz.be

Chile


Mónica Pérez


José Ignacio Mercado


Camila Suárez


Mariana Guzmán

Carey

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

No specific laws define "digital health". However, Technical Guideline 237 on Remote Healthcare Services and Telemedicine adopt the WHO definition, as "the field of knowledge related to development and use of digital technologies to improve the population's health", including "smart devices, the Internet of Things, artificial intelligence, Big Data and robotics".

In practice, the concept of digital health has been associated with "telemedicine", and it has been observed that specific regulations on telemedicine tend to identify both concepts.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Digital health activities in both the public and private sectors are mainly focused on the provision of telemedicine services. The Ministry of Health ("MoH") program "*Hospital Digital*" provided a total of 1,044,976 services during 2024, 17% more than 2023.[1]

In parallel, the MoH is advancing electronic prescribing – enabling prescriptions to be issued, stored and dispensed digitally – and healthcare providers are offering online booking, patient monitoring, online care journeys, and implementing electronic clinical records and their interoperability.

Other subsectors include healthcare software, AI-supported diagnosis, test and imaging processing, cloud technologies, and medical training.

1.3 What is the digital health market size for your jurisdiction?

There are no publicly available sources in this regard.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

There are no publicly available sources in this regard.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

There are no publicly available sources in this regard.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The **MoH** is responsible for setting forth national health policy and coordinating/implementing healthcare actions, including standards on digital health. At a regional level, the MoH operates through **Regional Ministerial Secretariats** ("SEREMIs"), which act as the local sanitary authority and conduct on-site oversight.

The **Superintendence of Health** supervises healthcare providers' compliance with applicable telemedicine, clinical records, and other healthcare-specific laws and regulations.

The **Public Health Institute** ("ISP") is responsible for the sanitary control of medical devices ("MD") and pharmaceuticals, including e-commerce.

The **National Cybersecurity Agency** ("ANCI") supervises/enforces cybersecurity duties for entities providing essential services, which include institutional healthcare providers as well as digital infrastructure, digital services, and third-party managed IT services, created by Cybersecurity Law 21,663 ("CFL").

The **Data Protection Agency** ("Agency"), created by the New Data Protection Law (Law 21,719 or "NDPL") will be the enforcement authority for personal data, including health data, as a relevant development for digital health, given the large-scale processing of health data and the NDPL's strengthened sanctions framework and risk-based compliance tools.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

- **Software as a Medical Device ("SaMD")**: Digital health products may be classified as MD when they meet the criteria set forth in the Sanitary Code, Decree 825/1998 and the ISP's medical-device classification guidelines. This includes SaMD, which are defined as follows: "*[An] intellectual creation that includes programs, procedures, rules and any documentation associated with the operation of a data processing system for medical purposes, so that it performs clinical functions or exerts an effect or action direct on diagnosis, therapy or preventive process. It extends*

to both those who are part of a computerized medical team, and to those supplied independently as a product in itself." Marketing authorisation is only mandatory for regulated MD, which currently represent a limited set of devices and do not include any type of software.

- **Telemedicine**: Decree 6/2022 regulates actions related to remote medical care. Then, Law 21,541 amended Law 20,584 on Patients' Rights and Duties ("RDPL") to expressly recognise remote healthcare attention at a legal level and authorise healthcare providers to perform telemedicine. The latter is complemented by ancillary plans and regulations, the main one being Technical Guideline No. 237/2024.
- **E-commerce of pharmaceuticals**: This is only permitted for pharmacies/pharmaceutical stores, requiring additional ISP authorisation, regulated by Decree 466/1984.
- **Digital clinical records**: Clinical records are regulated by RDPL and Decree 41/2012, which sets core requirements for their management, as mandatory instrument (physical or digital). Law 21,668 now requires interoperability of clinical records across providers, with MoH implementation and oversight supported by SEREMIs at a regional level.
- **E-prescription**: The Sanitary Code and Decree 466/1984 recognise that medical prescriptions can be issued as a graphic or electronic document, and expressly allow the use of digital tools or systems to optimise electronic prescription processes. Therefore, prescriptions may be issued through any e-prescribing system (as an alternative to advanced e-signature) with validation by the prescriber.

Regarding data protection and AI, please refer to sections 4 and 8 below.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Currently, a key area of enforcement is pharmaceutical e-commerce, focusing on illegal sales and black-market activities.

Regarding emerging enforcement, Law 21,668 mandates interoperability of clinical records across healthcare providers, with data-security safeguards; however, its technical/operational rules – and thus its practical enforceability – await MoH regulation. Additionally, with the CFL and the upcoming NDPL and Agency, stricter enforcement is expected regarding cybersecurity and data-protection aspects of digital health.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

As mentioned in question 2.2, SaMD is currently considered a non-regulated MD and, therefore, its commercialisation does not require marketing authorisation. A Customs Destination Certificate is required only for physical importations (*e.g.*, hardware).

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Currently, there are no specific authorities nor sanitary regulations applicable to AI/ML-powered digital health devices, notwithstanding specific regulations for SaMD (as noted above).

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

As no specific authorities nor sanitary regulations apply to AI/ML-powered digital health services, there are no current roadmaps or plans to evolve the applicable regulatory framework in this regard.

Bill of law No. 17.375-11, currently under discussion in the Senate, aims to create a National Digital Health Service, as well as to amend the general regulation applicable to MD. Although it modifies the approval process for MD, including SaMD, it does not include rules specific to this kind of product.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Further to the above, clinical validation data is not currently considered by regulators for AI/ML-based digital health solutions.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

No differences apply.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Please refer to questions 2.1 and 2.2.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Main issues relate to: (i) compliance with RDPL and telemedicine regulations (Decree 6/2022); (ii) clinical record rules (content, integrity, access controls, interoperability); (iii) compliance with Law 19,628 ("DPL") rules – plus NDPL after commencement; and (iv) CFL, if applicable.
- **Robotics**
  There are no specific regulations. However, if the necessary conditions are met, they could eventually qualify as an unregulated MD and shall comply with relevant regulations (please refer to questions 2.1 and 2.2). Regarding data protection and cybersecurity, please refer to "Telemedicine".
- **Wearables**
  No specific regulations apply. Generally, consumer protection regulations will apply. Depending on their intended use, they may qualify as MD (*e.g.*, some wearable glucose sensors). Regarding data protection and cybersecurity, please refer to "Telemedicine".
- **Virtual Assistants (e.g. Alexa)**
  Please refer to "Robotics". Additionally, liability concerns may arise regarding its impact on patient-care decisions

and the sanitary responsibility of healthcare professionals using this technology.

- **Mobile Apps**
  Please refer to "Robotics".
- **Software as a Medical Device**
  Apart from regulatory requirements (see questions 2.1 and 2.2), data privacy regulations must be complied with if there are data processing activities involved.
- **Clinical Decision Support Software**
  Please refer to "Virtual Assistants".
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Please refer to "Virtual Assistants".
- **IoT (Internet of Things) and Connected Devices**
  Core issues are related to: security, vulnerability management and incident handling; and, where applicable, reporting duties for significant incidents regulated under CFL. Regarding data protection, please refer to "Telemedicine".
- **3D Printing/Bioprinting**
  Please refer to "Robotics".
- **Digital Therapeutics**
  Please refer to "Robotics".
- **Digital Diagnostics**
  Please refer to "Virtual Assistants".
- **Electronic Medical Record Management Solutions**
  Please refer to "Telemedicine".
- **Big Data Analytics**
  There are no specific regulations. Regarding data protection and cybersecurity, please refer to "Telemedicine".
- **Blockchain-based Healthcare Data Sharing Solutions**
  There are no specific regulations. Regarding data protection and cybersecurity, please refer to "Telemedicine".
- **Natural Language Processing**
  Please refer to "Virtual Assistants".

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

There are no general rules regarding "digital health platforms". Where such platforms process personal data and/or CFL is applicable considering the services, the respective rules will apply.

However, Decree 6/2022 sets rules for providers of digital platform services serving healthcare institutions, in the context of telemedicine, requiring them to guarantee patients' privacy and comply with MoH technical standards, in line with DPL and RDPL rules.

Additionally, healthcare providers must ensure that used platforms enable reliable patient and healthcare professional identification, interoperability/technology neutrality, secure transmission of clinical data consistent with data protection and clinical-record confidentiality duties, and full traceability/audit logs; they must also implement privacy risk management, incident registers, secure backups and continuity measures, and role-based access controls, and notify any security incident within the legal deadline. Data processing/analytics may be used only for a defined health purpose and in compliance with rules on personal data.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

- Personal data processing is governed by DPL, which requires (a) prior, written, express consent, or (b) legal authorisation, as a legal basis. DPL was recently amended by the NDPL (effective December 1, 2026), which brings Chile closer to the EU GDPR by strengthening data-subject rights, expanding sanctions, and creating an Agency.
- CFL applies to entities classified as operators of vital importance or essential-service providers – categories that may include health-technology providers depending on their services – requiring enhanced safeguards and breach notification for incidents, among others.
- RDPL obligates healthcare providers to respect and protect patient privacy and dignity and, along with Decree No. 41/2012, contain the framework on clinical records. It also: imposes duties on confidentiality, access, retention, and custody of records; requires *privacy by design*, transparency on recordings, data uses, retention, and patient acceptance; governs access, portability, and custody; and allows use of technologies only with guarantees of care quality, autonomy, and safeguard of patients' personal data.
- Law 20,120 regulates human scientific research and protects personal and genetic data during research. It requires prior, free, informed consent with ethics committee oversight, and mandates confidentiality.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

No differences apply.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The rules mentioned above apply equally to public and private entities.

However, as personal health data qualifies as sensitive data under DPL and NDPL, its processing requires previous express consent from the data subject, with exceptions. Additionally, under NDPL – except for the exceptions explained below – health data and the human biological profile may only be processed with the data subject's explicit consent for the purposes provided for by special laws in the healthcare field.

Also, in clinical/genomic contexts, genetic data are subject to confidentiality and technical safeguards (including encryption of identifiable genomic data for storage/transmission) and may not be used for discriminatory purposes.

4.4 How do the regulations define the scope of personal health data use?

Under DPL, sensitive data may only be processed with prior

written consent of data subjects. Under NDPL, sensitive data relating to health and the human biological profile has special regulation as, further from consent, data may only be processed for purposes provided for by special laws on health matters. There are exceptions for processing without consent (*e.g.*, indispensable to safeguard life or health, the data subject is physically or legally prevented from granting consent, or sanitary alert). NDPL and the regulation stated above also impose purpose limitation, data minimisation, strong security and incident-notification duties, and, specifically for clinical records/telemedicine, provider custody, restricted access, and certain retention periods for health data.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

As a data controller, key contractual terms include:

- **Roles, purposes, and legal basis**: clearly define controller/processor roles, specify purposes, prohibit incompatible secondary uses, and sign a Data Processing Agreement ("DPA") when needed.
- **Sensitive-data safeguards**: treat health data as sensitive, require minimisation, role-based access, and privacy-by-default measures.
- **Security and incidents**: mandate encryption/pseudonymisation, risk-based technical and organisational measures, and prompt incident notice with full cooperation.
- **Data subjects' rights**: processors must assist with access, rectification, deletion, objection, portability, and consent withdrawal.
- **International transfer**: use approved clauses, especially for non-adequate jurisdictions for NDPL. Ensure adequate protection or equivalent guarantees, as data transfers need informed consent unless legally authorised. Processing agreements must specify the recipient's instructions.
- **Retention**: purpose-based retention; healthcare providers must keep clinical records for at least 15 years. Setting forth secure deletion/return at contract end with certification is advisable.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Although no data protection authority exists yet, DPL and NDPL already provide for criteria upon data inaccuracy, bias and/or discrimination:

- NDPL includes the quality principle, requiring data to be accurate, complete, current and relevant regarding their origin and processing purposes.
- NDPL and DPL grant data subjects rights to access and rectify their data.
- Under NDPL, data subjects may object to solely automated decisions (including profiling) with legal or similarly significant effects. Even when permitted, data controllers owe transparency, explanation, and human review.

Law 20,609 prohibits and sanctions acts of discrimination based on race, nationality, socioeconomic status, language, political opinion, sexual orientation, gender identity, religion, etc.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Please refer to question 4.1.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under NDPL, international data transfers require that the destination offers adequate protection[2] or equivalent guarantees exist, except when authorised by law. Also, NDPL establishes that data sharing and their purpose must be informed and requires the subject's consent unless legally authorised. If a data controller commissions the processing activities to a third party, a DPA specifying the transmitter's instructions, purposes of the agreement, type of data processed, etc., must be executed.

In addition to the rules mentioned in question 4.1: (i) Law 21,668 establishes the national interoperability of clinical records across healthcare providers, with safeguards for personal data protection and information security (with pending regulations); (ii) the public-sector transparency regime in Law 20,285 regulates access to public information and the conditions under which public entities may disclose data; and (iii) the State Digital Transformation Law 21,180 regulates the digital processing, interoperability and exchange of data between public entities.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Please refer to question 4.2.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

In addition to the general duties with respect to the processing and sharing of data stated above, regarding the sharing of data, public entities must specifically reconcile an obligation of transparency, as contained in Law 20,285, with privacy limits and a special confidentiality duty and to establish security measures regarding clinical records pursuant to DS 41/2012, in the case of healthcare providers.

Health and biological data are qualified as sensitive data as stated in question 4.3. Additionally, for international transfers, NDPL will require adequacy decisions or contractual/corporate safeguards in case of non-adequate jurisdictions.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please refer to question 5.1.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Please refer to question 5.1.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under Law 19,039 ("IP Law"), digital health innovations are patentable if new, inventive, and industrially applicable, with novelty determined against global prior art and earlier Chilean filings once published. Purely abstract or clinical subject matters are excluded, while preserving eligibility for the products enabling the same (*e.g.*, devices or software-based apparatus), steering drafting toward technical systems and *in vitro* implementations rather than body-applied steps.

Enforcement is limited by international exhaustion, a Bolar/regulatory-use exception, and exemptions for private, non-commercial use and experimentation, all relevant for clinical validation, regulatory processes, and pilot tests. Device-oriented innovations may alternatively use utility models to protect new, industrially applicable form/function configurations with technical advantage, subject to many patent rules *mutatis mutandis*.

Public-interest tools – especially compulsory licences – can affect market access and negotiation leverage for essential digital therapeutics and platforms.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Under Law 17,336 ("Copyright Law"), digital health technologies are protected through recognition of software as a "*programa computacional*" (covering source code, object code, and preparatory materials) and protection for creative databases or compilations, while excluding rights over the underlying data itself. Authors hold moral and economic rights, and service models must respect exclusive rights of reproduction (including temporary copies), public communication (including on-demand making available), transformation, and distribution (with exhaustion applying only to first sale of physical copies).

Ownership defaults are technology-relevant: software created by employees in the course of employment belongs to the employer unless agreed otherwise; commissioned software is presumed assigned to the commissioning party; and terms last for life plus 70 years, or 70 years from first publication when the employer is a legal entity. Copyright may coexist with industrial property protection for aspects of a digital health product.

Platforms hosting or transmitting third-party content may rely on ISP safe harbours if they do not select content, comply promptly with court-ordered blocking/takedown, and process notices appropriately; courts may order reasonable blocking of clearly identified infringing material, and providers have no general monitoring duty. Rights management information ("RMI") is expressly protected, with penalties for removing, altering, or distributing works knowing RMI was removed – this is important for clinical media and audit trails.

Enforcement exposure includes civil remedies (*e.g.*, compensation), criminal sanctions for commercial-scale infringement, and a presumption of subsistence for works published within the last 70 years.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets protect any undisclosed information with commercial value that is kept confidential through reasonable measures, covering algorithms, source code, datasets, product roadmaps, and technical know-how used in digital health solutions. Protection requires the information to be unknown to the public, valuable because it is secret, and subject to reasonable confidentiality safeguards. Civil remedies are available against unlawful acquisition, disclosure, or use, including breaches of confidentiality duties committed with intent to obtain benefit or cause harm.

In related proceedings, courts must consider the parties' legitimate interests in preserving industrial and commercial secrets when allocating evidentiary burdens or ordering disclosure, which is relevant where digital health patent disputes involve confidential algorithms or data pipelines.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Chile has no comprehensive statute governing academic technology transfer; instead, its regulation is dispersed across the IP Law, Copyright Law, Plant Variety Protection Law 19,342, Higher Education Law 21,091, State Universities Law 21,094 and the DPL.

A Technology Transfer Bill (Bulletin 16.686-19), now in its second constitutional stage, aims to establish a unified framework.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Please refer to question 6.2.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

Under current regulations, no. The IP Law defines inventive step by reference to a "person skilled in the art", anchoring inventiveness in a human standard. While applicants/owners can be natural or legal persons, inventorship and ownership rules presume natural person inventors.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Chile's IP and Copyright Laws do not grant the government special rights or automatic licences over publicly funded inventions; ownership follows the general rules for employers and commissioning parties.

Under the Technology Transfer Bill, when a scientific or technological project is partially or fully funded with public resources and generates results eligible for IP or copyright protection, the fund recipient may seek protection and must notify the National Agency of Research and Development ("ANID").

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Although Chile has not faced direct challenges of this kind, there have been related disputes. An example is *Girardi v. Emotiv Inc.*, Case No. 1050652023, concerning neuro-rights and the privacy of brain data collected through a headband with sensors that record electrical activity, capturing gestures, movements, preferences, reaction times, and cognitive activity. The Supreme Court ordered: (i) verification by the ISP and customs authority that the device's commercialisation, use, and data handling comply with applicable regulations; and (ii) deletion of information stored in the company's cloud due to the absence of required authorisations under Law 20,120.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Depending on the type of collaborative improvement, IP rights and ownership should be contractually defined, including copyright and industrial property assets, and intangible assets in general (*e.g.*, know-how, trade dress, etc.).

Improvements involving data processing must define roles, functions and responsibilities according to NDPL and, if applicable, CFL.

If the improvement is related to sanitary/regulatory (*i.e.*, MD) roles, responsibilities and ownership or title to authorisations must also be defined.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Further to the above, from a regulatory/sanitary standpoint, it would be necessary to adequately reflect parties' roles and responsibilities, and both shall advocate compliance with applicable sanitary regulations.

Additionally, depending on the circumstances, NDPL and CFL rules must be complied with, considering higher standards for the processing of sensitive data (such as health data).

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Please refer to question 5.1.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Please refer to question 7.1.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

For public entities, the Ministry of Science leads the implementation of the AI policy and issues non-binding governance guidelines, while the Transparency Council enforces transparency obligations and has issued a General Instruction on Algorithmic Transparency for automated systems for government agencies.

From a data protection standpoint, the Agency will oversee automated decision making and profiling, ensuring rights to object, request human intervention, explanation, and review.

Under the AI Bill, the Agency will handle enforcement, and the ANCI may be involved, if required.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Chile has no AI-specific law. A pending AI Bill (Bulletin No. 16.82119) adopts a risk-based classification imposing restrictions or compliance obligations depending on its level (unacceptable risk, high risk, limited risk, and no evident risk) and prohibits unacceptable-risk systems.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Chile has no specific regulation in this regard. However, according to criteria from the Copyright Protection Office, registrability depends on how AI is used. Works generated autonomously or randomly by AI are not considered copyrightable. Nonetheless, if the output is based on an original work owned by a human author and the AI is used merely as a tool to transform or derive a new version, registration is possible.

In all cases, the Intellectual Property Department of Chile ("DDI") evaluates feasibility case by case, based on the information provided.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Licensing health data for AI/ML must comply with DPL and NDPL. Agreements should define the legal basis, permitted purposes, rights over model improvements/derivatives, security measures, retention/deletion rules, liability, and

international transfer compliance, and ensure data accuracy. Because AI outputs may lack copyright protection without substantial human input, contracts must allocate ownership and reuse rights over outputs and derivatives.

For health data, contracts must also include clinical-record confidentiality and safeguards aligned with telemedicine and interoperability rules. To prevent discriminatory outcomes, deployments should incorporate bias testing, human oversight, appeal mechanisms, and respect the ban on using health data to train AI/ML models for commercial purposes.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Local regulations do not differentiate between standard AI and generative AI. The AI Bill differentiates AI uses and context rather than by "standard" *vs.* "generative" technology.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Key generative AI issues include training data provenance and rights, bias and safety of outputs, transparency, and personal data use (including sensitive data as a category). These are addressed through: (i) NDPL regime for solely automated decisions, especially relevant where generative systems materially affect individuals; and (ii) the pending AI Bill.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

This is not expressly regulated. However, under the AI Bill, high-risk AI systems that use data-driven model training techniques must implement appropriate data governance. Additionally, if a trained model includes personal data without appropriate rights, the Agency will be able to investigate, order cessation of unlawful processing, and apply sanctions under NDPL.

Additionally, general rules on copyright must be considered.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Chilean law does not provide for a specific or unified liability regime for digital health solutions, which may instead fall under different liability frameworks, both general and special, including the following:

- **General and supplementary civil liability regime**: The Civil Code governs contractual and tort (extra-contractual) liability. As a rule, liability is fault-based, although Chilean law provides for certain presumptions of fault (notably, in extra-contractual liability).
- **RDPL**: Liability of healthcare providers for telematic care is subject to the same rules applicable to in-person healthcare services, together with MoH regulations. The statute further clarifies that the use of third-party platforms does not exempt the healthcare provider from liability.
- **Special regime for defective MD**: In cases of SaMD, a special regime contained in the Sanitary Code may apply, dispensing with proof of fault or intent and focusing on the product's dangerousness and the safety risk posed to users. It is debated whether the product liability framework under the Sanitary Code should be classified as strict liability or not.
- **State liability for failure to provide public services**: Such liability, which addresses failure in the provision of public services – including inadequate functioning, omission, or delay – may arise where digital health services are delivered by public institutions.
- **Consumer protection and defective products**: Under the Consumer Protection Act, certain court rulings have recognised a product-liability style regime for defective products. However, the applicability of this regime to digital health solutions is at least debatable, as they expressly exclude healthcare services.
- **Data protection infringements**: Please see question 9.4. In addition to civil liability, healthcare providers may be exposed to administrative or regulatory liability, including sanctions and fines imposed by the Superintendence of Health, and in rarer cases, criminal liability.

9.2 What cross-border considerations are there?

Provision of healthcare services – digitally or otherwise – is governed by Chilean law. Moreover, pursuant to RDPL, telemedicine services are expressly governed by local law and MoH regulations.

Accordingly, the liability regime established in the Sanitary Code for defective MD identifies importers as potentially liable parties, confirming that such liability extends to products originating from abroad.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Risk mitigation in AI/ML for digital health requires robust internal policies, protocols, and continuous monitoring, supported by an oversight or compliance team and clear procedures to manage AI hallucinations. Users must receive concise information on proper AI use, including capabilities, limitations, and error risks, enabling distinction between simple and complex AI-related harms.

For personal data, mitigation measures must ensure confidentiality and compliance with MoH technical standards, alongside privacy-risk management plans, security-incident registers, and operational backups.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Information in medical records and data from medical procedures are sensitive personal data.

While under the DPL the absence of a supervisory authority has led to limited fines and sanctions, and civil claims are rare due to procedural complexity, high litigation costs, and the claimant-side burden of proof, under NDPL, the Agency will be empowered to initiate administrative proceedings and impose fines and other sanctions for personal data infringements, while civil liability mechanisms will be strengthened. These developments are especially relevant given the new medical record interoperability regime introduced by Law 21,668.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based digital health services must address several core compliance challenges associated with processing large volumes of sensitive health information. These include establishing a clear distinction between data controllers and processors, enforcing strict purpose limitations and access controls, and ensuring that contracts contain strong provisions for security, audits, and incident notification procedures.

Data centre locations are also relevant, as cloud providers are required to comply with applicable data transfer rules, as well as any specific health regulations that may apply (*e.g.*, those governing the storage of medical records).

Cybersecurity may also fall within a regulated scope. Healthcare institutions and, in some cases, cloud or managed IT providers acting as "digital service" partners may be subject to oversight and incident reporting obligations monitored by the ANCI.

Lastly, cloud agreements should consider the evolving interoperability and portability standards set by Law 21,668, which aim to minimise vendor lock-in and support secure information exchange across the healthcare ecosystem.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The healthcare industry is generally highly regulated, so depending on the type of services provided, or products involved, companies must comply with healthcare regulations, as well as additional regulations related to cybersecurity and personal data protection.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Investing in digital health ventures in Chile presents attractive opportunities within a stable and increasingly clear regulatory environment. Key considerations include compliance with the RDPL and the transition to the NDPL, which aligns Chile's regulation with international standards for the processing of sensitive health data. From an investment perspective, it is important to assess the venture's regulatory strategy, particularly regarding potential MD classification and registration before the ISP, as well as its readiness to integrate with existing healthcare systems. Overall, a well-defined compliance roadmap and an understanding of interoperability requirements can position digital health businesses for scalable and sustainable growth as Chile's ecosystem continues to mature.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

In general terms, this could be attributed to a lack of overall regulation and initiatives to introduce new forms or expressions of digital health. Even in areas such as electronic clinical record regulation and interoperability, despite the existence of regulations in this regard, there are still technical and operational barriers to their implementation.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

There are no certification entities dedicated exclusively to the approval or implementation of digital health solutions. However, the following may eventually influence the clinical adoption of digital health solutions:

- Clinical protocols and governance inside healthcare organisations (hospitals/clinic committees).
- Medical scientific societies issuing clinical guidelines and implementation recommendations that drive practice patterns.
- Evaluation committees for the implementation of health coverage or coverage applicable to the public sector.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

There are no specific reimbursement models for digital health as such; coverage depends on whether the product or service fits existing benefit frameworks (*e.g.*, Explicit Health Guarantees System or "GES" and the Ricarte Soto Law apply to "sanitary technologies", including MD, some of which may qualify as a digital solution, such as digital glucometers).

On another note, FONASA, as a public payor, reimburses telemedicine and remote services only when codified under MoH tariff rules, which were updated during COVID-19 (*e.g.*, Res. 54/2020).

No digital health-specific certification is required for reimbursement.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Digital health due diligence must be conducted on a case-by-case basis. The absence of consistent standards may result in uneven assessment of clinical validation, interoperability, cybersecurity, data governance, and AI-related aspects (including data provenance, bias, monitoring, and auditability).

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

Although they cannot be fully addressed due to space

constraints, bills of law such as Bulletins 17.375-11 (National Digital Health Service and MD); No. 16.686-19 (technology transfer); and No. 16.82119 may have interesting future developments.

Endnotes

1 https://portalsaluddigital.minsal.cl/unidad-hospital-digital-realizo-mas-de-un-millon-de-prestaciones-durante-el-ano-2024

2 Since the Agency has not yet been established, no official implementation rules have been issued. The Ministry of Economy has circulated draft standard clauses, but their binding nature is disputed.



Mónica Pérez is a partner at Carey and co-head of the firm's Litigation and Arbitration Group. Her practice concentrates on civil and commercial litigation, as well as domestic and international commercial arbitration. She advises on a broad range of matters, including contracts, torts, corporate disputes, consumer protection, unfair competition, distribution agreements, international trade, secured transactions, and environmental law, among others. In addition, Mónica provides pre-litigation and strategic advice to national and international clients across diverse industries, including mining, insurance, energy, automotive, and retail.
She has been consistently recognised as a leading practitioner in litigation and arbitration by international publications such as *Chambers and Partners*, *The Legal 500* and *Benchmark Litigation Latin America*.

Carey
Isidora Goyenechea 2800, 43rd floor
Las Condes, Santiago
Chile

Tel: +56 2 2928 2203
Email: mperez@carey.cl
LinkedIn: www.linkedin.com/in/m%C3%B3nica-p%C3%A9rez-quintana



José Ignacio Mercado is a counsel in Carey's Data Protection and Technology Group. His practice focuses on matters related to privacy, data protection and cybersecurity, as well as intellectual property and the development of strategies to protect intellectual and industrial property, including preparation, negotiation and implementation of technology transfer agreements such as licensing agreements, franchising agreements, distribution agreements, among others.
He also has experience assisting technology companies with the preparation and implementation of commercial scale-up and go-to-market actions, both in Chile and abroad.

Carey
Isidora Goyenechea 2800, 43rd floor
Las Condes, Santiago
Chile

Tel: +56 2 2928 2612
Email: jmercado@carey.cl
LinkedIn: www.linkedin.com/in/josé-ignacio-mercado-campero



Camila Suárez is a senior associate at Carey and her practice focuses on life sciences, biotechnology and public law, advising companies on issues related to the pharmaceutical, cosmetics and medical technology industries.
She advises various international pharmaceutical companies on day-to-day legal and regulatory matters for their operations in Chile, including health registration and public procurement procedures before the health authority, among other matters.
Camila graduated from Universidad Diego Portales and holds a degree in Regulatory Aspects of Medicines, Cosmetics, Medical Devices and Disinfectants from Universidad de Chile.

Carey
Isidora Goyenechea 2800, 43rd floor
Las Condes, Santiago
Chile

Tel: +56 2 2928 2612
Email: csuarez@carey.cl
URL: www.carey.cl/en/resume/camila-suarez



Mariana Guzmán is an associate at Carey and her practice focuses on personal data protection, privacy, regulation and protection of intellectual and industrial property, e-commerce and matters related to new technologies, as well as regulatory and pharmaceutical law with a special focus on the pharmaceutical products, cosmetics, and medical devices industries. She advises various national and foreign clients on matters related to privacy and data protection, including the preparation of privacy policies and related contracts.
Mariana graduated from Universidad de Valparaíso and holds degrees in Economic and Business Criminal Law as well as Personal Data Protection, both from Universidad de Chile.

Carey
Isidora Goyenechea 2800, 43rd floor
Las Condes, Santiago
Chile

Tel: +56 2 2928 2612
Email: mguzmang@carey.cl
LinkedIn: www.linkedin.com/in/mariana-guzm%C3%A1n-guiorguiadez-291073176

Carey is Chile's largest full-service law firm, with 45 partners and more than 280 legal professionals. The firm's corporate, litigation and regulatory groups comprise specialised attorneys across all areas of law. Clients include some of the world's largest multinationals, international organisations, and many of the most important local companies and institutions. In 2012 and 2022, Carey was selected as "Latin American Law Firm of the Year" by *Chambers Latin America*. The firm is a member of WSG, PRAC, FLI, TerraLex, The Interlex Group, Employment Law Alliance, RIELA, and ALAE.

www.carey.cl

/Carey

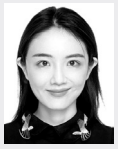
China



Yong Kai Chang



Chaoran (Oliver) Zhu



Jianing (Joy) Qiu

Allen & Gledhill LLP Shanghai Representative Office

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Though not legally defined in China, digital health usually represents a broad and interdisciplinary concept encompassing the use and integration of digital technologies in sectors such as medical services, public health, medical devices, pharmaceuticals, and health management.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The most prominent emerging subsectors include: AI-powered diagnostic and treatment support, especially in medical wearables, imaging and genomics; digital therapeutics ("**DTx**"); internet hospitals and telemedicine moving beyond consultation into an integrated health delivery ecosystem; "silver technologies" enabling real-time health monitoring, cloud-based healthcare delivery, and emergency response for the elderly population; and big data analytics platforms for population health management and drug research.

1.3 What is the digital health market size for your jurisdiction?

We are not aware of definitive data on the digital health market size in China. As an indication, "Market Research Future" estimates China's digital healthcare market size at USD 16.5 billion in 2024, and projects growth from USD 19.77 billion in 2025 to USD 120.67 billion by 2035, exhibiting a compound annual growth rate of 19.8% over the decade.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

We are not aware of definitive data on the comparative revenue of digital health companies in China.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Please see the response to question 1.4.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The principal regulatory authorities overseeing the digital health ecosystem include:

(i) National Health Commission ("**NHC**") – license and supervision of clinical practice and healthcare services relating to digital health, including medical ethics, professional qualifications and clinical protocols in internet hospitals and telemedicine.

(ii) National Medical Products Administration ("**NMPA**") – product classification, pre-market registration, and post-market safety surveillance to ensure that digital health hardware and software (including Software as a Medical Device ("**SaMD**") and AI-driven diagnostic tools) meet national medical standards.

(iii) National Healthcare Security Administration ("**NHSA**") – formulation of pricing and reimbursement standards for "Internet +" medical services and development of intelligent supervision systems to detect fraudulent claims, excessive prescribing, and other forms of clinical malpractice within digital platforms to ensure the integrity of national medical insurance funds.

(iv) Cyberspace Administration of China ("**CAC**") – data security and protection legislation and regulation, management of cross-border data transfers, core regulatory authority for AI/ML, covering regulation of AI algorithms and generative AI ("**GenAI**") used in the healthcare sector.

(v) National Data Administration (established in 2023) – facilitation of integration and sharing of healthcare data assets across different regions and institutions, including implementing the "Data Element x Healthcare" initiative and promoting the lawful development and commercial utilisation of health data to support the digital economy.

(vi) Ministry of Industry and Information Technology ("**MIIT**") – regulation of technical infrastructure and telecommunications through telecommunication licences for digital health platforms and mobile apps, and formulation and implementation of industrial standards.

(vii) Human Genetic Resources Administration of China – oversight of the collection, preservation, utilisation, and provision of human genetic resources within China.

(viii) State Administration for Market Regulation ("**SAMR**") – anti-monopoly and anti-unfair competition review for

digital health platforms, regulation of medical advertisements, supervision of service pricing, protection of patients' rights as consumers, and administration of national standards, including those for information security, medical device data, and quality management systems for digital health technologies.

(ix) Ministry of Public Security – criminal policing and enforcement for major digital health incidents (e.g., large-scale system breaches, hackings, and illegal data trading), public security matters, and cybercrimes.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Core healthcare regulatory schemes include:

(i) Medical devices/SaMD: The Regulations for the Supervision and Administration of Medical Devices ("**Regulations for Medical Devices**") issued by NMPA mandate strict registration for SaMD and AI diagnostic tools, ensuring algorithm-driven technologies meet high technical and clinical standards before market entry.

(ii) Medical services: Falling under the overarching policy of the Implementation Opinions on Promoting and Standardising the Application and Development of "AI + Healthcare", the Regulation on the Administration of Medical Institutions issued by NHC regulates internet hospitals and telemedicine.

(iii) AI/GenAI: The Interim Measures for the Management of Generative Artificial Intelligence Services ("**GenAI Services Measures**") issued by CAC govern the deployment of GenAI and require algorithm filings.

(iv) Data compliance: The Personal Information Protection Law ("**PIPL**"), the Cybersecurity Law ("**CSL**"), and the Data Security Law ("**DSL**") provide the foundation of comprehensive network security and data protection in digital health operations, classifying health information as sensitive personal information, necessitating strict consent and security measures. The specific national standards Security Technology – Guide for Health Data Security (GB/T 39725-2020) are implemented to further ensure data compliance at an operational level. Cross-border data transfers are subject to specific compliance formalities in specified circumstances. The Regulations on the Administration of Human Genetic Resources ("**Regulations on Genetic Resources**") ensure sovereign control over critical health data research.

(v) Market order: The Anti-Unfair Competition Law is enforced by SAMR to uphold market order by cracking down on unfair competition activities in digital health through the use of data, algorithms or technical advantages.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Key enforcement focuses on the enhanced protection of sensitive personal information, including medical and health data. Regulatory bodies, e.g., CAC, require internet applications to refrain from "excessive collection" of users' personal information and obtain "separate consent" for the processing of personal health data. Health data of the mass public, such as macro-level health statistics, infectious disease and population health information, and human genetic resources, are deemed as "Important Data" and any transfer of such data outside of China should undergo stringent security assessments.

Emerging enforcement areas are increasingly driven by the rapid integration of GenAI and large language models in clinical decision support and patient management. Both the amendment to the CSL and the GenAI Services Measures now require mandatory algorithm filing and security assessments for AI-driven diagnostic tools to ensure "scientific accuracy" and "ethical fairness". This aligns with the NMPA's enhanced management of AI-enabled medical devices, including "full-lifecycle" monitoring of algorithmic drift and software updates.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Under the Regulations for Medical Devices, together with their implementing rules and supporting technical guidance, these include but are not limited to, the Guiding Principles for Technical Review of Medical Device Software Registration, Guiding Principles for Technical Review of Medical Device Cybersecurity, Measures for the Administration of Medical Device Registration and Record-filing, and Technical Guidelines for the Clinical Evaluation of Medical Device Software. Based on its intended use, functional characteristics and risk profile, SaMD is generally classified as a Class II/III medical device, subject to product testing conducted by NMPA-designated testing institutions. Clinical trials are generally required for high-risk (Class III) or innovative software where existing data cannot prove safety and efficacy. For lower-risk or non-novel software, applicants may apply for approval by analysing clinical data from equivalent products already registered in China.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

For AI/ML-powered digital health devices or software solutions, their registration and approval are administered by NMPA and guided by the Guiding Principles for Technical Review of Artificial Intelligence Medical Device Registration ("**Guiding Principles for AI Medical Devices**"), which require applicants to demonstrate controllability, traceability and reliability across the entire algorithm lifecycle, including data sourcing, data annotation, model training, validation, performance evaluation and risk management. Where an AI-based medical device meets the statutory criteria for innovation and demonstrates clear clinical value, it may apply for an expedited review under the Innovative Medical Device Special Review Procedure.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Under the Guiding Principles for AI Medical Devices, NMPA emphasises continuous monitoring and risk management of "algorithmic drift" post-market. This moves away from a one-time static approval toward a dynamic oversight system

where any significant changes to the algorithm's core functions, intended use, or data processing methods may require change of registration. The GenAI Services Measures integrate mandatory algorithm filing and periodic security assessments into the clinical-use phase to ensure accuracy, transparency and ethical compliance of AI models as they evolve.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation is the core evidence required by NMPA to prove that an AI/ML algorithm translates into actual clinical safety and effectiveness. Under the Guiding Principles for AI Medical Devices, manufacturers must go beyond lab-test metrics and validate them against clinical datasets or through prospective clinical trials.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

China is a single-state jurisdiction with no federal system or distinction between state/regional regulation. China employs a hierarchical regulatory structure. At the national level, NMPA oversees the classification and approval of high-risk AI medical devices and sets unified technical and safety standards, while NHC regulates the provision of medical services and the clinical use of digital health technologies. At the provincial level, provincial counterparts of NMPA and NHC handle the registration of lower-risk medical devices, routine manufacturing inspections, and local supervision of healthcare services.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Regulatory enforcement of digital health products and solutions is evolving from static, licence-based oversight to tailored, lifecycle-oriented, function-focused governance targeting platforms, data flows, and algorithmic behaviour.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

Digital health technologies are subject to a dense, technical, and evolving legal and regulatory environment, where legal and regulatory issues tie into the technology's function (e.g., medical or non-medical), nature (e.g., AI or non-AI), type and use of data (e.g., whether sensitive personal information is involved), operational model (e.g., whether platform or hospital-based), and other factors.

NMPA regime: Technologies intended for medical purposes (e.g., SaMD, clinical decision support software, DTx, AI/ML-powered solutions, robotics, 3D printing/bioprinting, and medical-grade wearables, etc.) can be classified as medical devices, which require NMPA registration (Class II/III), rigorous clinical validation, and specific evaluations for algorithm integrity and safety as dictated by AI-specific regulatory guidelines.

NHC healthcare framework: Technologies/solutions focused on the delivery of care (e.g., telemedicine, virtual care, virtual triage assistants, and natural language processing for clinical documentation, etc.) should be affiliated with licensed physical hospitals to operate legally. The central regulatory constraint is the prohibition of online initial diagnoses, meaning these products must be technically configured to support only follow-up consultations for specific conditions. The technology serves as a digital extension of the hospital's existing medical practice licence rather than an independent provider.

Comprehensive data protection regime: The key issue regarding technical and data infrastructure (e.g., electronic medical record management solutions, big data analytics, IoT, mobile apps, blockchain solutions, etc.) is data processing and flow. Technologies involving human genetic resources, big data or bioprinting must strictly comply with the Regulations on Genetic Resources regarding the collection, preservation, and outbound transfer of human genetic resources to ensure national biosafety.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

One of the key issues is dual liability. If the platform facilitates online diagnosis and treatment, it typically must partner with or become a licensed medical institution, bearing legal responsibility for the quality and compliance of the medical services delivered through it.

As the digital platform consolidates vast amounts of sensitive personal health information from diverse sources (users, devices, partner institutions), platform providers should adopt heightened data security and compliance systems that involve rigorous data classification and encryption protocols, granular access controls, and mechanisms that support the fulfilment of data subject rights (access, deletion, portability, consent withdrawal).

Platform providers should regularly audit and monitor operational content including service and promotional information/materials, and practitioner qualifications on their platforms to prevent misinformation and illegal medical advertisements.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key issues in this regard include lawful basis for the processing of personal health data, data security and protection, sector-specific oversight by health authorities, and rigorous compliance requirements for cross-border transfers of personal health data, as set forth under the following major laws and regulations:

(i) The PIPL categorises health and medical information as sensitive personal information and imposes heightened requirements, including separate consent, purpose limitation, data minimisation, enhanced security measures, and the conduct of legally required personal information protection impact assessments ("**PIAs**") for high-risk processing activities.

(ii) The DSL and CSL impose obligations relating to data security management, risk prevention, and protection

of public interest in the process of processing personal health data, regardless of the types of the healthcare technologies.

(iii) The Provisions on Promoting and Regulating Cross-border Data Flow, Measures for the Security Assessment of Outbound Data Transfer, Measures for the Standard Contract for the Outbound Transfer of Personal Information, and associated regulations and guidelines impose different compliance formalities for cross-border transfers of personal health data outside of China, based on nature, application, volume, and risk of the data.

(iv) NHC and NMPA-issued health regulations (such as Administrative Measures on Internet Diagnosis and Treatment (for Trial Implementation), the Measures for the Ethical Review of Biomedical Research Involving Humans, the Good Clinical Practice for Medical Devices, and the Administrative Measures for Medical Device Clinical Trials) govern medical service quality, clinical research and trial activities, and the authenticity, integrity, and traceability of medical and research data, including requirements relating to consent, data management, and record-keeping.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

China is a single-state jurisdiction with no federal system or distinction between state/regional regulation. While national laws set the baseline, in Free Trade Zones ("**FTZs**"), certain pilot policies allow for streamlined approvals, cross-border data handling, and innovation in AI and clinical data use, but all activities must still comply with national data protection and medical regulations. FTZ policies provide regulatory flexibility for testing new digital health solutions while maintaining core obligations for data security, patient privacy, and clinical oversight.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

In terms of the nature of the entity, for a commissioned party (e.g., cloud storage service provider) who acts on behalf of a personal information processor (i.e., the entity that determines the purpose and methods of processing), its data processing is subject to instructions from and agreements with the personal information processor (it cannot process the data for its own purposes or disclose it to third parties without authorisation) and correspondingly, its obligations are relatively limited (including implementation of necessary data security measures, return or deletion of data upon completion of service, timely notification of data breach, etc.).

In terms of the nature of the data, personal health data is categorised as "sensitive personal information" under the PIPL, with heightened compliance requirements. Entities handling such personal health data must demonstrate that processing is truly necessary for the stated purpose, obtain explicit consent (which may require separate, specific authorisation beyond general consent), implement encryption and access controls, and will face more severe penalties for non-compliance.

4.4 How do the regulations define the scope of personal health data use?

Personal health data use is strictly defined by the PIPL and sector-specific regulations. Collection must serve a specific purpose and requires obtaining separate informed consent from the individual. Processing activities must adhere to the "minimum necessity" principle, limiting data use to the necessary extent to achieve authorised goals. However, for public interest (e.g., responding to public health emergencies or protecting life in crises), such data may be used without prior consent. China mandates that the cross-border transfer of such sensitive information must undergo certain required formalities, such as a CAC security assessment, signing standard contracts, or obtaining certification, to ensure national data security and patient privacy.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Contracts governing personal health data should include precise terms that clearly define the specific, legitimate purposes for processing and strictly limit data use to what is necessary for these purposes. The legal basis for processing, typically separate individual consent, should be specified, with clear allocation of responsibilities for obtaining and managing such consent and for fulfilling data subject rights. The contract should require robust technical and organisational security measures and explicitly prohibit data use beyond the agreed scope. It should also establish clear rules for data retention and stipulate the permanent deletion of data upon purpose fulfilment or contract termination, subject to statutory retention periods. Furthermore, the contract must outline comprehensive compliance and security governance for any third-party data sharing, include enforceable mechanisms for data deletion upon request or service termination, and detail incident response protocols and audit rights to ensure regulatory cooperation and provide indemnification for serious violations.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Data inaccuracy is primarily managed via the statutory "Right to Correction" under the PIPL, requiring processors to verify and rectify records upon request. Where personal health data is used in automated or algorithmic assessments with a significant impact on individuals, processors must ensure transparency and fairness, and provide individuals with explanations or the option to refuse significant automated decisions to combat bias and discrimination. As sensitive data, health information triggers heightened security and governance obligations, including mandatory PIAs for high-risk processing. These obligations are primarily enforced through CAC, while health authorities exercise parallel oversight through sector-specific regulation of medical services, clinical research, and data authenticity.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Please see the response to question 4.1.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Sharing personal health data in China involves navigating three primary legal challenges:

(i) Strict consent requirements: Under the PIPL, health data is classified as sensitive personal information, necessitating prior, specific, and separate individual consent for data sharing.

(ii) Balancing confidentiality and sharing: Healthcare professionals' statutory duty of confidentiality (as mandated by laws such as the PRC Civil Code) must be weighed against the legitimate needs for data sharing in treatment, referrals, and public health.

(iii) Lifecycle security obligations: The DSL mandates implementing comprehensive technical and organisational security measures throughout the data lifecycle to prevent unauthorised access, leakage, or breaches.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

China is a single-state jurisdiction with no federal system or distinction between state/regional regulation.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Nature of data-sharing party: The considerations change if an entity is a data intermediary. Please see the response to question 4.3. For professional confidentiality, whilst the core duty of confidentiality is mandated in fundamental laws such as the PRC Civil Code and applies uniformly, its application differs: healthcare institutions are governed by administrative rules (e.g., Medical Record Management Regulations), while individual professionals are bound by laws like the Doctors Law and professional ethical codes.

Nature of data: Please see the response to question 4.3.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please see the response to question 4.1.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Federated healthcare data sharing in China should comply with PIPL, DSL, CSL, and NMPA- and NHC-issued regulations. Key issues include obtaining user consent, limiting data use to specified purposes, and implementing strong data classification, encryption, and access controls. Participating entities must ensure auditability, traceability, and data integrity while complying with clinical and medical data standards. Cross-border transfers require security assessments or local approvals, and governance frameworks should address risk management, monitoring, and incident response.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patent protection is available in China for inventions, utility models and designs that satisfy the requirements of novelty, inventive step and industrial applicability. For example, for a new software-hardware combined wearable sensor, to establish patentability, the applicant must establish that the new system does not just adjust parameters of existing systems, but instead addresses a technical challenge in the medical field (such as symptom detection) and achieves specific clinical effects (such as diagnostic accuracy) by illustrating the clinical validation protocol and relevant results. The protection period for granted patents is 20 years for inventions, 10 years for utility models, and 15 years for designs, calculated from the application date.

In December 2024, the China National Intellectual Property Administration issued the Guidelines for Filing AI-Related Invention Patent Applications (for Trial Implementation), as a quick patentability reference for applicants seeking patent protection for AI-related inventions.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protection is available for digital health software to the extent of the entire software and its components, including source code, object code, user interface design, etc. For software authored by an individual, copyright lasts for the author's lifetime plus 50 years. For software created by a legal person or organisation, copyright lasts 50 years from the year of first publication.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected mainly through anti-unfair competition, contract and labour laws in China. Three key elements of trade secrets are secrecy, commercial value and reasonable confidentiality measures. In the context of digital health technologies, an unpatented diagnostic algorithm, unique clinical datasets, or proprietary data processing models, for instance, could qualify as protected trade secrets if they possess all the elements. Notably, trade secret infringements may incur civil, administrative and criminal liabilities depending on the circumstances in China.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

China has established a legal framework for academic technology transfers, centred on the Law on Promoting Scientific and Technological Achievements Transformation and detailed by its implementation provisions and other relevant regulations and policies. It promotes institutional autonomy by allowing transfer and commercialisation of technologies in various ways, encourages ownership reforms by launching pilot programmes where individual researchers may enjoy more rights in the service inventions, and emphasises market-oriented pricing mechanisms by introducing multiple pricing/trading modes such as auction, listing on a technology trading platform or negotiated agreements.

Notably, academic technology transfers are typically not required to go through governmental approvals or filings, unless national secrets, national security, transfers to overseas entities or applications for taxation incentives (if applicable) are involved.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

SaMD will be protected as software copyright under the copyright law. SaMD may also be eligible for patent protection if it is technically innovative, involves an inventive step and is capable of industrial application.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

An AI device cannot be named as an inventor of a patent in China. Under PRC law, an inventor refers to a person who has made creative contributions to the substantive features of the invention, and it has been clarified in the latest Guidelines for Patent Examination that such a person should be an individual and should not be an entity, organisation or AI.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

In principle, the undertakers (e.g., universities, research institutes, or companies) of government-funded projects typically own the resulting intellectual property ("**IP**"), but the government retains certain step-in rights to exploit or authorise others to exploit the IP for national security or public interest, or if the undertakers fail to exploit the IP within a reasonable period. Annual reporting to the authority supervising the project on the exercise and protection of IP rights is mandated.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Judicial precedents in China are influential but operate very differently from the "binding precedent" system in common law countries. Nevertheless, a 2023 ruling by the Beijing Internet Court recognised that an AI-generated picture constituted an original work protected by copyright (though the copyright is vested in its author, not AI), which was endorsed by the People's Supreme Court in its reports and publications. By the same logic, digital health software developed with AI tools may also qualify for copyright protection, provided its developer can demonstrate sufficient human intellectual input – such as innovative prompt design, parameter adjustment, or creative selection – that lends the work its originality.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Parties should strategically align their objectives to ensure mutual benefit, while contractually delineating clear terms for IP ownership, use rights, patent application rights and revenue sharing from jointly developed outputs. The contracts should also establish clear protocols for management of confidentiality, contributions and exit strategies to govern the partnership and mitigate risk.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Key considerations include separation of medical and non-medical functions, data governance, IP ownership, and regulatory and liability allocation (to the extent possible in law). The specific considerations would depend on the exact content of the cooperation and the parties' respective obligations, such as the nature of the data exchange involved.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Key considerations include the allocation of data processing roles, data governance, and coverage of associated risks arising from particular data security issues in such a structure, such as data breach or leakage, and accidental re-identification of improperly anonymised healthcare data.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Key considerations include: comprehensive data governance for legally sourced and sanitised data; and clear liability allocation with risk-proportionate indemnities for AI errors, data security issues, and IP infringement. When entering a market, digital health solution providers should define their product's position and intended medical use. These factors may govern the solution's risk category and the level of regulatory oversight.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

AI governance is a multi-level, coordinated system of authorities in China. The principal regulatory authority is CAC, with several other governmental organs playing key roles based on specific domains, technologies or industries. CAC is responsible for the overall planning, cross-department coordination, and enforcement of AI/ML regulatory schemes. MIIT is responsible for promoting AI industrial development, formulating industrial standards and managing AI infrastructure. The Ministry of Science and Technology administers the ethical review and compliance of AI research and development projects. SAMR supervises market competition in the AI industry. Other industry-specific authorities are responsible for regulating AI deployment in specific sectors, such as NMPA's regulation over AI deployment in digital health.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

China's regulatory framework for AI/ML is evolving rapidly from a principle-based approach to a more detailed and multi-layered system. At the fundamental level, CSL, DSL, and PIPL form the legal foundation for data processing, cyberspace security and personal privacy protection in all AI-related activities. In the key aspects of AI such as algorithm, deepfake technology and GenAI, the Provisions on the Administration of Algorithm Recommendation for Internet Information Services, the Provisions on the Administration of Deep Synthesis for Internet Information Services, GenAI Services Measures, and Measures for the Identification of Synthetic Content Generated by AI embody an inclusive but prudent, categorised and tiered regulatory strategy for different subjects, application scenarios and risk levels. In addition, more than 30 national standards related to AI provide the technical rulebook for the industry, covering aspects such as hardware/software, facial recognition, security, ethics, etc.

In digital health, the Implementation Opinions on Promoting and Regulating "AI + Healthcare" Application and Development (issued in late 2025) set forth a roadmap for systematic integration of AI across the medical field. Detailing 24 specific application scenarios across eight key areas, including clinical diagnostics, patient services and public health, the policy emphasises a dual focus on promoting innovative applications in healthcare while enforcing strict risk-based regulation to ensure public interest is protected.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Please see the case in the response to question 6.8. The affirmed principle is that AI is deemed a tool for humans' creative work, and copyright protection requires demonstrable human intellectual contribution, e.g., designing prompts, setting parameters, and making selective adjustments. Consequently, IP rights for algorithms improved by AI/ML without active human involvement cannot be attributed to the AI itself; such rights may only be granted when there is proven, active, and creative human involvement in the process.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Licensing data for AI/ML requires a precise definition of the scope of use, data rights, and risk allocation. The same applies to the licensing of healthcare data. In addition, more considerations will be given to ensure compliant use due to the privacy law compliance requirements and heightened liabilities for the mishandling of data.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

The regulatory focus is on functional risk and societal impact of the outcome, rather than the type of AI technology. As mentioned in the response to question 8.2, different authorities have issued different guidelines and specific rules to address the distinct risks inherent to different AI technologies, with a notable subset of regulations being tailored specifically for the challenges posed by GenAI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

GenAI introduces distinct challenges such as hallucination, lack of traceability, data poisoning, embedded bias and discrimination, malicious use, human accountability, etc. Key legislation such as the GenAI Services Measures adopts a balanced approach aimed at fostering innovation while ensuring security and mitigating systematic risks, combining both mandatory requirements such as security assessments and algorithm filings, synthetic content labelling and industry self-regulation and public supervision. These initiatives are expected to continue to evolve and refine along with technology and application upgrades.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

The primary approach to addressing AI/ML models trained with data lacking proper rights is through comprehensive *ex ante* compliance obligations in data processing and *ex post* corrective penalties, rather than specific "data disgorgement" laws. The regulations mandate that developers must ensure all training data is from legitimate sources, obtain necessary consents for personal information and respect IP rights, as detailed in analyses of risks from web scraping, internal data misuse, and open-source licensing. Violations may result in

administrative penalties, such as cessation of infringement, remedial action, fines and orders to suspend services if the violation is serious. Therefore, the legal focus is on prevention through strict data governance and enforcing corrective measures.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Civil liability for adverse outcomes in digital health is typically on a tort and contract law basis. Under tort law: product liability applies to defects in the software or device; medical malpractice or professional negligence claims may target healthcare providers who fail to exercise reasonable care when using or relying on digital tools; and various tort liabilities arise from breach of data protection duties causing unauthorised access, loss or misuse of patient data. Additionally, depending on the relationship between the parties, contractual liability may arise if the solution breaches stated performance standards or other contractual obligations.

9.2 What cross-border considerations are there?

The cross-jurisdictional nature of digital health complicates liability determination, as an adverse event may trigger competing claims under different legal systems. The core challenge lies in resolving conflict-of-laws questions, among others: (i) identifying the proper forum for litigation (e.g., the patient's location, the healthcare providers' domicile); (ii) determining which jurisdiction's substantive laws govern the standards of care for medical malpractice, product liability, or data breach; and (iii) addressing the practical hurdle of enforcing a judgment if the liable party's assets are located in a foreign jurisdiction. As liability exposure becomes fragmented and unpredictable, proactive contractual clauses on governing law and jurisdiction, as well as strategic consideration of local insurance and asset structures, are required to mitigate enforcement risks.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

To navigate the complicated liability risks in AI-driven digital health solutions, the best practices involve a proactive compliance strategy: implementing robust contractual and other frameworks that clearly allocate control, risks and responsibilities; ensuring rigorous clinical validation and continuous monitoring of AI performance to meet the requisite standard of care; maintaining clear human oversight to preserve accountability; and monitoring and adhering to stringent, evolving data governance and medical device regulations across all operational jurisdictions.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Misuse of healthcare data in AI/ML models typically involves three key pillars of liability:

(i) Administrative liabilities: Under the PIPL, unauthorised use, inadequate security, or failure to obtain proper consent for sensitive personal information may lead to severe administrative penalties, including fines, suspension of services, or revocation of business licences.

(ii) Civil liabilities: For infringement of personal information rights or privacy under the PRC Civil Code, the data subject may seek compensation against the processor for damage for unauthorised disclosure or misuse in model training or deployment.

(iii) Criminal liabilities: Serious misuse such as illegally obtaining, selling, or providing personal health data may constitute the crime of infringing upon citizens' personal information under the Criminal Law. Under the DSL, if the misuse involves "Important Data" or human genetic resources and harms national security or public interest, the processor may face further criminal sanctions.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud service providers (acting as commissioned data processors) operate within a stringent regulatory framework centred on liability sharing and regulatory compliance. A fundamental requirement is adherence to the Cybersecurity Multi-Level Protection Scheme, typically requiring Level 3 or higher certification for systems managing personal health data, which entails formal filing, periodic assessments, and security controls. Uploading/transferring sensitive personal information to cloud servers outside mainland China is a cross-border transfer, which may trigger mandatory compliance formalities for cross-border data transfer. Cloud service providers must hold qualified internet data centre and cloud service licences, and ensure hosted content complies with laws, safeguarding national security, state secrets, and third-party IP and privacy rights. Cloud service providers must operationally support data processing rights (such as requests for access, correction, deletion, and consent withdrawal) while maintaining application-layer security through strict access controls and identity management to prevent unauthorised breaches.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

They must navigate China's compliance regime involving healthcare, medical, data security laws, etc. Specifically, they must determine if their software functions as a medical device while simultaneously complying with the data compliance rules. In addition, the shift toward "Internet + Healthcare" requires non-traditional players to build deep partnerships with physical hospitals to ensure service legitimacy and access to public medical insurance settlements.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

China's healthcare sector is a highly regulated, public interest-oriented environment with varied and layered requirements that can vary significantly based on specific product, business and operational models. Venture capital and private equity

firms should prioritise regulatory due diligence to understand and mitigate exposure before committing to digital health investments. With regard to IP, the investors should assess third-party rights and infringement risks and ensure that the venture has adequately protected its own IP rights.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Major barriers include stringent regulatory supervision and approval requirements, clinical liability concerns, unclear claim policies by public insurance for various digital services, difficult integration with hospital IT systems and workflows, data silos and sharing challenges amid strict data security laws, automation bias fear, and entrenched cultural and organisational barriers.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Clinical adoption is heavily influenced by NHC and its affiliated academic societies in China, e.g., the Chinese Medical Information and Big Data Association. Professional bodies like the Chinese Hospital Association, Chinese Medical Association and the Chinese Medical Doctor Association shape clinical pathways and issue "expert consensus" that validate the use of digital tools. Relevant national quality control centres (e.g., for medical imaging) are crucial for the adoption of radiology AI, as they play a key role in setting the technical benchmarks for diagnostic accuracy.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Reimbursement for digital health solutions is primarily effected through National Basic Medical Insurance ("**BMI**"), supplemented by commercial insurance models and direct hospital procurement. To qualify for BMI reimbursement, products must first secure NMPA medical device registration (Class II/III) and obtain a standardised NHSA code.

Reimbursement is typically realised by integrating solutions into medical service price items or consumables catalogues, such as the now-standardised imaging cloud services. For high-value innovations not yet covered by BMI, certain government-guided commercial insurance (e.g., "Huiminbao") also provides an alternative channel for reimbursement through dedicated innovative device lists.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Key due diligence gaps in China's healthcare ecosystem for AI and data-driven solutions stem from a rapidly evolving regulatory landscape and fragmented data infrastructure. Navigating inconsistent data standards and "information silos" remains a significant challenge, often hampering the validation of training datasets and algorithms. A dynamic regulatory framework means that critical technical standards, ethical review protocols, and clear liability frameworks for AI-driven decisions are still maturing. Assessing algorithmic fairness, transparency, and safety is complicated by the absence of universal benchmarking tools and persistent concerns regarding data bias.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

Key trends include the "domestic substitution" policy, incentivising local procurement and the "Data Elements × Healthcare" initiative driving medical data commercialisation. Future growth lies in GenAI for clinical documentation and DTx for chronic disease management. Further, Chinese companies are increasingly exporting "Hard Tech" to Belt and Road markets while navigating cross-border compliance.



Yong Kai Chang is the Managing Partner of Allen & Gledhill (China) and a Partner of Allen & Gledhill Singapore. He leads our practice and growth in China and leads our engagements in the Chinese market, covering inbound and outbound investments and multi-jurisdictional matters involving China. Kai is native Singaporean and a Permanent Resident in China. He has close to 25 years of experience and over 20 years of experience in China and Hong Kong SAR. Kai has led and advised on global corporate, M&A, investments, and listings and capital markets transactions. He advises on corporate and commercial, regulatory and compliance, employment, restructuring, and white-collar investigations. He also has litigation, arbitration, and dispute resolution experience.
Kai is recognised by leading legal publications including: *The Legal 500 Asia-Pacific* for his expertise in Corporate and M&A, Regulatory & Compliance, and Restructuring & Insolvency; and *IFLR1000* for his expertise in Financial and Corporate work.
Kai's clients include state-owned and state-linked enterprises, multi-national and domestic companies, listed and private companies, banks and financial institutions in a wide range of sectors such as healthcare, pharmaceuticals, technology, banking and financial services, energy, infrastructure, construction, manufacturing, logistics, real estate, aviation, automotive, hospitality, and consumer goods. Prior to joining the Firm, apart from Singapore, Kai was in legal practice in Shanghai, Beijing, and Hong Kong SAR with leading international law firms. Most recently, he was an international partner in a Red-Circle Chinese law firm in China.

Allen & Gledhill LLP Shanghai Representative Office
Units 5001–03, Floor 50 Two Shanghai IFC
No. 8 Century Avenue Pudong New District
Shanghai 200120
People's Republic of China

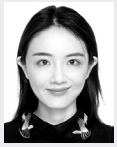
Tel: +86 138 1650 4248 (China) / +65 8139 5203 (Singapore)
Email: yong.kc@agasia.law
LinkedIn: www.linkedin.com/in/ykc76



Chaoran (Oliver) Zhu is a Senior Associate at Allen & Gledhill (China). His practices include international M&A, private equity investments (debt and equity), corporate and commercial advisory, regulatory and compliance, and other multi-jurisdictional matters involving China. He has also advised multi-national companies (including Fortune 500 companies) on their business operations in China, covering aspects such as investment structure, corporate governance, contract management practice, antitrust and competition, anti-corruption, data privacy, and labour compliance, and some of the world's top private equity funds that carry out investment strategies in Asia across various industries such as renewable energy, fintech, autopilot, pharmaceuticals, healthcare services, etc.

Allen & Gledhill LLP Shanghai Representative Office
Units 5001–03, Floor 50 Two Shanghai IFC
No. 8 Century Avenue Pudong New District
Shanghai 200120
People's Republic of China

Tel: +86 139 1847 6448
Email: oliver.zhu@agasia.law
LinkedIn: www.linkedin.com/in/oliver-zhu-a4a13660



Jianing (Joy) Qiu is a Senior Associate at Allen & Gledhill (China), specialising in corporate law, commercial transactions, and regulatory advisory. She has advised various multi-national corporations on the full business lifecycle in China, including foreign investment, M&A, corporate governance, financing, restructuring, relocations, and winding-up, etc. Joy also has extensive expertise in Chinese regulatory compliance across a broad spectrum of areas, including data protection, cybersecurity, healthcare, commercial advertising, technology, media and telecommunications, anti-money laundering, and employment law.

Allen & Gledhill LLP Shanghai Representative Office
Units 5001–03, Floor 50 Two Shanghai IFC
No. 8 Century Avenue Pudong New District
Shanghai 200120
People's Republic of China

Tel: +86 132 6290 5329
Email: joy.qiu@agasia.law
URL: www.allenandgledhill.com

Allen & Gledhill's Shanghai Representative Office comprises experienced Singapore, South-east Asia and PRC-qualified lawyers who are natively bilingual in English and Chinese. Many of them are also widely recognised as leading experts and specialists in their areas of practice by international legal publications. Our lawyers are committed to providing clients with holistic and practical legal services that are relevant to their multi-disciplinary needs in cross-border practices and matters. Combined with the support and resources across the Allen & Gledhill network known as A&G Asia, the team combines sound local knowledge with regional capabilities and international best practices to provide value-added advice and unparalleled service.
We have been involved in numerous China-related inbound and outbound matters, which span a variety of practice areas including international M&A, joint venture investments, capital markets, corporate and commercial, banking and finance, real estate, private equity, private wealth, international arbitration, and regulatory and compliance. We have also been involved in matters in areas such as banking and finance, high technology, family offices, energy, manufacturing, logistics, maritime, healthcare, mining, infrastructure, construction, technology, real estate, aviation, automobiles, hospitality, and retail.

www.allenandgledhill.com/cn

ALLEN & GLEDHILL
安 盛 律 师 事 务 所

France


Catherine Mateu


Pierre Camadini

Armengaud Guerlain

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

French law does not provide a global definition of "digital health", either at legislative or regulatory level. Only the concept of "telemedicine" is envisaged by the French Public Health Code, which states that "telemedicine is a form of remote medical practice using information and communication technologies". Teleconsultation, tele-expertise, telemonitoring and telemedical assistance, the purpose of which is to enable a medical professional to provide remote assistance to another healthcare professional during the performance of a procedure, are all considered to be telemedical acts.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Currently, France is expanding on the foundational need for telemedicine as an essential tool in post-pandemic Europe – saving doctors time with administrative tasks, reducing missed appointments and increasing the number of patients cared for. To this end, artificial intelligence (AI) software is being developed to help doctors save time, in particular by automating administrative tasks. "Thiana", for example, takes care of writing medical reports and prescriptions. In addition, the "*Mon Espace Santé*" platform serves as a digital health record launched in 2022 for all French citizens.

1.3 What is the digital health market size for your jurisdiction?

In 2019, the French "health unicorn", Doctolib – the largest digital health service in Europe – raised 150 million euros through funding, raising the company's value to over a billion euros. A study dated April 2025 reveals that in Europe, Doctolib claims 90 million patients, one million professional users, and 30 million teleconsultations, including more than 5.5 million in France. In 2025, Doctolib's value was estimated at 5.8 billion euros.

Recently, research conducted by the Institut Montaigne and McKinsey suggests that the digital health sector has the potential to yield an annual revenue from 16 to 22 billion euros in France.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

The five largest digital health companies in France, as far as we know and subject to evolution, are Doctolib (appointment scheduling, teleconsultation, practice management), Santéclair (health services platform), Qare (teleconsultation), Medaviz (teleconsultation) and Livi (teleconsultation).

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

The digital healthcare sector is booming, with rapidly evolving rankings, but as far as we know, certain companies dominate the market, such as Doctolib, Dassault Système (in the health division), Cegedim, Cerner France (Oracle subsidiary) and Medtronic (digital health technologies division).

Other players are also emerging on the French market: Nabla (AI for doctors); Alan (digital health insurance); and Owkin (AI in oncology).

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

In France:

- The French General Directorate of Health is one of the departments of the French Ministry of Health, responsible for preparing and implementing public health policy, health monitoring and health safety.
- The National Health Authority (HAS) aims to develop quality in the health, social and medico-social fields. It works alongside public authorities, whose decisions it informs, and with professionals to optimise their practices and organisations.
- The National Agency for the Safety of Medicines and Health Products (ANSM) is the public body that provides access to healthcare products (medicines and medical devices (MDs)) in France and ensures their safety throughout their life cycle via authorisation procedures.
- The Data Protection National Commission (CNIL) is responsible for ensuring the protection of personal data contained in computer files and processing, whether public or private.

- The Digital Health National Agency (ANS) sets out frameworks and best practices to facilitate the sharing and exchange of healthcare data (general security policy for healthcare information systems, guidelines, cybersecurity support and healthcare data).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

In France, these authorities regulate various aspects of digital health such as approval of MDs, AI and combination products (via CE marking and validation procedures), data compliance (especially personal data protection through the GDPR), as well as data security and cybersecurity. Rules against anti-competitive practices are also applied.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Digital health legislation focuses on the protection of personal health data, telemedicine oversight, cybersecurity of healthcare platforms and the regulation of connected MDs. It also applies to emerging technological fields such as AI, blockchain, public e-health and mobile health applications, aiming to ensure accessibility and quality of care.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

If a software product qualifies as a medical device, it must comply with commercialisation and monitoring requirements under EU Regulation 2017/745 (MDR) or Regulation (EU) 2017/746 on *in vitro* diagnostic MDs and in France specifically, by the French Public Health Code. These regulations also apply to devices with no medical purpose and include cybersecurity as a new essential requirement.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In 2024, the EU passed Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on AI, referred to as the AI Act.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Regulations are becoming more flexible, with regular updates to incorporate emerging technologies. The EU has specific AI regulations in place, including transparency and explainability requirements, and France is following these directives while developing harmonisation approaches for the digital marketplace.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data are crucial for AI/ML-based health solutions. These data are used to demonstrate the efficacy and safety of products before market entry. ANSM requires clinical evidence to assess the risks and benefits of digital health devices. Additionally, MDR regulations mandate clinical trials for high-risk devices.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Digital health products are regulated both by the State (via ANSM) and through European regulations (via MDR/IVDR). There are some differences at regional and national levels, particularly in terms of innovation support and specific requirements for certain product categories. However, France follows a unified approach at the national level while aligning with EU practices.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Regulatory enforcement in France is tailored to the specific characteristics of digital health products. For example, ANSM and CNIL work together to ensure compliance with both safety standards and data privacy regulations (GDPR). Enforcement actions also focus on post-market surveillance and traceability to ensure continued compliance.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Telemedicine, including teleconsultation, tele-expertise and remote assistance, requires minimal legal protection for patients' personal information. Platforms must ensure data security and the competence of doctors while complying with applicable laws.
- **Robotics**
  Robotics raises issues related to product responsibility and legal regulation to ensure the robots' capabilities and liability. The question of financial compensation for patients harmed by robotic medical errors remains inadequately addressed.
- **Wearables**
  Wearables such as smartwatches, fitness trackers and smart technology clothing are used to detect the health and wellness of people.
  However, by providing personal health information on their users, this digital health technology gives rise to legal issues such as data privacy, security and compliance with MD regulations.
- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants can help nurses schedule visits or remind patients to take their prescriptions. However, at the same time, they also bring about issues such as legal

liability and invasion of privacy if the personal health information is leaked out, and other legal risks.

- **Mobile Apps**
  Mobile apps are a tool for telemedicine and help patients access medical consults in a more effective way at anytime and anywhere in the world. However, the apps' liability and the protection of patients' information are to be taken into consideration.
- **Software as a Medical Device**
  Assigning responsibility in the event of a chain of liability is an important issue. Typically, the regulation on MDs and the provisions protecting health data apply. Social and public health issues related to the development of new devices will need to be addressed, and will probably be partly addressed in the forthcoming regulation on AI.
- **Clinical Decision Support Software**
  As far as legal issues about clinical decision support software are concerned, a few provisions can apply: the MDR to ensure compliance with the French regulations for MDs; the GDPR for personal data protection; and ethical considerations to ensure ethical principles during the decision-making phase.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Data protection, MD regulation and ethical principles are always the key issues when AI technology or a machine process with a great number of personal data provide solutions based on an algorithm. Inevitably, to avoid any litigation, it is necessary to have an individual's consent when an AI or machine processes their information.
- **IoT (Internet of Things) and Connected Devices**
  Apart from legal issues such as data protection, product liability and user consent, which are mentioned above, cybersecurity is also to be taken into consideration and must be compliant when the connected devices are put into use.
- **3D Printing/Bioprinting**
  3D printing or bioprinting involves several legal issues and must comply with MD regulation, GDPR for data protection, ethical principles (since human organs may be reproduced by a printer) and product safety provisions.
- **Digital Therapeutics**
  Concerning digital therapeutics, data protection, ethical considerations, user consent and MD regulation, and the issue of liability in case a wrong treatment occurs, are key issues.
- **Digital Diagnostics**
  As mentioned above, there are always legal issues such as MD regulation, data protection, user's consent and liability of digital diagnostics results to comply with. The regulation measures should also be taken to ensure that the collected data and used patients' data are not abused.
- **Electronic Medical Record Management Solutions**
  As mentioned above, data protection, preventing abuse of patients' information, users' consent and liability are the key issues. It is necessary to inform patients of the use, preservation and destruction of their information after a certain period of time.
- **Big Data Analytics**
  Data protection (GDPR), preventing abuse of collected data, consent of users (use of their data or information during a specified period then destruction) and the issue of liability. It is also necessary to strengthen the protection measures of personal information to prevent it from leaking.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The user's consent is the most important thing. Making sure that the data is shared with a credible partner to avoid any abuse or leaking of data, especially as there may be some very sensitive information that are strictly personal. Liability and data protection are also legal issues.
- **Natural Language Processing**
  Personal data protection with GDPR and user's consent are key issues. Compliance with specific regulations or guidelines issued by authorities such as the CNIL and ethical considerations are also mandatory.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Ensuring that everything on the platform is legal, there is no misleading information, no information against public order and good morals. Security measures are to be taken to prevent privacy information invasion, misuses or leaking of personal data.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Ensuring that personal data is perfectly protected and could not be easily leaked nor consulted by the public, and that consent is provided by the concerned individuals for the use of any personal data. In this area, the GDPR applies and apart from that, there are a few regulatory requirements such as the Data Protection Act (DPA, *Loi Informatique et Libertés*), other specific regulations or guidelines by the authority CNIL and the Telecoms and Electronic Communications Code.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In France and Europe, health data is regulated by the GDPR, which sets strict rules. France also has complementary laws like the French DPA, and regulation is centralised at the national level, although regional authorities may intervene in specific cases.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The GDPR allows some derogations in certain situations. However, it applies regardless of the nature of the entities involved.

4.4 How do the regulations define the scope of personal health data use?

The regulation especially defines the lawful practice of collection of data, the illegal use of collected data, and sanctions, in

order to ensure that the collection is not used for the collector's own interest only, or illegally.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

To ensure comprehensive rights regarding the use and collection of personal health data, key considerations include user consent, data usage aligned with contractual purposes, security measures to prevent misuse, a limited duration for data retention, and the individual's right to legal action in case of contractual breaches by the platform or organisation.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Transparency requirements, under the GDPR and the newly adopted AI Act, aim to address data inaccuracy, bias and discrimination by requiring data controllers to inform individuals about automated decision-making and its foreseeable consequences. The AI Act also prohibits AI systems that rank people's trustworthiness based on their social behaviour or personal traits, which could result in harmful treatment.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

In France, the collection and use of personal health data are governed by the GDPR, overseen by the CNIL, and complemented by the "*Informatique et Libertés*" law. Specific frameworks like the shared medical record (DMP) and the "*Ma Santé 2022*" law regulate the digitalisation of healthcare while ensuring personal data protection.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key legal and regulatory issues when sharing health data in France include compliance with the GDPR, which sets strict conditions for the processing of personal data. The French DPA complements the GDPR with specific rules for health data. Other laws, such as public health laws and data security regulations, may also apply. Additionally, considerations related to cybersecurity and the confidentiality of personal data are important, regardless of the technology sector.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There are no significant differences in regulation at the national and European levels, as rules are harmonised. However, national authorities may intervene in specific cases, especially regarding data security or compliance in certain public sectors.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The nature of the entities involved rarely matters. Most of the time the same provisions apply, whether the entities are public or private. The nature of the data is more important, since specific requirements can apply to medical data, as mentioned above.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

The European Health Data Space (EHDS), created in 2022, aims to provide a secure and efficient framework for the use of health data through common rules and standards. In France, the Health Data Hub, launched in 2019, facilitates the sharing of healthcare data and promotes standardised norms for their use.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

When it comes to federated models of healthcare data sharing, it is essential to inform patients and to facilitate the exercise of their rights. It is also essential to ensure data protection as well as data interoperability, especially for research and innovation. In that respect, the elaboration of standards and repositories can be very useful.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Contrary to what one might believe, exclusions from patentability are not an insurmountable obstacle to the patentability of e-health innovations.

If diagnosis methods are unpatentable *per se* in European law, this exclusion does not apply to the devices implementing these methods. Therefore, MDs or recording media are substantially patentable. Consequently, when it comes to connected health, the device itself can be protected, such as a wearable that measures blood flow and uses the data to diagnose cardiovascular problems.

Likewise, even though mathematical methods and computer programs are unpatentable as such, a computer program is patentable if it produces an additional technical effect (beyond the normal physical interactions between the program and the computer). In other words, a software controlling a dialysis machine or processing physiological data from sensors can be patented.

Finally, inventions incorporating AI can benefit from patent protection under certain conditions: their designated inventor must not be an AI system; their description must be sufficient; and their finality must be technical (concrete).

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Only original works in a fixed form can benefit from copyright protection. As concerns digital health, the design and multimedia elements of a device can be protected, as well as the expression of a software (their code and preparatory design material can be protected).

Regarding data, copyright can easily protect databases structures, not their content. Indeed, copyright protection of the data itself, which is at the heart of the valuation of e-health companies, is anything but obvious: raw data cannot be protected and processed data can be protected by copyright only if it is original, more precisely if it reflects free and creative choices. Besides, open data and open source may also limit copyright protection as connected health companies use a lot of open-source building blocks to develop their solutions. Indeed, improvements made from open-source software are generally subject to the conditions of a free licence, which implies a loss of value of the technology.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Raw or processed data, as well as databases, can be protected by trade secrets. E-health companies can therefore benefit from protection on the corpus of learning data used in their AI systems. Trade secrets may also protect algorithms, code, processes, parameters, etc. However, in those cases, trade secrets are more difficult to defend and promote; for example, it is not possible to prohibit a competitor from independently producing the same AI system.

To benefit from trade secret protection on data, whatever its nature, digital health companies must ensure that it meets three conditions: (1) it must be secret, that is to say confidential; (2) it must be subject to reasonable protective measures to maintain its secret nature; and (3) it must have commercial value. This last condition can be an obstacle, as in e-health innovations, the value results more from the combination of data than from the isolated data. In such cases, a contract controlling data access and use can be a complementary protection tool.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

In 2014, the European Commission enacted Regulation (EU) No. 316/2014. This regulation aims to guarantee that that technology transfer agreements respect competition rules. Its provisions create a safe harbour for most licensing agreements by providing guidelines and creating a so-called "block exemption" regulation. Besides this regulation, there are no specific rules applying to academic technology transfers in France.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

As mentioned above, a software as a MD can be protected and is patentable if it produces an additional technical effect. Patents offer strong protection but are limited in time (20 years). It is also important to note that this protection requires public disclosure of the invention as patent applications are published 18 months after being filed.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

According to EU law, an AI device cannot be named as an inventor of a patent according to EU law. In 2022, the Legal Board of Appeal of the European Patent Office (EPO) issued a decision in case J8/20, which confirmed that under the European Patent Convention the inventor designated in a patent application cannot be an AI machine. It can only be a human being with legal capacity, as a machine cannot defend and/or transfer any rights.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Beyond any rules or laws, it is the specific contract executed between the inventor and the government sponsor that determines intellectual property rights allocation. This is why public authorities must be careful and ensure that the contract enables them to use the products they ordered as they want to. For this reason, standard intellectual property provisions, adapted to the different public contracts, are made available by the government.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

In a renowned case, T 844/18, concerning a patent related to CRISPR-Cas9 technology (genetic scissors), the EPO had revoked the patent in question because the original applicants were not identical to those wishing to claim the right of priority. Recently, the EPO has softened its stance and now acknowledged that there is a rebuttable presumption that the applicant is entitled to claim priority (EPO Grand Chamber decisions, 10 October 2023, G1/22 and G2/22).

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

When dealing with collaborative improvements, parties should define a clear plan regarding the potential commercial results of their partnership, especially respecting intellectual property rights and their allocation to each party. For instance, joint ownership of results should be provided for when relevant.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

As the healthcare industry is a highly regulated sector, parties

must ensure regulatory compliance and guarantee continuity and traceability throughout the production and/or distribution.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

As personal data transfers are highly regulated, parties must implement adequate security measures during transmission. They should also investigate possible data breaches and agree on the correlative financial compensation.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties must make sure that the generative AI system presents sufficient guarantees in order to maintain control of the liability risks linked to its use. For instance, they could ask for the implementation of measures limiting the risks of violation of third-party rights via content filters or abuse detection mechanisms. More generally, parties must ensure that the supplier is able to offer a solid guarantee on possible third-party recourse in matters of intellectual property. Likewise, parties must ensure that the supplier does not provide in its contract for an assignment or licence on the content generated for its benefit, as this would likely hinder the free disposal of this content.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

In France, the main authorities are the CNIL, the Competition Authority and the *Autorité des Marchés Financiers* (AMF). The CNIL oversees data protection, the Competition Authority monitors anticompetitive practices, and the AMF regulates AI applications in financial markets.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

In France, key AI/ML regulations are governed by European frameworks such as the GDPR, overseen by the CNIL for data protection, and the Trust in Digital Economy Law (LCEN). For AI in healthcare, regulation is primarily through the Medical Devices Directive and the MDR, supervised by the ANSM.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

The author automatically owns the rights to such algorithms. However, if the author is an employee who acted within his duties or under instructions, his employer and/or company may acquire his rights.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

In France, licensing data for AI/ML requires compliance with the GDPR, ensuring consent, data security and transparency. Contracts should define the scope, duration and liability for data misuse. When licensing healthcare data, stricter conditions apply due to its sensitive nature under Article 9 of the GDPR and specific public health laws, requiring enhanced data protection and safeguards against misuse or discrimination.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

In France, regulatory bodies such as the CNIL and the European Commission differentiate standard AI from generative AI based on their functionality and potential risks. While standard AI typically involves data analysis and decision-making, generative AI creates new content. The EU AI Act places stricter regulations on high-risk AI systems, which include generative AI, due to the increased risks of bias, misinformation and misuse.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Generative AI technologies raise specific issues regarding intellectual property, data protection and liability. In France, the lack of clear legislation on AI-generated works creates challenges regarding copyright. The GDPR regulates data use, while AI liability remains unclear. At the European level, the AI Act aims to establish a legal framework for regulating risks, and in France, the National AI Strategy and institutions like the National Institute for Research in Digital Science and Technology (INRIA) are developing relevant standards and regulations.

In France, two decisions have highlighted the importance of introducing AI tools within companies and the need to regulate them.

The Nanterre Judicial Court had the opportunity to rule on the issue of a company's deployment of five new AI tools for internal use. More specifically, the CSE (social and economic committee, representative body for employees within companies) brought summary proceedings to suspend the deployment of the tools while its consultation was still ongoing. Based on Article L. 2312-8 of the Labor Code, the court noted that the CSE should indeed have been contacted in the event of "the introduction of new technologies, any significant changes affecting [...] working conditions", describing AI tools as measures affecting employees' working conditions. Thus, the CSE should have been consulted as early as the pilot phase, which concerned a significant number of employees.

On the same subject, the judge hearing the summary proceedings at the Créteil Court, on the basis of Article L. 2312-8 of the aforementioned Labor Code, reaffirmed the need

to consult the CSE in the event of the introduction of AI tools affecting employees' working conditions.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In France, the use of data in AI/ML models is primarily governed by GDPR, which requires data controllers to ensure that the data used in their AI/ML models is legally sourced and that the appropriate data rights are respected. If these obligations are not met, the data controller can be held liable and face administrative penalties, including fines of up to 20 million euros or 4% of global annual turnover. While France does not have specific data disgorgement laws, the control and sanction mechanisms under the GDPR, along with the transparency and accountability requirements, ensure that data is processed in compliance with European law.

The opt-out clause introduced by European Directive 2019/790 of 17 April 2019, has enabled copyright holders to prevent their works from being used via the data mining exception without their consent. This means that AI systems based on data collection will not be able to use works whose owners have decided to opt out.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Regulatory, civil and criminal theories of liability can apply to adverse outcomes in digital health solutions, depending on the case.

Regulatory liability often applies, as manufacturers failing to meet requirements can be sentenced to administrative sanction by regulatory authorities.

Civil liability also frequently applies, as manufacturers or distributors are liable for provisioning defective products in case of harm to the users.

More rarely, criminal liability applies, as manufacturers, distributors and other actors are held liable for ordinary offences or specific offences described in the French Public Healthcare Code.

9.2 What cross-border considerations are there?

E-health companies must consider the cross-border healthcare issue, especially if they wish to operate internationally within the EU. There are indeed specific conditions under which a patient may receive medical care from an HCP located in another EU country. Companies must therefore comply with the rules regarding the prescription, and the delivery of medications and MDs, as well as the healthcare costs. Likewise, companies should ensure their capacity to transfer data in compliance with the rules of the EHDS.

On top of this, non-EU companies should consider the specific rules applying to them. For instance, non-EU manufacturers must designate an authorised representative within the EU if they want to place one of their MDs on the EU market.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Implementing staff awareness measures and internal procedures can help minimise those risks. It is therefore important to monitor internal uses and to implement preventive measures. Training actions for staff should be carried out and a general use policy should be adopted. This policy could specify the basic points of vigilance.

Besides, evaluating the practices and guarantees applied by the AI suppliers is essential in controlling liability risks. The existence of sufficient technical and contractual guarantees must indeed be ensured.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

In French law, misuse of health data in AI/ML models may lead to a GDPR violation, particularly regarding unauthorised processing of sensitive data (Article 9) or failure to ensure security (Article 32). Civil liability could also arise from medical malpractice if AI causes harm to a patient. Additionally, sanctions may apply for non-compliance with future AI regulations in healthcare.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services for digital health must comply with the GDPR and guarantee ethical governance and sufficient security. They also have to enhance data assets and facilitate efficient data exchanges, in particular by promoting data interoperability. The key challenge is thus to find a point of balance between data sharing and protection of patient privacy.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Before entering today's digital healthcare market, non-healthcare companies should study the specificities of the sector, as it is a very complex industry. They should also review the applicable regulations, since compliance with the French and European norms is crucial.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Venture capital and private equity firms should study the market carefully before investing in digital healthcare projects. They should especially pay attention to the market needs and requests, to provide adequate and useful services.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

One of the key barriers in France is the lack of a comprehensive regulation with a body of dedicated norms. Other important barriers are the long and complex methodologies used regarding the assessment and reimbursement of medical health technologies. However, the efficiency of these processes may improve in the future.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In addition to the HAS (certifying), the ANS (public but non-certifying) influences the clinical adoption of digital health solutions. Besides, professional associations such as the SNITEM (*Syndicat National de l'Industrie des Technologies Médicales*) or the APIDIM (*Association pour la Promotion des Dispositifs Médicaux*) also encourage the certification of such solutions.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

In France, digital health solutions can be reimbursed under the "Health Innovation" reimbursement model, which includes telemedicine, remote patient monitoring and certain digital health apps. The government provides reimbursement through the French Social Security system, under specific conditions. To be eligible for reimbursement, digital health solutions must be certified as MDs by the ANSM and registered on the National Digital Health Platform. Additionally, these solutions must demonstrate clinical effectiveness and be approved by the French National Authority for Health.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence gaps for digital health solutions, particularly AI/ML-based, include algorithm transparency, data quality (especially GDPR compliance) and clinical validity. Legal liability is unclear, and interoperability with existing systems and data security (regulated by ANSSI) remain key concerns.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The pandemic has shown that innovation, alongside research and industry players, is key to bring out the best solutions for patients. Consequently, digital health actors are currently forming academic and industrial partnerships and developing new tools and practices, especially with the progress of AI. Legislators will certainly produce new norms to regulate these innovative strategies.



Catherine Mateu was admitted to the Paris Bar in 1999 and has over 15 years of experience in French and European intellectual property law. Defending the interests of all types of companies, her strategic analysis, litigation and contract practice encompass all intellectual property and related rights law.
A recognised expert, Catherine Mateu's work is regularly cited by *Who's Who Legal*, *Managing Intellectual Property*, *IP Stars*, *Chambers*, *The Legal 500*, *Décideurs*, *Women in Business Law*, etc.
Fluent in English and bilingual in French and Spanish, Catherine Mateu has developed extensive international expertise.

Armengaud Guerlain
12 Avenue Victor Hugo
75116, Paris
France

Tel: +33 1 47 54 01 48
Email: c.mateu@armengaud-guerlain.com
LinkedIn: www.linkedin.com/in/catherine-mateu-40330812



Pierre Camadini practises in all areas of intellectual property, providing legal advice and carrying litigation in trademarks, patents, copyrights and designs rights. Fluent in English, he regularly works for foreign clients on international cases.
Pierre Camadini previously worked in law firms specialised in intellectual property law, in France and abroad, and at the 3rd Civil Chamber of the Paris Judicial Court.
He holds a degree in Law from the Aix-en-Provence University, as well as a Master's degree in industrial and artistic property from the Paris I Panthéon-Sorbonne University. Pierre Camadini also holds a degree in comparative law from the Chongqing Southwest University of Political Science and Law in China.

Armengaud Guerlain
12 Avenue Victor Hugo
75116, Paris
France

Tel: +33 1 47 54 01 48
Email: p.camadini@armengaud-guerlain.com
LinkedIn: www.linkedin.com/in/pierre-camadini-191b05149

For 25 years Armengaud Guerlain has cultivated its first-rate reputation in intellectual property and intangible assets law.
Deepening and transmitting our expertise are the key elements that make up the firm's identity. Our know-how is rooted in the business realities of today and tomorrow.
We translate the law into clear advice that best serves our clients' needs.
www.armengaud-guerlain.com

ARMENGAUD GUERLAIN

Germany


Jana Grieb


Steffen Woitz


Dr. Claus Färber


Dr. Christian Lebrecht

McDermott Will & Schulte

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

German law does not define "digital health" specifically. Generally, the term is interpreted broadly and includes, *inter alia*: (i) digital healthcare services, including telemedicine; (ii) medical software applications for smartphones; (iii) medical devices that include artificial intelligence ("AI"); and (iv) other medical products that involve digital features, such as digital pills. Moreover, digital health is an umbrella term for the new markets in which the providers of the aforementioned products and services are active. Similar to "e-health", the term is symbolic of the rapidly advancing digitisation of the German healthcare sector.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Prescription and reimbursement of medical apps: In 2021, a new system for the reimbursement of medical smartphone apps (*Digitale Gesundheitsanwendungen* – "DiGA") was introduced under the statutory health insurance ("SHI"). The DiGA concept originally applied to apps that are CE-certified medical devices under the Regulation (EU) 2017/745 on medical devices ("MDR") risk class I or IIa. In 2024, class IIb medical devices were added to the DiGA system. DiGA can be prescribed by physicians and psychotherapists and are then reimbursed by SHI funds. In order to obtain reimbursement for a medical app, the manufacturer must file an application with the German Federal Institute for Drugs and Medical Devices (*Bundesinstitut für Arzneimittel und Medizinprodukte* – "BfArM"). Once approved, the applicable reimbursement thresholds are determined by and negotiated with the Federal Association of the SHI Funds (*Spitzenverband Bund der Krankenkassen* – "SpiBu").

To obtain approval for reimbursement, the manufacturer must prove that the medical app meets the requirements for safety, functional capability and quality and that it complies with data protection requirements. Additionally, the manufacturer must show that the app has positive effects in patient care.

At present, BfArM has approved 73 medical apps in total, 16 of which have meanwhile been deleted again, and 10 have so far only obtained temporary approval subject to further proof of positive healthcare effects.

In March 2024, the Digital Act (*Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens*) came into force. It aims at integrating DiGA further into the process of care and enhancing transparency. With the inclusion of class IIb medical devices, it will become possible to use DiGA in more complex treatment schemes such as telemonitoring.

Similar to the DiGA concept, a new system for the reimbursement of digital care applications (*Digitale Pflegeanwendungen* – "DiPA") was introduced in December 2022 under the statutory and private long-term care insurance regime (*Pflegeversicherung*). DiPA are intended to provide support to care recipients at home and designed to help alleviate the care recipient's loss of independence or capabilities or prevent their need for care from progressing further. Reimbursement is obtained under the same procedure that applies to DiGA.

Liberalisation of telemedicine: For many decades, telemedicine was largely restricted under German physicians' professional law. This had already started to change before the COVID-19 pandemic. In 2019, Germany set the legal basis for telemedicine, including video consultation by physicians, and their coverage by private and public payers.

Telemedicine is still subject to numerous regulatory restrictions. According to German professional laws, remote treatment can only take place if, among other things, the use of the telecommunication medium is medically justifiable, i.e. no further medical examinations are necessary to obtain a direct and comprehensive picture of the patient and his or her disease. Moreover, telemedicine business models are subject to high data protection and IT security standards, as they involve the processing of a significant amount of health data.

Electronic patient record: Since January 2021, Germany has been in the process of implementing the so-called electronic patient record (*elektronische Patientenakte* – "ePA"). The ePA is a central element of digital and networked healthcare. In January 2025, the "*ePA für alle*" version 3.0 entered a pilot phase in a selected model while simultaneously health-insurance funds began automatically creating an ePA for every person with SHI, unless they opted out. Since April 2025, the ePA has been available for use nationwide by medical practices, hospitals, and pharmacies. As of October 2025, the use of the ePA has become mandatory for physicians' offices, hospitals and other care providers.

1.3 What is the digital health market size for your jurisdiction?

The market for digital products and services in the healthcare sector is growing rapidly. Germany's digital health market is already several billion dollars in size. Most research firms place it at roughly USD 9–15 billion in the mid-2020s. They expect continued fast growth – usually double-digit percentages every year – which pushes the projected market size into

the tens of billions by 2030. Broader estimates that include many digital health categories show even larger totals, but the common takeaway is that Germany's digital health sector is expanding quickly.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

It is not possible to make a blanket statement in this regard. Many of the companies specialising in digital health are also active in other health or technology markets. As in other countries, the global tech companies such as Apple, Google, AMD Global Telemedicine Inc., Philips Healthcare or IBM play a significant role in the digital health market, offering solutions in remote monitoring, AI-driven diagnostics, telemedicine platforms, and connected medical devices. At the same time, university spin offs and other early stage companies are making their mark in this emerging sector as well. In the telemedicine sector, there are a number of promising platform operators that use their e-commerce and IT expertise to connect patients and physicians online.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Germany's digital health sector has witnessed significant growth in the last few years, with companies like Climedo Health, Noventi Health SE, Dyrad Networks GmbH and Avi Medical making notable strides.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The BfArM regulates the market clearance and reimbursement for most digital health products.

Market surveillance for medical devices, including medical apps, is carried out by supervisory authorities at a regional level.

The SpiBu and the Federal Assembly of the SHI and the Federal Panel Doctors' Association (*Gemeinsamer Bundesausschuss*) are the highest bodies of the SHI and are involved in the majority of reimbursement decisions for digital health products and services.

Federal and Regional Data Protection Commissioners (*Datenschutzbeauftragte des Bundes und der Länder*) are responsible for the supervision of data protection efforts.

The Telematics Society *(Gesellschaft für Telematik – gematik GmbH*) was created specifically regarding the task of developing a suitable and functioning healthcare telematics infrastructure ("TI"), including an electronic patient health card, electronic patient files and e-prescriptions. These applications are coordinated at the federal level with the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) and the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – "BSI"), which also have representation on a digital advisory board within gematik GmbH (*Digitalbeirat*).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Digital health products, including medical apps, often qualify as medical devices or *in vitro* diagnostics and, therefore, fall within the scope of the MDR and Regulation (EU) 2017/746 on *in vitro* diagnostics ("IVDR"). As EU regulations, the MDR and IVDR are directly applicable in Germany and do not have to be transposed into national law. The regulations are complemented by the German Act on the Implementation of EU Medical Devices Law (*Medizinprodukte-Durchführungsgesetz*).

Digital health services are subject to German healthcare regulations on the inpatient sector (e.g., hospitals and care homes) and outpatient sector (e.g., medical offices and home care providers). In these sectors, services are typically reserved for physicians or other healthcare professionals ("HCPs") who may be entitled to provide healthcare services. Physicians are subject to the requirement of a German approbation or other permit to provide physician-only services and bound by strict regulations under their professional codes.

Reimbursement of digital health products and services under the SHI regime is predominantly governed by the Fifth Book of the Social Insurance Code (*Fünftes Buch Sozialgesetzbuch* – "SGB V").

The laws on data privacy, in particular the General Data Protection Regulation ("GDPR") and the German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "BDSG"), are particularly relevant to digital health products and services. It is key for any digital health company to ensure that patient data are treated in line with these legal frameworks and protected against undue third-party access. Furthermore, depending on the respective health product or service, additional data protection regulations may apply, e.g., for the approval of medical apps or telemedicine services.

In Germany, the cooperation between the health industry and HCPs is subject to various healthcare compliance regulations. Their purpose is to protect independent medical decisions of HCPs, patient health and fair competition among healthcare providers. To this end, the regime in particular seeks to prevent any undue influence on HCPs. The applicable healthcare compliance provisions are manifold and complex. They equally apply to any cooperation and business activities in the digital health sector.

On 1 August 2024, the Regulation (EU) 2024/1689 ("AI Act") entered into force. As an EU regulation, it is directly applicable in Germany. The AI Act provides additional requirements for medical applications that include or are AI systems.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The key areas of enforcement for digital health are still the compliance of products that constitute medical device software ("MDSW") with the sector-specific laws and regulations and the compliance of any digital health services with the laws on the provision and reimbursement of physician services, as well as pharmacy laws and restrictions that are relevant to digital health applications and websites that offer medicinal products.

Where digital health products or services require the transfer and processing of personal health data, data protection authorities supervise the market as well. Failure to meet

data protection requirements may result in severe sanctions, such as an injunction to stop the processing, and/or fines of up to EUR 20 million or 4 per cent of the total worldwide annual turnover, which can be publicly issued.

In future, the enforcement of the AI Act will become relevant. According to Article 70 of the AI Act, Member States had to appoint competent authorities by August 2025. In Germany, the Federal Ministry of Economics and Climate Protection and the Federal Ministry of Justice are jointly responsible for implementing the AI Act. While some areas of enforcement are presumed to lie with data protection authorities, others will likely be supervised by the BSI. According to a 2025 draft of the implementing legislation (*Gesetz zur Durchführung der KI-Verordnung*), the Federal Network Agency (*Bundesnetzagentur*) is intended to serve as the central market surveillance authority and notifying authority for AI systems in sectors not already covered by specialised supervision.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

MDSW is regulated under the MDR or IVDR, under which it must be certified as conforming to safety and other requirements before being placed on the market. To obtain a CE-mark in accordance with the MDR or IVDR, MDSW must undergo a conformity assessment procedure that, depending on the risk class, can be passed through by the manufacturer (self-certification) or requires the involvement of a notified body. Upon successful completion of the conformity assessment procedure, the CE-mark can be affixed to the MDSW product.

Before the MDR came into force, MDSW was generally classified under risk class I and subject to self-certification under the Directive 93/42/EC on Medical Devices ("MDD"). Under the MDR, many MDSW are now subject to higher risk classes. Therefore, manufacturers must regularly obtain their CE certificates from notified bodies.

The transition scheme under the MDR allows for manufacturers of class I MDSW to benefit from a grace period. Initially, the transition periods were set to expire in May 2024. However, the European Commission acknowledged by the end of 2022 a significant threat to the availability of medical devices in the EU and thus extended transition periods with Regulation (EU) 2023/607.

Under the transition scheme, manufacturers of up-classified former class I MDSW may continue to market their products under the previous MDD regime until 2028. For MDSW in higher risk classes, transition periods vary according to the risk class. To benefit from the extended transition periods, manufacturers must have initiated measures to comply with the MDR before the expiry of the original transition period. In particular, manufacturers must by then have implemented a quality management system in accordance with the MDR and lodged a formal application for conformity assessment with a notified body. A written agreement among manufacturer and notified body must have been signed by September 2024.

As a result, while the fundamental principle remains – MDSW require MDR/IVDR conformity to be placed on the market – many devices that were formerly self-certified under the old directives may still legally be available under the extended transitional regime, provided they meet the relevant conditions.

Finally, the Medical Device Coordination Group of the European Commission continues to issue guidance documents on qualification and classification of MDSW, which remain relevant for manufacturers and regulatory professionals seeking to assess whether a given product qualifies as MDSW and which regulatory path applies.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Germany has not enacted a specific law on AI or ML so far. Products that include AI/ML are subject to the same regulations as other products, including medical devices law and data protection, as well as cybersecurity regulations. As part of a medical device, AI/ML software must comply with the requirements of the MDR or IVDR.

However, as the AI Act is directly applicable in Germany, the regulatory requirements under the AI Act apply even without implementing laws. The requirements under the AI Act depend on the risk the AI systems present in the specific use case. According to Article 70 of the AI Act, there will be three types of competent authorities in Member States under the AI Act: a Market Surveillance Authority; a Notifying Authority; and a National Public Authority. In Germany, a draft national implementing act – the AI Market Surveillance and Innovation Promotion legislation (*Gesetz zur Durchführung der KI-Verordnung*) – has been published and is currently subject to hearing of the German states and relevant associations. According to the draft, the Federal Network Agency (*Bundesnetzagentur*) is proposed as the central market surveillance authority and notifying authority. In addition, existing market surveillance authorities, such as the Federal Financial Supervisory Authority for the financial sector, will remain responsible for their respective areas.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Notified bodies will in future have to adapt their review of medical devices to reflect the dynamic nature of AI/ML to a certain extent. Guidance comparable to the US FDA AI/ML discussion paper is not yet available. The applicable standards, such as EN/IEC 62304 and EN/IEC 82304-1, provide a framework for software lifecycle development including device architecture and detailed design.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Where AI/ML systems are medical devices, the MDR requires rigorous clinical evaluation that includes validation data. Clinical validation data also informs the design of post-market surveillance plans, which monitor the AI/ML system's performance in real-world scenarios after deployment.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

While such products are predominantly regulated on EU and national levels, there are certain state level laws, such as laws on data protection, that affect digital health products.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Besides overseeing compliance with the EU MDR, GDPR, and now the AI Act, German regulators are increasingly scrutinising cybersecurity practices in digital health products to safeguard patient data and system integrity.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Despite significant liberalisation (see question 1.2 above), telemedicine and virtual care services are still considerably restricted. Remote treatment of patients must be medically justifiable, i.e. the case must not require an in-person examination at the physician's practice, and the patient must receive adequate disclosure regarding the specific risks, limitations, and procedural characteristics associated with exclusively digital consultation and treatment modalities.
- **Robotics**
  Robotics are machines that have the capacity to (partly) substitute HCPs. Such machines will, in most instances, qualify as medical devices (see question 2.6). Depending on their functionality and autonomy level, they may additionally fall within the scope of high-risk AI, triggering enhanced governance, testing, documentation, and oversight obligations.
- **Wearables**
  Wearables, such as smartwatches or smartglasses, often serve multiple purposes, and their primary purpose may not even be of a medical nature. However, if wearables come with health-related features, they might qualify as medical devices and require CE-certification.
- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants (such as Amazon's Alexa, Microsoft's Cortana, or Apple's Siri) usually have not been designed with health-specific features and are thus not considered medical devices.
- **Mobile Apps**
  Mobile apps that implement health-related features may be considered MDSW and, thus, may require CE-certification. Medical apps of MDR risk class I, IIa or IIb may be approved for reimbursement (see question 1.2 above).
- **Software as a Medical Device**
  As with mobile apps, other software that implement health-related features may equally qualify as MDSW (see above).
- **Clinical Decision Support Software**
  As with other software that implements health-related features, clinical decision support software may qualify as MDSW (see above).
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Digital health solutions powered by AI and ML can be a powerful tool for medical diagnostics and monitoring. The training of neural networks and similar AI/ML algorithms necessarily requires a large amount of personal health data that must be obtained in compliance with data protection laws. At the same time, the results are often not sufficiently protected by intellectual property rights (see question 8.3).
- **IoT (Internet of Things) and Connected Devices**
  Connected medical devices such as long-term EKG or blood pressure metres are subject to the MDR and thus require CE-certification.
- **3D Printing/Bioprinting**
  3D printing and bioprinting can be used to manufacture prosthetics and tissues. In the future, this technology might even be used to create whole organs. The use of 3D templates for prosthetics and tissues also raises new intellectual property and licensing questions.
- **Digital Therapeutics**
  Digital therapeutics are treatment procedures based on digital technologies. Such technologies may, depending on their specific features, qualify as MDSW (see above).
- **Digital Diagnostics**
  The same applies to diagnostic procedures based on digital technologies. These technologies may, depending on their specific features, qualify as MDSW (see above).
- **Electronic Medical Record Management Solutions**
  Electronic medical record management solutions have been used for decades as stand-alone systems. Under the continued expansion of the TI, accredited providers must ensure full interoperability with TI-compliant components. This includes mandatory connection of practice management systems, implementation of certified interfaces, and support for core applications such as the ePA, e-prescriptions, and Communication in Medicine (*Kommunikation im Medizinwesen*).
- **Big Data Analytics**
  Big data are key to successful research and development in the life sciences sector. A major challenge is to collect, use and commercialise large amounts of health data in compliance with the GDPR, either through anonymisation or based on consent of the relevant data subjects.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The current Federal Government's e-health/telematic infrastructure is not based on blockchain technology but on a more traditional public-key scheme. Furthermore, the use of public or semi-public blockchains for digital health is a no-go because on that basis, it would not be possible to adequately protect health data.
- **Natural Language Processing**
  Natural Language Processing ("NLP") describes techniques and methods for automatic analysis and representation of human speech. NLP is, *inter alia*, used in pharmaceutical research. If used for digital health, the confidentiality of spoken text needs to be preserved under data protection and professional secrecy laws.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Platforms that facilitate transactions between healthcare providers and patients are subject to the requirements of Regulation (EU) 2019/1150 (Platform-to-Business Regulation), which sets out minimum standards for terms and conditions, transparency and fairness. Furthermore, large health platforms could in the future reach the thresholds for a designation as a gatekeeper under Regulation (EU) 2022/1925 (Digital Markets Act). As such platforms do not qualify as licensed healthcare providers, they are not authorised to process health data under Article 9(2)(h) of the GDPR but will often need to obtain valid consent from end-users.

Increased data security requirements for health data means that they cannot rely on unencrypted e-mail but need to establish a more secure channel with patients.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The use of personal data is governed by the GDPR. Health data qualifies as a special category of personal data; its collection and further processing is generally prohibited unless a special exemption applies (Article 9 of the GDPR).

In addition to the requirements of the GDPR, the unauthorised disclosure of personal secrets of patients by HCPs and their auxiliaries is subject to criminal liability under Sections 203 and 204 of the German Criminal Code (*Strafgesetzbuch*).

For connected medical devices and other equipment, the Telecommunication-Digital Services Data Protection Act (*Telekommunikation-Digitale-Dienste-Datenschutzgesetz*), which transposes certain parts of Directive 2002/58/EC, imposes additional restrictions on remote access to data, even if it is not personal data.

The EU Data Act (Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data) also covers digital health products and services. It requires vendors to make available both personal data and non-personal data to the user and third parties requested by the user. Additional design requirements for connected (medical) devices will apply from 12 September 2026.

Under the GDPR, every entity responsible for the processing of personal data (data controller) is subject to transparency and documentation obligations. In particular, the data controller must:

- inform the individuals (data subjects) how their data is processed;
- maintain a record of processing activities; and
- conduct data protection impact assessments ("DPIA") and possibly consult with the competent authority prior to certain risky types of data processing – this will often apply to digital health applications that involve sensitive health data and new technologies.

Under the BDSG, an entity is required to appoint a data protection officer ("DPO") if it employs 20 or more persons with the processing of personal data, or if it needs to conduct a DPIA. Hence, digital HCPs in Germany will usually require a DPO.

HCPs are also required to take additional measures to ensure that their staff and service providers are warned of their potential criminal liability and thus maintain confidentiality.

Furthermore, HCPs that are medium-sized enterprises or bigger must comply with the requirements of the Directive (EU) 2022/2555 (NIS 2 Directive) and the German Act on the Federal Office for Information Security and on the Cybersecurity of Entities (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen*).

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

While the GDPR and federal laws apply throughout Germany, different state laws apply to the processing of personal health data by public healthcare providers operated by the State or by local authorities. These vary in the exact requirements and security standards for the processing of personal health data by these entities, and whether and under which conditions they allow engaging a data processor outside the EU/EEA.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The GDPR sets out different requirements for health data, depending on the nature of the entities involved and the purposes for which personal data is processed.

Licensed HCPs are permitted to process special categories of personal data for the purpose of occupational and preventive medicine, diagnosis and treatment (Article 9(2)(h) of the GDPR). This covers laboratories and other HCPs that cooperate with physicians, as well as medical and non-medical service providers acting on behalf of these professionals, and organisations that manage insurances and social security systems.

Research organisations, conversely, may rely on a permission to process personal data for scientific and historical research purposes under Article 9(2)(j) of the GDPR and Section 27 of the BDSG.

Data processed by public payors enjoys additional protection as "social security data" (*Sozialdaten*) under Section 35 of the Social Insurance Code I (*Sozialgesetzbuch Erstes Buch – Allgemeiner Teil*). Sections 67a *et seq.* of the Social Insurance Code X (*Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz* – "SGB X") imposes stricter requirements on the processing compared to those of the GDPR.

For private organisations that are neither involved in the provision of healthcare nor in scientific research, the use of health data is more challenging. In many cases, such organisations must obtain explicit consent as set out in Article 9(2)(a) of the GDPR, as no other exception from the ban on the processing of special categories of personal data applies. This includes suppliers of medical equipment or diagnostic services that wish to re-use personal data for their own purposes, such as product improvements, as well as entities that provide health-related products and services, such as vendors of wearables that record health data, or digital platforms that facilitate finding the best doctor who is an expert for specific ailments.

4.4 How do the regulations define the scope of personal health data use?

Under the GDPR, the scope of data use is limited by the purpose for which the data was originally collected, and the legal basis used.

Health data as a special category may only be processed for certain purposes. By way of example, HCPs can use health data for the provision of medical services and related administrative purposes. However, if they exceed this scope – even if they just want to share anonymised data with the vendor of their equipment – they will need to obtain consent from their patients.

Under Regulation (EU) 2022/2065 (Digital Services Act), digital platforms – whether health-related or not – are not permitted to target advertisements based on the profiling of health data or other special categories of data (Article 26(3)).

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Regarding compliance with the GDPR, one of the key considerations is identifying the roles of the parties in relation to the processing of personal data:

- if an entity (processor) processes personal data on behalf of another (controller), a data processing agreement is required under Article 28 of the GDPR;
- if two entities are jointly responsible for the processing of personal data, they need to enter into a joint controller agreement under Article 26 of the GDPR; and
- between independent controllers, the GDPR does not directly require specific contractual provisions; however, the parties may want to restrict the re-use of data in order to minimise the risk of non-compliance with the GDPR.

Liability and indemnification obligations are two of the key considerations for every contract. For the use of health data, this is amplified due to the potential for high fines under the GDPR.

Under the EU Data Act, providers are also required to inform the users about the non-personal data generated by a product or service before entering into a contract.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Data inaccuracy is currently not in the focus of data protection authorities. There have been a small number of investigations or warnings reported where data was inaccurate. Due to the fact that automated decision-making is limited by the GDPR, there is a relatively low risk of bias and discrimination based on profiling and data use.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The German BSI publishes various technical standards regarding IT security for handling personal health data. This includes mandatory technical standards for participation in the health telematic infrastructure as well as common standards such as the C5 (Cloud Computing Compliance Criteria Catalogue), which are made mandatory for healthcare providers and public payors by Section 393 of the SGB V.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the GDPR, there must be a legal basis for sharing personal data. In digital health markets, this often means that the HCP collecting health and other personal data for purposes of diagnosis and treatment must obtain explicit consent from his or her patients in order to share data for other reasons, such as research or product improvement. This applies even when the professional aggregates or anonymises the data before sharing, as this preparation of data is already a processing activity outside the scope of the provision of healthcare. When data must be made available under the EU Data Act, e.g., when a user requests this, such data must be shared under fair, reasonable and non-discriminatory terms and in a transparent manner.

When sharing data outside the EU, the GDPR imposes additional restrictions to ensure that the personal data remains adequately protected. If the target jurisdiction is not subject to an adequacy decision of the European Commission, adequacy must be ensured through effective contractual undertakings. For transfers to the United States, the new Data Privacy Framework ("DPF") allows the transfer of personal data to participating entities. However, it remains to be seen whether this new framework will – unlike its predecessors – hold up to the scrutiny of the Court of Justice of the EU.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

While the GDPR and federal laws apply throughout Germany, different state laws apply to the processing of personal health data by public healthcare providers operated by the State or by local authorities. These vary in whether and under which conditions they permit data sharing and transfers outside the EU/EEA.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The GDPR sets out different requirements for health data depending on the nature of the entities sending and receiving the data.

Sharing data between HCPs for the purposes of diagnosis or treatment is usually covered by an authorisation stipulated in Article 9(2)(h) of the GDPR. Similarly, professionals can share information with the health insurance for the purposes of billing under this provision. However, these entities must also take professional secrecy into account and must ensure that patients' secrets will only be shared with others who are subject to professional secrecy or written confidentiality undertakings.

For public payors intending to cooperate with others, Sections 67d to 76 of the SGB X contain an exhaustive list of the purposes for which health data and other social data may be disclosed to third parties. Section 77 of the SGB X also bans most transfers to jurisdictions outside the EU/EEA for which no adequacy decision exists. For recipients in the United States, this means that they can only receive social data under the EU–U.S. DPF.

For private payors, these rules do not apply. However, according to Section 213 of the Insurance Contracts Act (*Versicherungsvertragsgesetz*), they may only receive personal health data from HCPs, public payers and certain public bodies, and only with the patient's consent. This limits the cooperation with third parties, such as the providers of digital health products and services.

In order to be able to share data with research organisations, one may rely on the permission to process special categories of personal data for scientific and historical research purposes under Article 9(2)(j) of the GDPR and Section 27 of the BDSG.

Public healthcare providers (e.g., a municipal hospital) and research organisations (e.g., a state university), as well

as private hospitals, may be subject to additional restrictions from state data protection laws and governmental policies when sharing health data.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

When sharing personal data, one of the key requirements is ensuring that there is a legal basis for the disclosure of personal data. For health data in particular, one of the exceptions set out in Article 9(2) of the GDPR must apply. In many cases, this requires obtaining the patient's or data subject's consent. For this consent to be valid, the data subject must be informed how their personal data will be used, and with whom it will be shared. The EU Data Act would also require data to be shared with government bodies under certain circumstances.

The ePA and electronic prescriptions (*E-Rezept*) are available for patients covered by public health insurance and certain private health insurers. Patients who opt-in to the ePA can store or have their HCPs store medical reports, standardised medication plans, x-rays and other documents. These documents are currently not machine-readable, although this is planned.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

With the ePA, the governmental system already provides for a federated model of data sharing. As this system is designed around the public health insurance models, one of the key issues is the inclusion of private health insurers.

Furthermore, the Health Data Use Act (*Gesundheitsdatennutzungsgesetz*) provides a legal basis for pharmaceutical companies in Germany to access and use patient health data for research purposes.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patent protection plays an important role for digital health technologies and is granted upon application for any invention having a technical character if it is new, involves an "inventive step" and is suitable for industrial application. The digital health market's core technology (e.g., sensors and hardware) is generally patentable. The number of worldwide IoT patent applications has increased substantially; the health sector is contributing significantly to this development.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright law has the purpose of granting exclusive, non-registered rights to the author or creator of the original, non-technical work. The work can also be a computer program, e.g., a statement, program language or mathematical algorithm, if it is an individual work and therefore the result of the author's own intellectual creation. However, efficient protection of an invention can only be achieved with the help of a patent; at most, copyright law can offer accompanying protection. Data created by digital health computer programs, however, can never be subject to copyright, because they are not an individual work and therefore, not the result of an author's own intellectual creation.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets can be a useful tool to generate value for digital health companies if patent protection is not available, e.g., regarding software source codes or algorithms. The prerequisite of trade secret protection is that it relates to something that can be kept secret and actually is kept secret through reasonable efforts. For example, obvious elements of technology (design, etc.) or business strategies will not remain secret once placed on the market. To maintain secrecy, companies must – in accordance with the Trade Secrets Law (*GeschGehG*) – implement a confidentiality programme that includes organisational (e.g., trade secret policies), technical (e.g., IT security) and legal steps (e.g., extensive confidentiality clauses). Only the trade secret as such is protected, not the results achieved with it. This is relevant in the context of data protection, since, for example, a trade secret covering data processing means it does not cover generated data.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Academic technology transfer from university employees to their university employer is subject to certain university employee privileges under the German law on employee inventions because of the freedom of teaching and research. As opposed to normal employees, a university employee does not have an obligation to report or to disclose a service invention. If a university employee wishes to disclose his or her invention, he or she must notify the university employer of the invention. If a university employer claims a service invention that was disclosed by its employee, the inventor retains a non-exclusive right to use the service invention within the scope of his or her teaching and research activities. If the university employer exploits the invention, the amount of the remuneration is 30 per cent of the income generated by the exploitation. This percentage is much higher than the employee-invention remuneration of a normal employee.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

In the healthcare sector, the main question is whether intellectual property protection is available for software inventions, e.g., MDSW. If MDSW represents an abstract idea and, therefore, protection is sought for computer programs as such, there is no protection according to patent law. Under German and European patent law, protection is only possible for algorithms and methods underlying the programs that have an inventive step over the prior art – one that is found based only on features that contribute to the technical character. According to German case law, however, computer programs that immediately trigger a technical effect or directly optimise data-processing hardware are considered patentable. The same rules apply to copyrights, since the underlying concept is

never fully protected. Trade secret protection for MDSW is only possible under the restrictions described in question 6.3.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

In Germany, an AI device has not been named as the inventor of a patent yet. Several applications for the registration of patents "invented" by an AI device have been rejected. The German Patent Act requires an invention to have a human inventor. On a deeper level, the "inventive step" is still seen as an intellectual achievement of a human and product of their personality, which an AI is not capable of. The Federal Supreme Court confirmed this view in a court order dated 11 June 2024 (file number X ZB 5/22) but also stated that AI-generated inventions are generally patentable.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The contractor may be obliged to grant a back licence under the EU, federal or state level funding regulations on publicly funded research and development projects. In general, public grants contain ancillary provisions that must be fulfilled to avoid a possible revocation of the funding decision and the reimbursement of the grant. In addition to exercise and exploitation obligations, the funding conditions include obligations to grant access and utilisation rights in favour of the funding agency, as well as the subcontractors. The Subsidiary Conditions for Grants from the German Federal Ministry of Research and Education (*Bundesministerium für Bildung und Forschung*) for Research and Development Projects (NKBF 2017), for example, require that the results be made available to research and teaching in Germany and in the EU free of charge.

In addition, inventions that are the result of publicly financed research and development or innovation activities are subject to the EU regulatory framework for state aids according to Articles 107 and 108 of the Treaty on the Functioning of the European Union and the corresponding EU Commission Communication on State Aid rules for research, development and innovation (2022 RDI Framework). Under these rules, any transfer of funded inventions to commercial undertakings must be remunerated at market price.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

According to the case law of the Federal Supreme Court, AI-generated inventions are generally patentable, but AI devices cannot be named as an inventor (*cf.* Federal Supreme Court, order dated 11 June 2024, file number X ZB 5/22). The Federal Supreme Court is of the opinion that currently no systems exist that can make inventions without any human influence. Therefore, it is always possible to deduce a human being as the inventor, even if an invention was developed by an AI device.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Collaborations in the digital health sector typically require comprehensive contractual frameworks. These agreements must carefully balance the allocation of intellectual property and commercialisation rights with the delineation of regulatory responsibilities and product liability.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

When entering agreements with healthcare companies or HCPs, non-healthcare companies should refrain from providing any benefits, whether unilaterally (e.g., gifts) or as part of bilateral or multilateral cooperation agreements. Such agreements must ensure that services and consideration are equivalent, with remuneration reflecting arm's-length terms, in accordance with the principle of equivalence.

Any benefits provided must not create the impression of commercial expectations or incentives influencing procurement or therapy decisions. Benefits should serve legitimate, objective purposes and remain entirely separate from other business or commercial interests, adhering to the principle of separation.

All details of cooperation with healthcare companies or HCPs should be documented in clear, written agreements, ensuring maximum transparency. Verbal agreements or other non-transparent arrangements should be avoided, as they risk creating an impression of secrecy, in line with the principles of transparency and documentation.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

When dealing with federated healthcare data-sharing agreements, companies must address data protection requirements, as processing personal data for algorithm training requires a legal basis under the GDPR. For healthcare or patient data, explicit consent is typically required for such processing activities. Additionally, parties must assess whether the algorithm's training results still qualify as personal data or can be deemed anonymised, allowing for unrestricted sharing.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

The use of generative AI is governed by the AI Act, which also applies to providers and deployers of AI systems established outside the EU, insofar as the AI system's output is used within the EU. Providers of generative AI in digital health solutions must ensure compliance with the phased implementation of the legal framework, including proper employee training in AI literacy, the prohibition of certain AI practices, completion of necessary conformity assessments, adherence to transparency

requirements and the establishment of a compliant intellectual property strategy.

Moreover, given the absence of consistent case law on the ownership of AI-generated results, contracts should explicitly define ownership rights. Parties must also carefully address data protection considerations when integrating generative AI into digital health solutions.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

The primary regulatory authority for AI in the EU is the AI Office, established by the European Commission to oversee the implementation, monitoring and supervision of general-purpose AI and to promote AI governance.

In Germany, the oversight of other AI systems, particularly high-risk AI systems, is expected to fall under the responsibility of the *Bundesnetzagentur* (Federal Network Agency). The agency is anticipated to play a pivotal role, not only in regulatory supervision but also in fostering innovation within the AI sector. As of July 2025, a dedicated AI Service Desk has been established within the *Bundesnetzagentur*, providing practical guidance on the new EU AI Act requirements to companies (including SMEs and startups).

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

The core regulatory framework for AI/ML in the EU is the AI Act, which applies directly across all EU Member States.

On 9 September 2024, the European Medicines Agency issued a Reflection Paper on the Use of AI in the Medicinal Product Lifecycle, which outlines specific requirements for companies leveraging AI in this sector. Additionally, on 10 September 2024, the first formal meeting of the AI Board, established with the AI Act's entry into force on 1 August 2024, took place.

One of the AI Board's priorities in Phase 1 (2024) was addressing the interplay between the AI Act and the MDR and IVDR, with a strong focus on harmonising these regulatory frameworks for AI applications in healthcare.

Germany's draft implementing legislation, currently as of September 2025 still pending approval by both the *Bundestag* and the *Bundesrat*, is intended to designate the competent national authorities and to establish the procedural rules required to administer the AI Act's penalty regime.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

As a general principle, intellectual property rights can only be created and owned by humans, not machines. Therefore, improvements made by AI/ML without active human involvement typically do not qualify for protection under most intellectual property regimes.

In certain instances, the results may be eligible for protection under *sui generis* database rights, which safeguard substantial investments in data collection or management rather than intellectual creativity.

Additionally, such improvements might be safeguarded as trade secrets, provided they meet the legal criteria of being confidential, commercially valuable and subject to reasonable measures to maintain secrecy by the entity responsible for their creation.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Training data is often protected under *sui generis* database rights, as established in Sections 87a *et seq.* of the Act on Copyright and Related Rights (*Urheberrechtsgesetz*), implementing Directive (EC) 96/9, and can be licensed like other intellectual property. However, licensing personal health data is challenging due to GDPR protections, typically requiring anonymisation and robust safeguards against re-identification through technical and contractual measures.

A key consideration is ownership and access to the trained algorithm, which may not be protected by intellectual property rights. Contracts must clearly define each party's rights and obligations regarding its use. Liability and indemnification provisions are essential to address potential GDPR violations, such as invalid patient consent or improper anonymisation.

When licensing healthcare data, compliance with AI Act standards is critical. Data used for training, validation and testing must be pre-assessed for availability, quality, quantity, relevance, representativeness, accuracy and completeness to ensure the AI system operates correctly and safely.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

The AI Act does not establish a separate concept for differentiating standard AI from generative AI, but instead adopts a risk-based approach. Obligations vary according to the risk level of the AI application: lower-risk AI systems face minimal requirements; while high-risk systems, which may include certain generative AI applications, must implement a risk management system, conduct conformity assessments and maintain detailed technical documentation.

Generative AI systems are specifically subject to transparency requirements under the AI Act, particularly regarding the disclosure of AI-generated content.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Germany does not have specific laws governing generative AI technologies. Regulatory issues related to generative AI are primarily addressed at the EU level under the AI Act, which imposes transparency obligations specific to generative AI systems.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Germany does not have explicit data disgorgement laws, but unauthorised data use can lead to court-ordered deletion or cessation of processing under GDPR, intellectual property law and trade secret law. Processing without appropriate data rights is unlawful and may result in fines, liability or injunctions.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Besides regulatory responsibility and potential criminal charges, civil law liability plays a significant role in digital health markets. Under German law, there is contractual liability on the one hand, and tort liability under the Civil Code (*Bürgerliches Gesetzbuch*), as well as product liability under the Product Liability Act (*Produkthaftungsgesetz* – "ProdHaftG") that each cannot be restricted by a contract on the other hand. MDSW is subject to liability under the ProdHaftG, even if not offered in a material object as data carrier. The EU AI Act (effective from 2 August 2026), the EU Directive on AI liability (currently in draft form; the timing remains uncertain), the new General Product Safety Regulation (applying since 13 December 2024) and the new EU Directive on liability for defective products of 23 October 2024 (to be transposed by 9 December 2026) are or will soon become relevant, in particular with regard to the use of generative AI in the provisioning of digital health solutions.

9.2 What cross-border considerations are there?

Liability rules are primarily governed by Member State law. In cross-border matters, the Regulation (EU) 593/2008 ("Rome I Regulation") and the Regulation (EU) 864/2007 ("Rome II Regulation") determine the applicable national legislation. Under Article 4 of the Rome II Regulation, the law of the place where the damage occurs applies, regardless of where the harmful act took place. Exceptions include cases where (i) both parties reside in the same country, making that country's law applicable, or (ii) the tort is more closely connected to another country, in which case the law of that country applies.

For product liability, Article 5 of the Rome II Regulation may make the location where the product was acquired decisive. The Rome I Regulation allows parties, under certain conditions, to contractually agree on the applicable law. In the absence of such an agreement, the law of the service provider's residence generally applies to services, except in consumer contracts, where the law of the consumer's residence usually governs.

Cross-border liability cases carry significant legal and reputational risks. Digital health companies operating across borders should implement a global compliance regime and establish robust structures to address the specific legal requirements of each jurisdiction.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Risks posed by using generative AI can be mitigated by implementing, monitoring and enforcing adequate policies. Potential legal pitfalls and risks include, *inter alia*: the infringement of copyrights and other intellectual property; data security and privacy; confidentiality; contractual obligations; product liability; and AI- and sector-specific regulation. The use cases of generative AI should be carefully evaluated. One important question in this context is whether sufficient licences are in place. The use of dedicated AI models should be considered. It must be identified whether the use includes personal (or health) data.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Currently, there is no specific theory or concept of liability that would apply to misuse of healthcare data included in trained AI/ML models; therefore, the general theories and standards of liability apply.

According to the standard concept of liability, the user is always liable for the content/results generated by AI/ML models. This means the company or individual person that uses AI/ML model-generated contents/results in its own name or adopts the results of an AI/ML model as its own – be it as content on a website, in products or in documents – is liable.

AI/ML models themselves are not liable because they lack the necessary legal personality. The manufacturer of AI/ML models can only be held liable if, for example, the AI/ML model does not have the contractually warranted characteristics or if the manufacturer has not taken sufficient safety precautions within the AI/ML model, resulting in damage.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Healthcare organisations that transfer IT operations to Cloud-based services are facing, *inter alia*, technical and legal challenges. Security and confidentiality are key aspects for a wide-scale offering and use of Cloud-based services. To reduce the risk of cyber-attacks and the loss of personal data, healthcare organisations must ensure a safe system to transfer, maintain and receive health information. Confidentiality can be achieved by access control and by using encryption techniques. Healthcare data may be exchanged only in pseudonymised or even anonymised form. In certain legal regimes, it may be obligatory that Cloud-based services are carried out in Germany or the EU at the very least.

In Germany, the legislator enacted the Health IT Interoperability Governance Ordinance (*Gesundheits- IT -Interoperabilitäts-Governance-Verordnung*) to ensure the secure and fast Cloud-based transfer of patient data.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

As shown above, digital health products and services are

strictly regulated and under a high level of surveillance. To offer such products and services on the market, companies must establish a comprehensive compliance organisation, including to meet the various regulatory, data protection and healthcare compliance requirements.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

There are restrictions to corporate ownership of certain healthcare service providers. While there are no ownership restrictions for hospitals, such restrictions exist in the outpatient health services sector with regard to physician practices and medical care centres (*Medizinische Versorgungszentren* – "MVZ"). As hospitals are entitled to hold MVZ, investors usually choose hospitals as their preferred vehicle to indirectly operate MVZ and thereby employ physicians. A hospital reform has been launched in 2024 and may result in certain hospitals not qualifying as vehicles for MVZ anymore. However, the law is subject to ongoing modifications. Moreover, the coalition agreement for the new German government includes a statement that indicates that the new government shall adopt a law to regulate investor-operated MVZ in order to ensure transparency regarding the ownership structure and the proper use of health insurance funds. In fall 2025, the Alliance 90/The Greens parliamentary group in the *Bundestag* presented specific changes in a motion (21/1667): they call for easier establishment of municipal MVZ and mandatory registration of all MVZ with details of the operator and beneficial owner. In a parliamentary hearing in November 2025, experts and stakeholders clearly diverged – with the support of the German Medical Association for clear rules and transparency, while other voices saw a problem with blanket interventions in medical independence.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barriers include stringent market entry, reimbursement, and compliance requirements. The entry of MDSW is significantly restricted by certification procedures under the MDR and IVDR, which often necessitate the involvement of notified bodies. These challenges are expected to intensify with the AI Act, which introduces specific conformity assessment procedures for AI MDSW classified as Class IIa or higher. On the reimbursement side, while it may be difficult and time-consuming to convince SHI funds of new and innovative digital health products or services, recent legal developments have facilitated reimbursement, e.g., in the area of medical app prescriptions. Still, companies entering the German digital health markets must observe a number of regulations, including with respect to the processing and use of health data and cooperation with healthcare companies or HCPs. In clinics, many healthcare services are still reserved to the physician by statutory laws and, hence, not or only partly replaceable by digital health solutions. Since the adoption of the *Digital-Gesetz* and related reforms, the landscape for digital health in Germany has evolved: the nationwide rollout of the ePA and mandatory e-prescriptions are underway, potentially facilitating integration of digital health solutions into standard care. While this also raises new interoperability, data security and compliance challenges, it will certainly enhance adoption of digital health solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Germany, all practising physicians are supervised by their respective State Physicians' Chamber (*Landesärztekammer*) competent at the federal state level. The German Physicians' Chamber (*Bundesärztekammer*), serving as the joint association of all State Physicians' Chambers, actively participates in legislative procedures by representing physicians' interests and issuing public statements on legislative drafts and proposals. The Panel Doctors' Associations (*Kassenärztliche Vereinigungen*) supervise doctors that are entitled to provide healthcare services reimbursed under the SHI regime. Medical societies (*Fachgesellschaften*) issue guidelines that determine whether a treatment is considered state of the art.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

In Germany, medical apps have recently become subject to a general reimbursement scheme (see question 1.2 above).

Besides that, reimbursement depends on the legal status of the respective digital health product or service. Medical devices may be reimbursable as medical aids (*Hilfsmittel*) or – in certain cases after testing periods – as new treatment methods. Digital healthcare services provided by physicians are reimbursed in the same manner as traditional physician services: their reimbursement in the outpatient sector in the SHI is subject to the Uniform Assessment Measure, (*Einheitlicher Bewertungsmaßstab* – "EBM"). New digital health products or services must be listed in the EBM in order to obtain reimbursement. Where such listing takes too long, companies still have the option to enter into reimbursement negotiations with individual SHI funds.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

The primary due diligence challenges in evaluating digital health solutions in Germany include navigating complex regulatory frameworks, ensuring robust data protection and privacy measures, and achieving seamless interoperability with existing healthcare systems. Addressing these challenges necessitates a multidisciplinary approach, engaging legal, technical, and clinical expertise to ensure comprehensive evaluation and compliance within Germany's healthcare ecosystem.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The Health Data Use Act (*Gesetz zur verbesserten Nutzung von Gesundheitsdaten*) was issued in 2024 and creates a framework to unlock existing health data for research and innovation: it enables access to SHI data for "public-interest" research while retaining decentralised data storage. It establishes a

central data access and coordination office under the BfArM to mediate data requests, maintain a metadata catalogue, support applications, and ensure data protection and pseudonymisation. It aims to improve healthcare quality, foster medical research and innovation, and support evidence-based planning and evaluation in the health system.

Since its introduction, e-prescriptions have been widely used: by October 2025, over a billion digital prescriptions had been filled. In future, the concept of e-prescription shall be extended to other healthcare products and services, such as physical therapy, medical aids or home care.



Jana Grieb, Partner, based in Frankfurt, has been advising pharmaceutical and medical technology companies on all aspects of health law for over 20 years. She accompanies pharmaceuticals, medical devices and *in vitro* diagnostics throughout their entire life cycle – from research and development to market access, advertising and distribution. One main area of her work is providing legal and strategic advice on market entry and reimbursement paths in the EU, with a particular focus on the EU regulations on medical devices and *in vitro* diagnostics and the law governing statutory health insurance in Germany.

McDermott Will & Schulte
Oberlindau 54 – 56, 60323 Frankfurt a. M.
Germany

Tel: +49 69 951145 252
Email: jgrieb@mwe.com
LinkedIn: www.linkedin.com/in/jana-grieb-58b33a135



Steffen Woitz, Partner, based in Munich, focuses his practice on litigation, intellectual property, antitrust and competition law and alternative dispute resolution. Steffen has in-depth litigation experience in all major German courts and assists clients in cross-border disputes and transactions. He represents German and international clients in patent infringement and other contentious matters relating to trademarks, unfair competition and antitrust law.

McDermott Will & Schulte
Nymphenburger Str. 3, 80335 Munich
Germany

Tel: +49 89 12712 181
Email: swoitz@mwe.com
LinkedIn: www.linkedin.com/in/steffen-woitz-b316092b6



Dr. Claus Färber, Counsel, based in Munich, represents clients in all legal matters related to the telecommunications, media and information technology (IT) industries and has extensive experience advising international clients across industries on European data protection matters. Claus drafts and negotiates software licence agreements, other IT contracts, business process outsourcing agreements and significant procurement agreements in the telecommunications, e-commerce and IT industry, and assists with significant litigation in these industries. His transactional experience includes major cooperation and framework agreements, such as Internet access in aircraft, WiFi hotspots, roaming, Cloud platforms and machine-to-machine (M2M) communications.

McDermott Will & Schulte
Nymphenburger Str. 3, 80335 Munich
Germany

Tel: +49 89 12712 151
Email: cfaerber@mwe.com
LinkedIn: www.linkedin.com/in/cfaerber



Dr. Christian Lebrecht, Counsel, based in Frankfurt, advises businesses in the life sciences sector. He focuses on medical devices, *in vitro* diagnostics and digital health solutions, guiding clients through complex, industry-specific challenges. Christian develops tailored legal strategies for market entry, distribution and commercialisation, ensuring regulatory compliance and strengthening competitive advantage. He regularly provides support to clients in product liability matters and interim injunction proceedings, especially in areas of unfair competition and medical advertising law.

McDermott Will & Schulte
Oberlindau 54–56, 60323 Frankfurt a. M.
Germany

Tel: +49 69 951145 011
Email: clebrecht@mwe.com
LinkedIn: www.linkedin.com/in/christian-lebrecht

McDermott Will & Emery is an international full-service law firm with a particular focus on Health and Life Sciences. We advise our clients on legal and regulatory challenges in an increasingly growing digital health market and provide tailor-made solutions for the successful market entry of new digital health products and services. With more than 20 locations on two continents, our team works seamlessly across practices, industries and geographies to deliver highly effective and extraordinary legal and strategic advice. More than 1,750 lawyers strong, we bring our personal passion and legal prowess to bear in every matter for our clients and the people they serve. Looking to the future, we will continue to expand geographically and enhance our existing practices and industry-focused strengths. We are committed to building from these strengths in order to best serve our clients and our communities.

www.mwe.com

McDermott Will & Schulte

Israel


Adv. Eran Bareket


Adv. Alexandra Cohen

Gilat, Bareket & Co., Reinhold Cohn Group

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no general definition of "digital health" in Israel. However, the definition can be derived from the government's "National Digital Health Plan as a Growth Engine" approved on 25 March 2018, which defines digital health as follows: "*The vision of the digital health strategy as published by the Ministry of Health is to enable a leap in the healthcare system so that it will be a sustainable, advanced, innovative, renewable and constantly improving health system, by leveraging the best available information and communication technologies.*"

In the framework of a Supervisory Report on the digital health sector issued by the Privacy Protection Authority ("PPA") in 2024, the term "digital health" was defined as referring to the integration of technology into healthcare services to improve the delivery of medical services, diagnosis, treatment and monitoring of patients' health conditions.

Although there is no legal definition, the digital health sector is very developed in Israel and there are hundreds of innovative companies – including start-ups – dealing with digital health and developing technologies in different digital health sectors. The Ministry of Health ("MOH") established a division dealing with digital health, which is aimed at implementing innovative technologies and improving the quality of treatment, medical services and economic efficiency. Collaborating with governmental partners, the division is engaged in crafting a robust digital health ecosystem. This ecosystem is designed to foster synergies among health organisations, industry stakeholders and academia, fostering innovation and advancement in the realm of healthcare.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging technologies in digital health in Israel include digital tools and platforms that enable consumers to proactively track, manage and treat their own medical conditions, as well as digital tools of remote monitoring, decision support, clinical workflow, diagnostics, patent engagement and assistive devices.

For example, ContinUse Biometrics Ltd. is an Israeli company that developed methods using artificial intelligence ("AI") techniques for nano-level detection and analysis of vibrations associated with the movement of internal organs and molecules. This technology enables the continuous measurement of vital signs and other bio-parameters (such as heart and respiration rates and blood pressure) from a distance and with high accuracy.

1.3 What is the digital health market size for your jurisdiction?

According to the Startup Nation Central Finder Annual Report for 2024, Israel's health tech and life sciences sector accounts for about 27% of the ecosystem, with close to 1,600 companies – making it the largest sector in the Israeli ecosystem by company count.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Private companies are not required to publish their financial results; therefore, there is no detailed information regarding the revenue of private digital health companies in Israel. However, based on the *Calcalist* article "*Full list of Israeli high-tech funding rounds in 2025*", several Israeli healthcare companies secured significant funding rounds in 2025, underscoring the sector's resilience and innovation. Notable examples include:

1. **Eleos**: In January 2025, Eleos raised $60 million to disrupt behavioural healthcare through AI tools.
2. **Navina**: In March 2025, Navina secured $55 million. The startup seeks to redefine clinical workflows and improve patient outcomes.
3. **Healthsee**: In April 2025, Healthsee raised $50 million to automate the complexity of U.S. health benefits.
4. **Hyro**: In October 2025, Hyro secured $45 million. The startup seeks to alleviate staffing shortages and expand patient access by deploying AI agents across hospitals and health systems nationwide.
5. **Popai Health**: In November 2025, Popai Health raised $11 million. The startup aims to turn patient phone calls into actionable data.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

As mentioned above, private companies are not required to publish their financial results; therefore, there is no detailed information regarding the revenue of private digital health companies in Israel.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The principal regulatory authorities enforcing regulatory schemes related to digital health in Israel are:

- The MOH – responsible for registration and marketing approvals, regulates the approval of clinical trials and regulates secondary use of health data. In addition, uses of health data and collaborations involving health data are also regulated and monitored by the MOH.
- The PPA – regulates maintenance of databases containing personal data (including health data) and enforces privacy requirements for the use of such data. The privacy protection commissioner has enforcement authority in cases of unauthorised use of data. In 2024, the PPA released a Supervisory Report on the digital health sector, evaluating entities providing digital health services across three main criteria: organisational control and corporate governance; data repository management; and data security. The report found that most entities demonstrated a high level of compliance in these areas.
- The courts have jurisdiction over all issues.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

In Israel, the core healthcare regulatory schemes related to digital health include:

- Healthcare and patient rights: National Health Insurance Law (1995); Patients' Rights Law (1996); and the Public Health Ordinance, 1940.
- Medical devices and technology: Medical Devices Law (2012); and the MOH Director General circulars.
- Privacy and data security: Protection of Privacy Law (1981); and Data Security Regulations (2017).

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Since the field is new and not comprehensively governed by Israeli legislation, it is still unclear how enforcement of legislation governing the digital health industry will evolve.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Software medical accessories and devices ("MADs") are registered by the MOH as medical accessories, e.g., CoroFlow Cardiovascular Measurement System & Accessories (software that assists in measuring flow changes in coronary arteries), as well as Insulin Insights (measurement software for diabetes patients). Other medical devices were once registered as software MADs, such as 3D medical image processing, simulation and design software or Neurosurgical Navigation Software.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In Israel, there is no specific regulation dedicated exclusively to AI/Machine Learning ("ML")-powered digital health devices or software solutions. However, such devices are generally regulated under existing medical device laws and standards, such as the Medical Devices Law, 2012, overseen by the MOH Medical Devices Division.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

The MOH is adapting its regulatory framework to address the dynamic nature of AI/ML-based digital health solutions through several key initiatives:

- Guiding Principles for AI-Based Technologies: During 2023, the MOH published guidelines aimed to establish good ML practices for digital medical technologies (see here: https://www.gov.il/en/pages/digital-medical-technology-gmlp-1).
- Alignment with International Standards: The MOH is aligning its regulations with evolving international standards, such as those from the European Union, to ensure that Israel's regulatory framework remains current and effective. For example, the Health Information and Cyber Security Division of the MOH published a document on 30 April 2022, requiring healthcare organisations in Israel to comply with ISO 27001 and ISO 27799 standards for information security as a condition for obtaining and maintaining a licence from the MOH.
- Support for Innovation in Digital Health: Through programmes like the Support Program for Innovation in Selected Fields – Digital Health, operated jointly by the Innovation Authority, the MOH and the Headquarters for the National Digital Israel Initiative, the MOH supports Research and Development ("R&D") and pilot projects in digital health, fostering an environment conducive to the development and implementation of AI/ML solutions.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data plays a critical role in regulatory approval for AI/ML-based digital health solutions in Israel. Products must demonstrate efficacy and safety through robust clinical studies to meet the requirements of the Medical Devices Division of the MOH.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Israel, digital health products are regulated centrally by the MOH, with no differential regulation at state or regional levels.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

In recent years, Israel has started addressing digital health specifically in official publications. For example, the PPA issued guidelines to ensure telehealth services comply with privacy and data protection laws, safeguarding patient information during remote consultations. In addition, the PPA published during 2025 a guidance clarifying the application of Israel's Privacy Protection Law to AI systems throughout their entire lifecycle, from model training to deployment. The guidance emphasises lawful bases for processing, informed consent and transparency, limits on data scraping, enhanced accountability (including Data Protection Officer appointment and privacy impact assessments), and the applicability of data subject rights, signalling closer regulatory scrutiny of high-risk AI uses.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  It is to be noted that the MOH has not yet published any comprehensive, binding guidance regarding the technologies below, which continues to create a degree of regulatory uncertainty for the entities active in the digital health field:
  - Regulation, ethics and jurisdiction of medical practice – the issue arises when practitioners are outside the country's jurisdiction.
  - Liability of misdiagnosis – the risk of misdiagnosis increases when medical services are provided without doctor supervision.
  - Health data privacy – collection, use and security standards for health data.
  - Software and hardware validation.

  The TytoCare, a remote examination kit and telehealth platform, is an example of an Israeli telemedicine technology – it enables remote clinical examinations (heart, lungs, skin, throat, ears) using connected hardware guided by mobile devices.
- **Robotics**
  Robotic technologies are considered as emerging technologies in the field of medicine, generally used for performing human surgical/medical operations. The incorporation of new technologies, such as AI or Internet connections in robotics, enhance the performance and flexibility of this technology, while also raising additional issues relating to cybersecurity, software updates and system reliability.
  In Israel, the company Yaskawa developed medical rehabilitation robots, which help maintain the body's quality of movement and function, rehabilitate from injuries, wounds and traumatic events and maintain daily functioning.
  XACT Robotics also developed a robot designed to perform a variety of invasive medical operations such as biopsy, ablation (catheter insertion), drainage and medication in specific areas of the body.
  Another example is of the ReWalk Robotics company that develops robotic exoskeletons that allow individuals with spinal cord injury to stand and walk, bridging mobility rehabilitation technologies with medical robotics.
- **Wearables**
  Unlike other devices, wearable devices are always close to the user and thus have additional data collection capabilities (walking and pulse rate, for example). Furthermore, most wearable devices are also capable of operating without the Internet and thus the scope of data collection is greater, as is the concern of leaking sensitive information. Examples of wearable devices developed in Israel are:
  - Orcam – a wearable assistive AI device for the blind and visually impaired, that instantly reads text, recognises faces, identifies products and much more.
  - Hip-Hope of Hip-Hope Technologies – a smart wearable device, designed as a belt, worn around the user's waist. A proprietary multi-sensor system detects impending collision with the ground. Upon detection, two large-size airbags instantly inflate and protect the wearer's hips. Fall alert notifications are automatically sent to pre-defined destinations.
- **Virtual Assistants (e.g. Alexa)**
  Since virtual assistants collect a broad spectrum of data about their users, they get a more complete, accurate and in-depth picture of the user. In view of this, the data is extremely sensitive, and any leakage may jeopardise the user's privacy, as is the case with wearables. Similar privacy, consent and data-minimisation considerations therefore apply as with wearables.
- **Mobile Apps**
  Mobile apps are quite similar to wearables and virtual assistants and therefore raise similar issues. Moreover, mobile phone apps can incorporate additional hardware features (such as fingerprint, voice recognition or various sensors) that are integrated into the mobile device.
- **Software as a Medical Device**
  This technology raises at least two main questions:
  1. Can medical device software provide medical treatment? When does provision of medical information constitute medical treatment?
  2. When is medical device software classified as a medical device, as defined in the Medical Equipment Law, 5772-2012, thereby requiring to be MAD-registered?

  In this context, digital medical technologies are defined by the MOH as software-based technological applications intended for medical purposes, including health applications, communication tools, decision-support software, diagnostic and therapeutic tools, sensors and AI-based systems, and are the subject of ongoing regulatory development by the MOH's relevant divisions.
- **Clinical Decision Support Software**
  Clinical decision support systems are currently being developed by various start-ups in Israel. At the time of writing, there is no comprehensive, binding regulatory framework specifically governing the implementation of such systems. Key issues include the need to build physician trust in the reliability of such systems while preventing over-reliance on automated recommendations, particularly where AI-based tools increasingly approach autonomous decision-making. Recent discussions in the Knesset Health Committee highlight concerns regarding the risk of medical errors, lack of explainability, and insufficient clinical context in AI-based recommendations, as well as the importance of maintaining human oversight and transparency,

including disclosure to patients when AI tools are used in clinical decision-making. In response, the MOH has been asked to develop professional guidelines and ethical principles governing the use of AI-based decision-support tools by medical staff.

- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  While systems that specialise in a particular field may support human judgment or serve as a basis for analysing a specific patient's case and determining a physician's findings, there are specialist systems that completely replace human judgment, namely, to simulate professionals' behaviour, by using ML. The K system, for example, is a personalised medical information search app designed to replace medical information Internet searches that are not individually customised. The system provides relevant information according to the case, while mentioning that such information is not a diagnosis or medical advice, and that medical attention should be sought if the symptoms are severe.
  In Israel, Sight Diagnostics, an AI-driven blood diagnostics platform, uses proprietary machine vision and AI to perform point-of-care blood analysis, transforming traditional lab diagnostics.
- **IoT (Internet of Things) and Connected Devices**
  Please see "Wearables".
- **3D Printing/Bioprinting**
  The 3D printing field is a flourishing industry in Israel, used, *inter alia*, for the manufacture of hearing and surgical aids, dental models and physical models of organs, as well as living cellular products and tissues, some of which are medically approved for human contact and transplantation.
  It is estimated that Israel is the manufacturer of approximately 40 per cent of all 3D printers worldwide, and more than 1,400 Israeli companies dedicated to life sciences. For example, the company Synergy3DMed designs and prints customised 3D models and surgical instruments. Recently, Tel Aviv University researchers used a 3D bio-printer to create a heart that includes real cells, blood vessels, ventricles and chambers. Another example is the collaboration between Israel's CollPlant Biotechnologies and the US-based United Therapeutics Corporation to begin the production of 3D-printed kidneys.
  While this technology significantly contributes to the development of healthcare, *inter alia*, by reducing global organ shortages, the different reactions of individuals to 3D-printed organ transplantations may raise an issue as to the efficiency of such organs.
- **Digital Therapeutics**
  The digital therapeutics sector, which includes software-driven medical interventions that provide validated, evidence-based treatments for a range of physical and mental health conditions, constitutes a significant portion of Israel's digital health industry. For example, Theranica, which specialises in wearable devices for migraine relief, integrating neuromodulation and smartphone technology, developed Nerivio, a remote electrical neuromodulation wearable for migraine treatment and prevention.
- **Digital Diagnostics**
  Digital diagnostics constitute part of the outputs arising from using digital technologies. The data used by digital diagnostics is collected from various sources, such as the user's electronic health records, medical imaging and real-time patient-generated data from wearables, requiring interoperability standards. It is essential to ensure that digital diagnostic tools can seamlessly integrate with existing healthcare systems and technologies. EFA Technologies developed the RevDx, a mobile end-point solution for performing automatic microscopy tests, including whole blood sampling and an automatic diagnosis of blood count. Ibex developed Galen, a clinical-grade, multi-tissue platform that helps pathologists detect and grade breast, prostate and gastric cancer, along with more than 100 other clinically relevant features. Ibex's Galen platform also uses AI to analyse pathology images for cancer detection and grading, aiding diagnostic decisions.
- **Electronic Medical Record Management Solutions**
  The large access to electronic medical records based the need for digital systems designed to store, manage and retrieve user health data in order to provide the user with a comprehensive view of his data. Legal considerations arise in terms of the ownership of electronic medical records and the provision of access to third parties, demanding scrutiny and resolution. InvenTech developed HSM, a cloud-based clinic management system.
- **Big Data Analytics**
  Big data analytics is integrated into digital technologies through a large variety of means such as predictive analytics or clinical decision support systems (for example, the K system mentioned above) and constitutes an important part of the digital healthcare field.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain-based healthcare data sharing solutions allow exchange of data among healthcare providers, insurers, researchers and other stakeholders, leading to more efficient and timely healthcare services. For example, Brya developed a platform allowing hospitals, clinics and health systems to seamlessly and safely access and exchange data with researchers and life sciences.
- **Natural Language Processing**
  Natural language processing may be used as part of ML activities applied to electronic health records, whether text or audio. Usage of this technology is not regulated or standardised in Israel, and there are no provisions regarding its application in digital healthcare.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Among the various goals defined in the government's "National Digital Health Plan as a Growth Engine" is the goal to create a national digital platform for the purpose of sharing health data. However, this goal has not yet come to fruition. One of the issues in this regard is the data holders' willingness to share their data to the national central database and to agree to revenue-sharing arrangements that will allow research on data originating from multiple sources.

- Problems of uniformity and standardisation also arise, since different bodies collect the data and classify the types of data stored in their databases in different ways.
- Privacy protection of the data shared through the digital platform, including its security, is also a key issue.
- Obligation to present medical data to the patient (in accordance with the provisions of the Director-General ("GD") circular on patient access to personal health data, "*Healthcare under your Control*").

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The main legal and regulatory issues that must be taken into account at the time of using personal data are: ownership of data; scope and nature of the independent use and sharing of the data (including compliance with GD circulars regarding secondary uses of and collaborations based on health data and with the Medical Information Mobilization Law, 5784-2024, when sharing personal data between various health organisations); and privacy protection of the data (including compliance with the Protection of Privacy Law, 5741-1981). See further below.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Israel, personal health data is regulated through the Privacy Protection Law, 1981, with no differential regulation at state or regional levels.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

Health Maintenance Organisations ("HMOs"), the entities holding most of the health data in Israel, are subject to strict regulation. For example, HMOs are limited in holding equity in start-ups and cannot invest the money generated by using health data other than for the advancement of treatment, medical service, public health or scientific research in the health field. Privacy regulations apply always, regardless of the nature of the entities.

4.4 How do the regulations define the scope of personal health data use?

Circular provisions prohibit the use of health data for purposes that do not serve the advancement of treatment, medical service, public health or scientific research in the health field. Health data should also not be used for inappropriate social purposes, with an emphasis on discrimination in insurance or employment.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The main key contractual terms to consider are: ownership of data; ownership of know-how products based on collaborations through which data is used; consideration for data sharing or know-how products based on use of the data, such as ownership in the outside organisation (if a company is concerned); right to use the know-how products; monetary compensation (such as royalties, licence fees and exit fees); period of use of the data; exclusivity of the data's use; reach through royalties/licences; royalty rate and stacking; and the need to use other databases.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

According to the Protection of Privacy Law, 5741-1981, a person may request the owner of a database (or the possessor thereof as applicable) to amend or delete data about himself that is not correct, not complete, not clear or not up to date. If the owner of the database refuses to comply with such request, the person requesting the amendment or deletion of his data may appeal to the Magistrate's Court, as regulated under the Privacy Protection Regulations (Conditions for Reviewing Data and Rules of Procedure for Appealing Refusal of Review Requests), 5741-1981. In addition, the Privacy Protection Regulations (Instructions Regarding Information Transferred to Israel from the European Economic Area), 2023, includes a duty of data accuracy, according to which the database owner must implement a mechanism – organisational, technological or otherwise – to ensure that the information in the database is correct, complete, clear and up to date.

The circular regarding collaborations based on secondary uses of health data, published by the GD of the MOH in January 2018, prohibits the use of health data for improper social purposes, with emphasis on discrimination in insurance or employment. According to this circular, a collaboration agreement shall include a provision that allows the health organisation to cancel or suspend the agreement if the CEO of the MOH orders so due to a violation of one of the guidelines set forth in the circular, including the prohibition to use health data for discrimination purposes.

It is worth noting that the World Medical Association Declaration of Helsinki sets forth provisions aimed to protect the health and rights of the subjects participating in medical research. For example, the declaration states that medical research involving a disadvantaged or vulnerable population or community is only justified if the research is responsive to the health needs and priorities of this population or community and if there is a reasonable likelihood that this population or community stands to benefit from the results of the research.

In addition, ISO 27799:2016 provides guidelines for medical organisations in order to ensure that the level of security used maintains the integrity, confidentiality and availability of health data.

As to bias, there is no express regulation.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The laws determining standards for using and collecting personal health data include the following:

1. The Protection of Privacy Law, 5741-1981, establishes the legal basis for safeguarding personal data in Israel.
2. The Protection of Privacy Regulations (Data Security), 5777-2017, set organisational mechanisms to integrate data security into the management routines of all entities processing personal data.
3. MOH GD circulars, such as: the Secondary Use of Health Data Circular (17 January 2018), which regulates the use

of health data for non-medical purposes, ensuring that any secondary use is de-identified unless otherwise specified by law or approved through explicit opt-in consent; the Collaborations Based on Secondary Uses of Health Data Circular (17 January 2018), which provides guidelines for collaborations involving secondary health data use; and the Patient Access to Personal Health Data: "Healthcare Under Your Control" Circular (11 November 2019), which empowers patients by granting them access to their electronic health records, promoting transparency and patient engagement.

4. The Medical Information Mobilization Law, 5784-2024, enacts to facilitate the sharing of health data between health organisations; this law establishes standards for data interoperability and patient consent, ensuring that data exchange occurs securely and with respect for patient privacy.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The main legal and regulatory issues that must be taken into account at the time of sharing personal data are: ownership of data; scope and nature of the independent use and sharing of the data (including compliance with GD circulars regarding secondary uses of and collaborations based on health data and with the Medical Information Mobilization Law, 5784-2024, when sharing personal data between various health organisations); and privacy protection of the shared data (including compliance with the Protection of Privacy Law, 5741-1981).

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Israel, personal health data sharing is regulated uniformly at the national level, with no differential regulation at the state or regional levels.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

HMOs, the entities holding most of the health data in Israel, are subject to strict regulation. For example, HMOs are limited in holding equity in start-ups and cannot invest the money generated by using health data other than for the advancement of treatment, medical service, public health or scientific research in the health field. Privacy regulations always apply, regardless of the nature of the entities. If the personal health data is shared between health organisations, the Medical Information Mobilization Law, 5784-2024, applies.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

During 2024, the MOH published a new plan aimed at establishing the infrastructure for implementing Fast Healthcare Interoperability Resources ("FHIR") standard interoperability in the healthcare system, in accordance with the provisions of the Medical Information Mobilization Law, 5784-2024.

In addition, the MOH has implemented a range of cutting-edge systems and infrastructures to facilitate the seamless exchange of healthcare data and enhance health promotion in Israel. The key initiatives include:

- The Innovative Healthcare Data Sharing System, which is a pioneering system facilitating the exchange and transfer of healthcare data among HMOs and hospitals.
- The "Tamna" system (Research Infrastructure for Big Data), which is a national platform dedicated to conducting extensive big-data research on health data. Data shared with researchers is anonymised, ensuring it remains untraceable and cannot be cross-referenced with other data that may lead to subject re-identification.
- The "Psifas" system (mosaic), which is a national platform with the overarching goal of advancing health in Israel by establishing and overseeing a comprehensive data infrastructure and biological sample repository for personalised medicine research. This collaborative initiative, managed through inter-university cooperation, includes vital partners such as HMO Klalit Health Services and its medical centres (Rabin, Carmel, Soroka and the Valley), along with medical centres Sheba, Ichilov, Sha'are Zedek and Hadassah.

The GD circulars regarding secondary uses of and collaborations based on health data set standards should also be mentioned. For example, the GD circular on secondary uses of health data states that the medical data shared for secondary use will be de-identified and sets detailed conditions for privacy, medical confidentiality and data security. This circular prohibits use for improper social purposes, with emphasis on discrimination in insurance or employment.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

The key issues to consider with respect to federated models of healthcare data sharing include the following: ownership of the federated shared data; the consent of the data subjects to federate and share such data and the scope of access granted; the privacy and security of the data, the standardisation of data, its quality and integrity; the trust and transparency among the data providers and users; and the legal and ethical frameworks for data sharing across different contexts, collaboration and innovation among the data stakeholders.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

The Patents Law, 5727-1967, shapes the scope of patent protection for digital health technologies by defining the criteria for patentable inventions. According to the law, a patentable invention must be a product or process in any area of technology that is novel, involves an inventive step, and is capable of industrial application. However, the law specifically excludes certain types of inventions, such as processes for human medical treatment, though diagnostic and veterinary methods are not excluded.

Additionally, discoveries, scientific theories, mathematical formulas, game rules and computer software *per se* are not patentable, as clarified by case-law precedents. However, if an invention addresses a technological problem with a technological solution – whether the solution involves software or not – it may be deemed patentable.

There is no specific legislation tailored to digital health technologies in Israel. Each application in this field is evaluated based on its individual merits under the general framework of patent law.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protection is governed by the Copyright Law, 5768-2007. Copyright law protection may be particularly relevant to software and certain compilations of data, but there is no protection of databases *per se*.

As of 2018, icons, graphical user interfaces and screen presentations are not protected by copyright but rather by the Designs Law, 5777-2017. Non-registered designs are protected for three years, and registered designs are protected for up to 25 years. There is no specific legislation applicable to digital health technologies. Consequently, the scope of protection for such technologies depends on how their components align with the existing frameworks for software, data compilations and design protection.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secret protection is governed by the Commercial Torts Law, 5759-1999, which defines a trade secret as "*business information, of all kinds, which is not in the public domain, is not easily disclosed by others lawfully, and whose confidentiality affords its owners a business advantage over competitors, provided that reasonable steps are taken to protect its confidentiality*". This definition applies broadly, including digital health technologies. The law prohibits the misappropriation of trade secrets, which includes: (1) taking a trade secret without the owner's consent through improper means, or using the secret obtained this way; (2) using a trade secret without the owner's consent in breach of a contractual obligation or duty of trust; or (3) acquiring or using a trade secret knowing it was unlawfully obtained under (1) or (2). It should be noted that disclosure of a trade secret through reverse engineering will not, in itself, be regarded as improper.

Health data is a classic example of a trade secret due to its proprietary nature and potential to provide a competitive edge, but there is no specific legislation applicable to digital health technologies. This lack of specificity underscores the importance of implementing robust internal measures (e.g., access controls, encryption) to secure trade secrets in the digital health sector.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Israel is very active in this area and has been a world leader since the 1960s. All main academic institutions operate a tech transfer unit experienced in granting product-use licences and obtaining equity and/or royalties from commercialising products based on them.

Every academic institution has Intellectual Property ("IP") bylaws. Such bylaws bind the employees of the institution (including the researchers) by virtue of appropriate provisions in their employment agreements. Some institutions also require students to subject themselves to these bylaws. In general, academic institutions require ownership of any IP generated in the framework of the institution, and various provisions grant the inventors a certain share in the revenues of the academic institution's commercialisation company. It is common practice for the academic institutions that if the institution is not interested in patenting the technologies, then the inventors can own the IP in exchange for a revenue-sharing agreement with the academic institution.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Computer software is protected by copyright, and no specific reference is made to the software of a medical device. However, copyright protects a method of expression only; thus, protection over functionality requires patent protection. The limitations of copyright and the complexity of patenting software create challenges for comprehensive protection.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

This question was discussed in Israel in the framework of the examination of the patent applications nos 268604 and 268605, in which an AI machine (DABUS) was listed as an inventor. The Patents Registrar decided that an AI machine, claimed to have conceived the invention, lacks eligibility as an inventor, and thus cannot bestow patent ownership upon itself (Patents Registrar Decision regarding Patent Applications nos 268604 and 268605 of Applicant Dr. Stephen Thaler (15 March 2023)). The ruling is currently under appeal.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The Law for the Encouragement of Industrial Research and Development, 5744-1984, establishes the Israel Innovation Authority ("IIA") (formerly the Office of the Chief Scientist), which provides, *inter alia*, funding platforms to various entities such as: early-stage entrepreneurs with technological initiatives; mature companies developing new products or manufacturing processes; and academic groups seeking to commercialise their ideas and turn them into revenue-generating products/services.

The government, through the IIA, typically funds up to 50% of the costs of development projects, including IP protection. There is no need to return the funding, unless the research generates revenue, and then the funding is returned by way of royalties.

In addition, IP developed through funding of the IIA should be exploited in Israel and cannot be transferred to a foreign entity without receiving prior permission from the IIA. While the government does not directly own the IP, it exercises control over its commercialisation and transfer,

particularly regarding exploitation outside Israel. These restrictions aim to safeguard national interests and promote economic growth within the country.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Since there is no specific legislation or landmark decisions tailored to digital health, the generally applicable laws and case law establish the framework for protecting digital health innovations (see question 6.1 above).

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

In general, the following points should be addressed:

- The R&D phase: responsibilities of the parties; goals; deliverables; and regulatory approval process. Technical details of access to data (whether copies will be made, or the data remotely accessed) and anonymisation thereof.
- IP: ownership and licences to background and foreground IP; and responsibilities and duty to collaborate in the enforcement of foreground IP.
- Arrangements for revenue sharing of commercialisation of the collaboration results: royalty bases; rate; definition of net sales; dilution; stacking; term; milestone payments; audits; and the like.

More considerations include: exclusivity; term of the agreement; anonymisation of the data; implications of the duty to call back; and opt in *v.* opt out.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Agreements with public healthcare companies require special attention be given to the regulatory environment of the healthcare entity (e.g. an HMO).

- Public-regulated healthcare entities are limited in their ability to hold equity in non-healthcare companies.
- Public-regulated healthcare entities are restricted in their ability to accede to requests for non-compete/exclusivity arrangements.
- Healthcare organisations involved in the development of new technologies will typically consider implications on the operations, such as the duty to call back, the cost of adding a new technology to their basket of services, etc.
- In addition to access to data, healthcare organisations may serve as an alpha site for the development of new technologies.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

In addition to the points mentioned above (question 7.2), when dealing with federated learning healthcare data sharing agreements between companies, the following points should be addressed: ownership of the federated shared data; the consent of the data subjects to federate and share such data and the scope of access granted; the standardisation of the data; adherence to all pertinent healthcare regulations and the seamless integration of such compliance into operational frameworks; technical infrastructure compatibility for federated learning and agreement allowing future adaptability; and the liability scope of the parties.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

The considerations parties should take into account when dealing with the use of generative AI in the provisioning of digital health solutions include the following:

- IP – the content created by generative AI models may be similar or identical to existing contents protected by IP rights such as copyrights, trademarks and patents, raising questions of ownership and infringement. In light of the current case law in Israel, since an AI machine cannot be considered as inventor, the matter of ownership should be considered and addressed.
- Data privacy – since generative AI models use large amounts of data (including personal and sensitive data) to train and generate content, parties using generative AI must ensure compliance with all privacy protection laws and proper security measures in order to avoid any unauthorised access, misuse or theft.
- Content regulation – parties using generative AI must ensure that the contents generated by AI models are not harmful, misleading, offensive or illegal. In addition, the parties should ensure that the content they generate or distribute is accurate, authentic and ethical, including with regard to algorithmic bias and fairness.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is no specific regulatory authority dedicated to enforcing AI/ML-related regulatory schemes. The courts have jurisdiction over disputes or enforcement matters across all sectors.

For AI/ML products in digital health, regulatory oversight typically falls under the purview of health sector authorities and is addressed by applicable medical device or healthcare laws (see question 2.1 above).

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

See question 8.1 above.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Ownership of an enhanced AI/ML algorithm without human intervention may occur in respect of any of the following: the machine; the owner of the machine; the programmer of the code; the data scientist who created the algorithm; or the medical doctor who assisted in the characterisation of the algorithm.

Israeli law does not regulate the ownership of IP created by ML, and this should be regulated in collaboration agreements. However, it is generally accepted that the company conducting the research will have the rights to the resulting products, including their IP rights. It is important to note that in Israel, if the invention is a method in the field of healthcare (such as precision medicine), two problems arise: (1) a patent shall not be granted for a procedure for a therapeutic treatment on the human body (section 7 of the Patents Law); and (2) discovery, scientific theory, mathematical formula, game instructions and thought processes shall be considered abstract ideas or processes of a technical nature.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Some of the main commercial contractual and strategic considerations are:

- Restrictions on licensing: privacy laws may limit licensing rights, especially for sensitive data like healthcare records. De-identification is often required.
- Use and control of data: the permitted use should be defined and misuse prevented (e.g., unauthorised disclosure). Ownership of AI/ML outputs should be addressed.
- Remuneration models: fixed payment or revenue sharing of revenues received from exercising the licence; in the latter case, agreeing on the royalty base may sometimes be challenging.
- Data security and compliance: compliance with privacy laws should be ensured, particularly for healthcare data.
- Healthcare-specific considerations: in some cases, healthcare data should be anonymised.

In healthcare, stricter regulations and ethical implications require tailored agreements to address these challenges effectively.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

As of December 2025, Israel does not have specific regulations that distinguish between standard AI and generative AI technologies. The country's approach to AI regulation is characterised by a general framework that applies to all AI systems, without explicit differentiation between various types of AI technologies.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

The legal issues that are unique to generative AI technologies include the following: ownership (who is determined as the owner of AI-generated content – creators of the AI, the operators, the end-users that generate outputs?); copyright; privacy (generative AI models are often trained on large datasets, including personal data, which can conflict with privacy laws); ethical issues (generative AI can be used to create disinformation, harmful content and deepfakes); bias (generative AI systems can perpetuate or amplify biases present in training data). According to the Ministry of Justice's opinion from December 2022, except in exceptional cases, the use of copyrighted materials for the purpose of ML falls under fair use and therefore does not constitute a copyright infringement. However, the opinion does not make definitive determinations regarding the output of ML.

While Israel does not yet have generative AI-specific legislation, ongoing national initiatives and global collaborations aim to create a robust regulatory environment that balances innovation with ethical and legal responsibilities, such as:

- National AI strategy – In December 2023, Israel published its Policy on Artificial Intelligence Regulation and Ethics, underscoring a commitment to responsible innovation and addressing challenges associated with AI deployment across various sectors.
- In the healthcare sector, regulators are adopting practical, iterative approaches to AI oversight. For example, during 2025, the MOH and the Israel Innovation Authority issued a Call for Information inviting companies, startups, research institutions and healthcare organisations to share details about innovative AI solutions relevant to the healthcare system. The purpose of this call is to explore the need for and design of a regulated testing environment ("regulatory sandbox") where advanced AI technologies could be tested under supervision, with the aim of improving care quality, reducing wait times and managing associated risks.
- Global collaboration – Israel has engaged in international agreements on AI governance, such as signing the Council of Europe's AI Convention. This commitment aligns Israel's regulatory standards with global human rights and democratic values, ensuring that AI technologies, including generative AI, are developed and utilised responsibly.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In Israel, there are no specific laws or regulations directly addressing trained AI/ML models that include data for which the developer lacks appropriate rights. In such case, this issue would likely be governed under general property or IP (if proprietary or copyrighted data is used without authorisation), contract (if developers violate contractual obligations) and privacy laws (if personal data is used without proper consent).

Israel does not currently have explicit data disgorgement laws requiring the removal or destruction of AI/ML models built on improperly acquired data. However, courts have the

authority to issue remedies in legal disputes, such as orders to cease the use or distribution of such models, delete improperly acquired data or provide financial compensation. Additionally, under the Unjust Enrichment Law, 5739–1979, if a party gains a benefit or service without legal entitlement, they may be obligated to make restitution of the benefits or its value, which could apply in cases involving improperly used data.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

There is no specific legislation on digital health; hence, general tort law applies. This includes, primarily, the tort of negligence and the regime of strict (no fault) liability under the Defective Products Liability Law, 5740-1980. Breach of contractual warranties may also come into play.

9.2 What cross-border considerations are there?

The laws of Israel are in principle limited to its territory. However, actions conducted outside the country's borders may be subject to the jurisdiction of Israeli courts if the foreign entity collaborated with a local entity, remotely provided service to recipients located within the territory, and possibly also when damages occur or are expected to occur in Israel.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

According to the Ministry of Justice's opinion, the use of content protected by copyright for the purpose of training a machine will be permitted even without obtaining the approval of the owners of the rights in the content. However, if generative AI ventures beyond training digital health technologies, it is advisable to adopt the following measures to mitigate potential legal complications: using content from databases wherein the content owners have granted explicit consent for such usage; employing technologies designed to minimise the probability of generating infringing content; adhering to pertinent healthcare regulations to ensure compliance with industry standards and legal requirements; implementing and maintaining sufficient administrative, technical and physical safeguards; documenting the development and the decisions taken with regard to the technology; including liability clauses in agreements with third parties; and establishing clear terms and responsibilities.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

In Israel, misuse of healthcare data in AI/ML models used in digital health solutions can give rise to liability under the following laws:

1. The Privacy Protection Law, 1981: since healthcare data is deemed sensitive information, unauthorised use or inclusion in AI/ML models without explicit consent breaches privacy and may lead to civil liability or enforcement by the PPA.
2. Copyrights: While raw healthcare data itself is not protected by copyright, the specific way in which this data is organised, curated or presented – such as in a database or a structured dataset – can be protected. According to the Ministry of Justice's opinion from December 2022, except in exceptional cases, the use of copyrighted materials for the purpose of machine training falls under fair use and therefore does not constitute a copyright infringement. In cases where the structure of the dataset significantly influences the outputs of the AI/ML model, there may be grounds to argue that the outputs constitute infringement.
3. Trade Secrets: Healthcare data can qualify as a trade secret due to its proprietary nature and its ability to provide a competitive advantage. The use of such data for training AI/ML models without the rightful owner's consent, or when improperly acquired or utilised, may be subject to legal remedies under the Commercial Torts Law, 1999.
4. Torts: Misuse of healthcare data in AI/ML models could be analogised to violations of ownership and possession rights under laws protecting property, such as sections 15–20 of the Real Estate Law, 5729-1969. If entities exercise unauthorised control over data, similar to a "holder" misusing property, they may face liability. In addition, the Movable Property Law, 5731-1971, supports extending these principles to healthcare data, treating it as intangible movable property, thereby reinforcing protections against misuse under privacy and contractual frameworks.
5. Patient Rights Law, 1996: Using patient data in AI/ML without informed consent breaches medical ethics and legal obligations.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

When using Cloud services, questions arise regarding the privacy and security of the data uploaded to the Cloud and its security.

When the Cloud is located outside of Israel, questions arise regarding the authority to transfer such data outside the country's borders. The Privacy Protection Regulations (Transfer of Personal Information to Databases Outside the State Borders), 5761-2001, set out conditions for transferring data abroad; for example, the party the data is transferred to must undertake to comply with the conditions for data retention and use applying to a database located in Israel (section 2 (4) of the Regulations).

In July 2019, the MOH authorised, for the first time, hospitals and healthcare organisations to use Cloud services. Alongside the benefits of using Cloud services (such as digital medicine upgrading and cutting back on computing costs), there is concern regarding stealing patient medical data and the risk of cyber-attacks.

In response to these legal and security considerations, and to address data sovereignty requirements, Oracle has established a dedicated Oracle Cloud region in Israel. The region provides locally based cloud infrastructure that allows organisations to store and process data within the country, thereby limiting cross-border data transfers. This local deployment is intended to support compliance with Israeli regulatory requirements and data protection obligations.

In parallel, the Israeli government has established the Nimbus project, a national cloud initiative designed to provide a comprehensive framework for the provision of public cloud services to government ministries and other public bodies, with the aim of improving digital infrastructure, supporting cloud adoption, and addressing security and data-localisation requirements.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The digital healthcare market's landscape is in constant flux and there are many areas of uncertainty, not to mention that it may vary among countries. Thus, partnering with an institution with experience in the field is advantageous. Special care must be paid to the regulatory schemes applicable to both the R&D stage as well as the commercial marketing and sales stage.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

The arrival time of a large part of digital medicine technologies (such as smart apps and medical devices) is significantly short (unlike in pharmaceuticals where the arrival time may take years).

The following are key factors that should also be considered:

- Maturity of the venture's product.
- Time to market ("TTM") (generally speaking, in digital health technologies TTM may be significantly shorter than in past traditional industries).
- Background of founders and major managers (serial entrepreneurs with proven track records are highly sought after).
- Collaboration with strategic partners (for example, having a leading HMO as a commercial partner or as the alpha site provider).
- Scope of required investment and expected return.
- Characteristics of the product's market and commercial and regulatory IP challenges.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

There are no specific key barriers in Israel, but rather general key barriers that may be relevant in other jurisdictions as well and include, *inter alia*, the following: regulatory requirements in the targeted market (which are evolving and constantly taking shape and form); the characteristics of the targeted market/population; the need to cooperate with additional entities (strategic partners); etc.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The sole clinician certification body in Israel is the MOH. The decision whether to adopt digital health solutions is dependent on clinical benefit and cost-effectiveness, regardless of the technology.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

The Israeli market is different from the American market, since it is nationalised – namely, most of the health services are provided by HMOs, which are budgeted by the State. The services provided by the HMOs (including services, drugs, medical equipment and devices) are those that are included in the "health basket". The "health basket" is based on the health services that were being provided by the Clalit HMO as of 1 January 1994 and the health services that were provided by the MOH as of 31 December 1994. Once a year, new drugs and medical technologies are added to the "health basket" following approval by the MOH and subject to additional budgeting allocated for this purpose by recommendation of a public committee. The decision regarding which drugs and medical services are to be added to the "health basket" are made based on clinical benefit and cost-effectiveness, regardless of the technology. It is to be noted that some digital technologies, especially applications, are not regulatorily defined as MADs, which is a basic condition for the inclusion of a technology in the "health basket". Nonetheless, the "health basket" includes digital technologies such as CGM systems (continuous glucose monitoring) or smart pacemakers.

The health insurance market, however, is completely private, and each company determines the terms of the reimbursement.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence gaps in the healthcare ecosystem for analysing digital health solutions, particularly those involving data-driven products like AI/ML-based solutions, can arise due to the complexity and novelty of these technologies. These gaps typically include:

- **Regulatory Compliance**: In general, there is often a lack of understanding of applicable regulatory frameworks (e.g., FDA, EMA, HIPAA and GDPR) and unclear pathways for approval or certification due to evolving regulations. For AI/ML models, the adaptive nature of these technologies creates additional challenges in meeting regulatory standards, particularly as regulations lag behind advancements.
- **Data Privacy**: General gaps include insufficient assessment of compliance with data protection laws (e.g., GDPR and CCPA) and inadequate measures for securing sensitive healthcare data. For AI/ML models, additional concerns arise regarding sourcing of training data, obtaining informed consent, data anonymisation and ensuring the prevention of algorithmic bias.
- **Clinical Validation**: Many digital health solutions lack rigorous evaluation of their efficacy, safety and real-world performance. For AI/ML models, limited validation of their robustness, generalisability across diverse population, and adaptability to new clinical scenarios is a common shortcoming.
- **Bias and Transparency**: General digital health solutions may overlook ethical considerations, such as equitable access and fairness in outcomes. For AI/ML models, there

are additional risks of algorithmic biases and disparities, often due to underrepresentation in training datasets, which can lead to unequal outcomes.

- **Cybersecurity**: General gaps include weak evaluations of data security measures and resilience against breaches. For AI/ML solutions, these gaps extend to vulnerabilities in the handling of training data and protecting models from adversarial attacks.
- **IP**: General ambiguities arise regarding ownership of co-developed digital health solutions or datasets. For AI/ML models, unclear ownership of algorithms, training datasets and derivative insights can create legal and operational conflicts.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

It is worth noting that the PPA published in August 2022 a document detailing the challenges of privacy protection involved in the use of telemedicine services. The document maps the types of remote medical services currently provided in Israel, reviews the risks to patients' privacy when using telemedicine services, summarises legal provisions and relevant guidelines and presents clarifications and recommendations regarding the manner in which telemedicine services should be used in order to reduce the harm of patients' privacy (including collection, documentation, storage and processing). While the recommendations are not mandatory, companies interested in entering the digital healthcare market should be aware of these recommendations and ensure that they are applied by the telemedicine services suppliers.



Adv. Eran Bareket holds an LL.B. degree, 1990, from Tel Aviv University and teaches in leading Israeli universities.
Eran's expertise is in litigation, in particular: IP rights; unjust enrichment; competition law and complex litigations, particularly those involving technology issues; and management of multi-jurisdiction IP litigations.
Eran has vast experience appearing before all Israeli courts, including the Patents, Designs and Trademarks Registrar. He is well versed in the fields of: IP; high technology; technology transfer and licensing; digital health; big data licensing; competition law; agency and distributorships; regulatory law (pharmaceuticals/medical devices); defence and homeland security; and governmental companies.
Eran is often involved in the Israeli Parliament (*Knesset*) legislative process, acting on behalf of various entities. He serves as a consultant for IP matters to the Accountant General's Division of the Ministry of Finance and represents the government regarding disputes surrounding inventions by state employees (service inventions).
Eran is continuously commended by leading international guides.

Gilat, Bareket & Co., Reinhold Cohn Group
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: eranb@gilatadv.co.il
LinkedIn: www.linkedin.com/in/eranbareket



Adv. Alexandra Cohen holds an LL.B. degree, 2016, from Tel Aviv University.
Alexandra handles various aspects of IP rights, including patents, trademarks and copyrights, and represents clients in litigation proceedings before Israeli courts and the Registrar of Patents, Designs and Trademarks. Alexandra's expertise extends to various patent litigations across different sectors, including the pharmaceutical industry, serving a diverse clientele both locally and internationally. She also provides services with respect to commercial law, licence agreements and privacy issues. Additionally, she has contributed to several guides, particularly in the areas of patents, trade secrets, digital health and privacy.

Gilat, Bareket & Co., Reinhold Cohn Group
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: alcohen@gilatadv.co.il
LinkedIn: www.linkedin.com/in/alexandra-cohen-502b192a7

Reinhold Cohn Group (RCG) is the leading IP consulting firm in Israel. RCG offers a full breadth of IP-related services and expertise including protection, asset management, due diligence, and litigation & legal services. The firm operates in all areas of IP such as patents, trademarks, designs, copyrights, open source, plant breeders' rights, etc.
The group includes the patent attorneys firm, Reinhold Cohn & Partners, and the law firm, Gilat, Bareket & Co.
The synergy of patent attorneys experienced in a diverse spectrum of technological and scientific disciplines working alongside legal professionals, creates a unique and effective platform for maximising the value of a client's IP assets by securing optimal protection.
RCG and its team of professionals are internationally renowned for excellence and continually ranked amongst the top tiers in leading international and local guides.

gilat-bareket.rcip.co.il

Gilat Bareket Attorneys at Law | Reinhold Cohn Group

Italy


Sonia Selletti


Claudia Pasturenzi


Chiara Screpanti

Astolfi e Associati Studio Legale

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

A legal definition is not provided by Italian law; however, "digital health" can be defined as the use of information and communication technologies in the health sector for the purposes of prevention, diagnosis, treatment and monitoring of diseases (in compliance with the definition provided by the World Health Organization). The term also takes on a larger significance than that of the medical-therapeutic field, including the use of lifestyle and wellness technologies.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

In Italy, the practical applications implemented to date in part or in full as regards digital health are the online sale of (non-prescription) medicinal products, the health card, electronic medical prescriptions, reservations for online healthcare services (through the *Centro Unico Prenotazioni*), electronic health records (EHRs, *Fascicolo Sanitario Elettronico*), digitalised reports, telemedicine and teleconsultation. In this regard, in September 2025 the State–Regions Conference approved the draft decree setting out the rules, governance framework and security requirements for the operation of the National Telemedicine Platform (PNT), established within the National Agency for Regional Health Services (*Agenas*). *Agenas* itself published, on 14 October 2025, two new documents containing guidelines to support the design, quality and interoperability of telemedicine services within the PNT, one relating to telemonitoring and telecontrol and the other relating to televisits.

Also, on July 2025, the Social Affairs Commission of the Chamber of Deputies presented a consolidated draft bill establishing a national committee within the Ministry of Health to guide the inclusion of Digital Therapeutics (DTx) within the Essential Levels of Care (LEA).

1.3 What is the digital health market size for your jurisdiction?

According to a 2025 analysis by NetConsulting cube, in 2024, the digital health market in Italy exceeded 4.6 billion euros, marking an increase compared to the nearly 4.2 billion euros recorded the previous year. The main driver of growth is represented by social-care and territorial applications, which rose from 54.8 to 375 million euros, reflecting the shift toward community-based healthcare models. The EHR also expanded significantly, with its value increasing fivefold (from 69.3 to 375 million euros), confirming its strategic role. Telemedicine continues to grow gradually, from 46.8 to 70.7 million euros.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Among the digital health companies with a more relevant market, we could mention Philips Healthcare, Reply, Dedalus Italia S.p.A., Healthware Group, Artexe S.p.A., Afea S.r.l., AlmavivA S.p.A. and Maticmind S.p.A.

We should add that the digital health ecosystem is also populated by numerous start-ups with innovative, high-performance proposals, who successfully obtain the approval, economic and otherwise, of other more structured organisations, as well as of State/regional authorities to begin operating at territorial level.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

We do not have direct information on the fastest growing digital health companies in our jurisdiction but, as far as we know from the public access sources, we can include: Dedalus Group; Telbios; Healthware Group; and Exprivia-Italtel.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The main healthcare regulatory authorities in Italy are: the Ministry of Health, as the promoter and implementing body and controller of initiatives aimed at the development of digital health both at an EU and national level, through coordination that serves to guide and optimise efforts and resources made available by all stakeholders; the Ministry of Economy and Finance, responsible for planning public expenditure and verifying its progress; the Ministry of the University and Research, promoting research; and the Privacy Authority, as the controller of the application of Regulation (EU) 2016/679 (GDPR) and the Privacy Code and guarantor that

the processing of personal data is compliant with the fundamental rights and freedoms of individuals. Although this is not an authority with an assigned role in health IT issues, the Ethics Committee can play an important role with reference to projects (including clinical trials) using digital/new health technologies, and may serve as a consultation body for any ethical health-related issues as well as a guarantor of the rights, safety and well-being of the subjects involved.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

In Italy, the regulation of digital health is governed by different regulatory schemes. In particular, the main regulatory schemes are Regulations (EU) Nos 2017/745 (MDR) and 2017/746 (IVDR) and national Decrees Nos 137/2022 and 138/2022 cover traditional devices and software such as medical devices (Software as a Medical Device (SaMD)), imposing strict requirements in terms of quality and safety.

The protection of personal data is regulated by the GDPR and the Italian Privacy Code (Legislative Decree No. 196/2003).

Anti-kickback rules govern the financial relationships between healthcare workers and medical device companies, with the National Anti-Corruption Authority tasked with preventing unethical practices and ensuring transparency.

In the area of national security, the National Cybersecurity Agency is responsible for protecting healthcare infrastructures from cyber-risks, particularly considering the ever-increasing value of health data, applying cybersecurity laws, including Legislative Decree No. 138/2024, which transposed the Directive 2022/2555 (so-called NIS2).

The national Law No. 132 of 2025 (in force since 10 October 2025) on Artificial Intelligence must be interpreted in accordance to the EU Regulation No. 1689/2024 on Artificial Intelligence (AI Act), which introduces specific requirements for AI systems used in healthcare.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The factors that may slow down the "take-off" of digital health in Italy constitute the "mirror" of the areas for intervention and improvement. The intervention areas are:

- investment programmes to train dedicated HCPs – both the new generations and the already active health workers – an increasing number of universities offer courses on the subject and continuing medical education (CME) is an important way to spread knowledge and develop culture;
- management of the social and relationship-based aspects with patients and caregivers to reassure that the required assistance and care are ensured despite the use of new tools: this fosters efficiency and promotes quality; and
- development of culture, and education on the use of digital health technologies to patients, caregivers and patient associations; it is important to engage in information, keeping in mind that patients are increasingly "experts" and "demanding" interlocutors, while also being vulnerable subjects suffering from an illness, with a desire to recover.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

SaMD is governed by the MDR, IVDR and the following local decrees that have been issued to complete the framework (No. 137/2022 as the adaptation to the MDR, and No. 138/2022 as the adaptation to the IVDR). The competent authority in this sector is the Italian Ministry of Health.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Italy recently implemented Law No. 132 of 2025 (in force since 10 October 2025), which transposes the European AI Act principles (EU Regulation No. 2024/1689). Article 7 specifically governs the use of AI in healthcare, affirming the fundamental principles on the subject, including the fact that AI systems constitute "*a support in the processes of prevention, diagnosis, treatment and therapeutic choice, without prejudice to the decision, which is always referred to the medical professional*" and that they, together with the data used, "*must be reliable, periodically verified and updated in order to minimise the risk of errors and improve patient safety*".

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Regulatory authorities are adapting their traditional approval schemes to better address the dynamic nature of AI/ML-based digital health solutions. The Italian Medicines Agency (AIFA) and the Ministry of Health have begun exploring frameworks for more agile assessments, recognising the need to evaluate digital health tools as they evolve through continuous updates. Key efforts include developing guidelines and best practices that consider real-world data and performance monitoring as part of post-market surveillance, acknowledging that AI/ML solutions often undergo changes that impact their functionality and efficacy.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data plays a critical role in the regulatory considerations for AI/ML-based digital health solutions. Italian regulatory authorities, aligning with European frameworks like the MDR and the AI Act, require evidence of clinical validation to ensure that AI/ML algorithms consistently deliver accurate and reliable outcomes across diverse patient populations and in different healthcare settings. Specifically, according to Law No. 132 of 2025, AI systems used in healthcare, and the data on which they rely, must be reliable, periodically tested, and updated in order to minimise the risk of errors and enhance patient safety.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Digital health products and solutions are primarily governed by national-level regulations that align with broader European directives and frameworks, such as the MDR and GDPR. These regulations are enforced and implemented by national bodies, such as the Italian Ministry of Health, AIFA and the Italian Data Protection Authority. However, certain aspects of healthcare services and the practical application of digital health initiatives may be subject to regional regulations and oversight. While national regulations set the broad framework, regional healthcare bodies may influence how these standards are applied in practice, resulting in some variations in the accessibility, governance and operation of digital health solutions across different regions. The aforementioned *Agenas* guidelines on telemonitoring, telecontrol and televisits are an example thereof.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Enforcement is primarily guided by overarching European regulations, such as the MDR and GDPR, with Italian authorities like the Ministry of Health, AIFA and the Italian Data Protection Authority playing key roles in ensuring compliance. Tailored actions have focused on both pre-market approval and post-market surveillance to manage risks, promote patient safety and ensure adherence to data protection standards.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  The main legal issue is the need of a prior authorisation for the performance of healthcare activities. On this point, telemedicine initiatives have received support from case law, which has recognised that non-purely health activities that pertain to broader telemedicine projects (such as the collection of health data through patient/technology interaction with subsequent sending to a physician for reporting) are not subject to the prior authorisation required by Italian legislation for the performance of healthcare activities (Supreme Court, criminal section, decision No. 38485/2019).
- **Robotics**
  Openness to the use of robotics requires the adequate training of health professionals as well as exhaustive information to patients, in order to comply with the rule of informed consent for the service, which is an expression of the principle of the inviolable freedom of choice of each individual. The main legal issue regarding the use of this healthcare technology is connected to the individuation of responsibilities in case of damages occurred to patients.
- **Wearables**
  The core legal issues related to the use of wearables in the healthcare sector are connected to the management of security and the protection of information collected in compliance with confidentiality and data protection laws and the qualification of certain instruments as medical devices to ensure the application of the relevant legislation.
- **Virtual Assistants (e.g. Alexa)**
  The main issues connected to this technology consist of the management of the large amount of data and the liability of subjects involved in their creation and use.
  Another key issue is profiling and the respect of the principle of non-algorithmic discrimination, which requires the data controller to use appropriate profiling procedures and adopt suitable technical and organisational measures to minimise the risk of error. In this regard, in 2023, the Italian Privacy Authority adopted a decalogue on the responsible use of AI.
- **Mobile Apps**
  The main issues concern the legal classification of the app (notably, whether they fall within the definition of a medical device), as well as the processing of the enormous amount of data.
  With reference to apps for illness management or diagnosis support, it will also be essential to provide adequate information to the patient and physician.
  As regards data processing, the Italian Authority for the Protection of Personal Data expressed important indications for their correct management.
- **Software as a Medical Device**
  Software that falls within the definition of a medical device must comply with applicable legislation on the matter. While many different software currently fall into risk class I (affixing the CE marking without the intervention of the notified body), the MDR establishes stricter rules that may potentially lead to an increase in the risk class, with the consequent involvement of the notified body.
- **Clinical Decision Support Software**
  Clinical decision support software uses technologies such as ML, Natural Language Processing (NLP) and Big Data analytics to assist physicians with clinical decision-making tasks, delivering actionable recommendations and providing complimentary materials such as data reports, guidelines, clinical document templates, etc. Consequently, the main issues are connected to liability profiles, should the clinical decision harm the patient, and the management and security of the personal data and information processed by the software.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  With reference to AI and ML solutions, regulatory assessment of the context and rules to be applied may be necessary, depending on the type of activity covered by the digital health solution. Relevant profiles include management and processing of personal data and correct identification of liability for damage arising from system errors or malfunctions.
- **IoT (Internet of Things) and Connected Devices**
  Internet of Things (IoT) should ensure the protection of privacy and the correct use of personal data collected. Risks related to the safety of devices should not be underestimated: if they are not adequately safeguarded, it can lead to multiple issues of liability in the event of malfunction.
- **3D Printing/Bioprinting**
  Among the main fields of application of 3D printing and bioprinting technology in healthcare are the production of medical devices and the recreation of realistic models

of organs to facilitate the understanding of complex surgical interventions in the surgical field. 3D printing can also be used to reproduce biological material for the replacement of human organs and tissues (bioprinting).

- **Digital Therapeutics**
  DTx are hybrid solutions that present specific characteristics of medical devices but also affinities with pharmaceuticals. This also has implications as regards the national authorities responsible for the assessment of DTx. Other questions to be considered are personal data privacy and security, and, depending on the type of technology and functions applied, risks relating to the safety of devices. Another complex issue is certainly the liability of the parties involved in the production, marketing and use of these solutions. As mentioned before, the Social Affairs Commission of the Chamber of Deputies presented a consolidated draft bill establishing a national committee within the Ministry of Health to guide the inclusion of DTx within the LEA.
- **Digital Diagnostics**
  The main legal issues are connected to the fact that the diagnosis is reserved only to the physician, who cannot be replaced by a machine in the performance of this activity.
- **Electronic Medical Record Management Solutions**
  Different subjects (HCPs, patients, etc.) can access electronic medical records; therefore, security measures should be adopted in order to ensure the correctness and accuracy of data and information and the confidentiality of personal data.
- **Big Data Analytics**
  Big Data analytics in the healthcare sector involves the processing of large volumes of data, often containing personal or sensitive information, and for this reason it is regulated by the GDPR and the Guidelines of the Privacy Guarantor. These regulations state that health data, when used for the analysis of Big Data, must be managed in a secure manner and, where possible, anonymised to reduce the risk of violation of patients' privacy. Furthermore, the processing of health data requires a sound legal basis, such as informed consent or clearly defined legitimate interests. In the European context, the use of Big Data for health purposes must also comply with the ePrivacy Regulation, which provides guidelines on how to collect, store and share sensitive data in a safe and ethical way, avoiding improper or discriminatory uses.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain technology is emerging as an innovative tool for the secure management and sharing of health data, but it is subject to specific regulatory requirements to ensure privacy and data protection. The GDPR requires that any processing of personal data, including its storage in a decentralised network, respects the principles of transparency, security and erasure possibilities, which can be complex to implement in a blockchain. In Italy and in the EU, there are no specific regulations for the use of blockchain in healthcare, but several guidelines are being studied to establish how this technology can comply with existing laws.
- **Natural Language Processing**
  It is necessary to develop solutions inspired by different disciplines (e.g. linguistics, computer science, neuroscience, etc.) to understand and generate text in a natural language that is more similar to human language, and have a large amount of data to validate and implement services.
  The use of NLP-based tools should be subject to prior information to educate the user on the decoding of information received and its application in everyday life.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

In Italy, digital platform providers operating in the digital health sector must navigate a complex regulatory framework encompassing healthcare regulation, data protection and digital law. Key issues include compliance with the MDR where applicable, the lawful processing and security of health data under the GDPR, interoperability with public digital infrastructures such as the EHR and the PNT, and the allocation of liability between platform providers and healthcare professionals.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In Italy, the use of personal health data is primarily governed by the EU General Data Protection Regulation (GDPR) and its national implementing framework, including Legislative Decree No. 196/2003 (the Italian Privacy Code), as amended. Health data qualify as a special category of personal data and may be processed only where a lawful basis and a specific exemption under Article 9 of the GDPR apply, subject to enhanced security and accountability requirements. In addition, Regulation (EU) 2023/2854 (the Data Act), fully applicable since September 2025, introduces rules on access to, sharing and use of data generated by connected devices and related services, including in healthcare contexts, without prejudice to GDPR protections for personal data.

Key issues are related to the circulation of health data, the outsourcing and delocalisation of systems and services, as well as the storage of data in geographic locations often regulated by different legislation.

When processing personal health data, orders and guidelines issued by the Italian Data Protection Authority should also be considered, since they give useful indications on different questions, such as security measures to be implemented, the different roles in the processing, the legal basis, etc. With specific reference to personal data processing in the health sector, the Italian Data Protection Authority adopted opinions and guidelines on the processing of health-related data through AI systems, as well as through websites and apps aimed at putting into contact patients and HCPs.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Italy, the use of personal health data is primarily regulated at the national level, with uniform application of the GDPR at the EU level and further detailed by the Italian Privacy Code.

According to our Constitution, Regions have the authority to adopt specific regulations in the health sector, always within the regulatory framework established on a national level. For

example, Regions have a degree of autonomy regarding the operational aspects, including the processing of health data, of implementing and managing EHRs and telemedicine platforms, while still adhering to national requirements and ensuring that access and data sharing across healthcare facilities comply with national security and privacy standards.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

According to the Italian Privacy Code, processing by a public authority is always allowed if it is necessary for the performance of a task conducted in the public interest or for the exercise of the authority's public powers and that if the purpose of processing is not expressly envisaged under a law or regulation, it shall be decided and indicated by the authority consistently with the task conducted or the power exercised.

Furthermore, the Italian law provides specific rules on the processing of health data by health professionals and health facilities (Privacy Code and Acts issued by the Italian Privacy Authority). The Privacy Code rules on information disclosed to patients by general practitioners and paediatricians (Art. 78), as well as public and private health facilities (Art. 79). Provision No. 55 of 7 March 2019 of the Italian Privacy Authority gives indications on the privacy information scheme, the legal basis of the processing activity, the appointment of the Data Protection Officer, and processing records specifically for the processing of health-related data carried out by HCPs, regardless of whether they operate as freelancers or within a public or private healthcare facility.

4.4 How do the regulations define the scope of personal health data use?

A definition exists at neither a national nor European level. The GDPR has established that the processing purposes must be specific, explicit and legitimate. It is up to the data controller to identify the processing purpose and specify it in the disclosure provided to the data subject (Arts 13 and 14 of the GDPR).

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Since there are no specific national provisions on this topic, GDPR rules shall apply.

Firstly, the data subject should be clearly informed of the specific purposes for which personal health data is collected and processed, in accordance with the principle of purpose limitation established by the GDPR. It is essential to outline the rights of data subjects, including access, rectification, erasure and the right to object, ensuring compliance with GDPR provisions. Additionally, the legal basis for processing health data should be specified and, if the explicit consent of the data subject represents the legal basis for a specific purpose of the processing, it shall be collected through a request that shall be presented in an intelligible and easily accessible form, using clear and plain language. Provisions on data minimisation and retention should ensure that only the necessary data is collected and retained for a limited time and the data subject should be informed on the specific retention period of his/her personal data. Appropriate technical and organisational measures should be implemented in order to safeguard the data security. If data processors are involved, the agreement should require adherence to data protection obligations provided for in Art. 28 of the GDPR.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The Italian Privacy Code provides for the possibility of submitting a complaint to the Italian Privacy Authority or, alternatively, of pleading the judicial authority, as long as a violation of rights under the GDPR occurs. The Italian Privacy Authority also has the power to issue the provisions pursuant to Art. 58 of the GDPR, including the application of administrative fines, pursuant to Art. 83 of the GDPR, both on reporting and *ex officio*.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

In Italy, standards for the collection and use of personal health data are primarily set by the GDPR and the Italian Privacy Code (Legislative Decree No. 196/2003), complemented by sector-specific measures. Key initiatives include national rules and technical guidelines on the *Fascicolo Sanitario Elettronico* (EHR), issued by the Ministry of Health and *Agenas*, which define interoperability, security and data access standards. Additional standards derive from telemedicine guidelines, national interoperability frameworks for digital public services, and binding measures and guidance adopted by the Italian Data Protection Authority, which play a central role in shaping operational requirements for health data processing.

Finally, Article 9 of Law 132/2025 provides for the adoption of a decree by the Ministry of Health (not yet adopted) aimed at regulating the processing of personal data using the most simplified methods for research and experimentation purposes, including through AI and ML systems, including the establishment and use of special experimentation spaces for research purposes, and including through the secondary use of personal data.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In Italy, the sharing of personal health data, just like any other personal data, is primarily regulated by the GDPR and the Italian Privacy Code, the Data Act on access to and sharing of data generated by connected products and related services, and opinions and guidelines of the Italian Data Protection Authority.

The identification of subjects who have access to the personal data processes and their respective roles is the main focus; in complex supply chains, it could be difficult to identify who processes the personal data involved among the various managers of intermediate services. It is important to

establish the capacity of each subject, identifying who acts as an independent data controller, who works as joint controller and who is designated as a data processor or sub-processor for the processing activity, stipulating specific agreements that govern relations among the various subjects.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal data sharing is subject to the same laws and regulation generally applying to personal data processing. For this reason, the same analysis reported above (see question 4.2) may be considered here.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Data-sharing operations require more caution for health-related data processing as performed by HCPs. The processing of such data is carried out for purposes of care, and any sharing or transfer to other subjects would need to "match" the purposes (e.g. marketing purposes). It is therefore necessary to carefully evaluate the subjects with whom the data collected are shared, and verify the purposes for which they will be processed.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Ministerial Decree of 7 September 2023 ruled the "Electronic Health Records 2.0", which includes more documents and information and a "personal section" of the record, in which personal documents related to health treatments could be inserted, together with the "patient summary", an informatic document written and updated by the physician, in order to ensure the continuity of care.

Additionally, the guidelines adopted by the Italian Data Protection Authority on websites and apps aimed at putting into contact patients and HCPs is an example of an initiative regarding standards for sharing health data (see question 2.6).

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

When sharing data and, in particular, healthcare data, it is necessary to implement adequate security measures, in order to protect the accuracy and confidentiality of personal data from any unauthorised access. For this scope, the subjects entitled to collect and upload data, have access to and process them shall be identified. Furthermore, an appropriate retention period of data should be determined, taking into account the purpose of the processing, and data subjects' rights should be granted. The same rules governing data privacy already mentioned shall apply.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

In Italy, patent laws impact the scope of patent protection for digital health technologies by setting specific criteria for patent eligibility under the Industrial Property Code (IPC, Legislative Decree No. 30/2005). The Code outlines the scope of the patent by indicating patent requirements and the cases that remain excluded from the patentability. Patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible to industrial application. Methods for surgical or therapeutic treatment of the human or animal body and the diagnostic methods applied to the human or animal body cannot be patented.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

In the Italian jurisdiction, the Copyright Law (Law No. 633/1941) impacts the scope of copyright protection for digital health technologies by safeguarding the expression of ideas – such as the source code and graphical interfaces – rather than the underlying functionality or concepts.

In particular, the Copyright Law gives the creator the exclusive right to use his/her work, which lasts for the entire life of the creator, and up to 70 years after his/her death. According to the law, computer programs (software) and databases that, due to the choice or arrangement of the material, constitute an intellectual creation of their creator, are protected by copyright (see question 6.5).

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

In Italy, trade secrets play a key role in protecting digital health technologies by safeguarding confidential information such as algorithms, data analytics models and proprietary know-how.

Legislative Decree No. 63/2018, implementing the EU Trade Secrets Directive on the protection of confidential know-how and confidential business information, strengthened the existing framework under the IPC by expanding protection and increasing penalties, including for IT-related infringements.

Protection covers information that is secret, has economic value because it is secret, and is subject to reasonable confidentiality measures (art. 98 of the IPC); the legitimate holder may prohibit unlawful acquisition, use or disclosure. This regime is also particularly relevant for confidential test data in the pharmaceutical sector and requires tailored confidentiality agreements and appropriate internal organisational measures.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Technology transfer covers the movement of knowledge, technology and skills from research to the market, as a result of a

collaboration between academia and industry, with the aim of making innovation publicly accessible.

Under Italian law (Art. 65 of the IPC), inventions developed in universities follow two main regimes: in institutional research, ownership generally lies with the researcher, and the university is granted the right to receive at least 30% of the profit of the invention in the event that it is actually exploited economically; and in "funded research", ownership typically belongs to the institution, which may negotiate exploitation rights with the financing party.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

In principle, according to Legislative Decree No. 518/92 (enforcing Directive No. 91/250/EU), which integrated the law on copyright (Law No. 633/1941), software is protected by copyright, which covers its source and object code, but not its underlying ideas or functions; protection arises automatically upon creation, with optional registration to prove authorship.

However, it cannot be excluded that a software can have a technical function, thus be assimilated to an invention, and therefore be patentable; this is possible for SaMD. The Italian IPC (Art. 45) and the European Patent Convention (Art. 52) exclude the patentability of software "as such"; although, if it is possible to demonstrate the additional technical effect of a software, the protection deriving from the patent gains more significance because it allows the protection of the invention in any form it is reproduced, even if the patent has a shorter duration of protection (20 years) than that of copyright (70 years from the death of the creator), and requires registration in all of the areas in which protection is sought. As such, the costs are higher. Distinguishing between patentable and non-patentable software is often complicated and requires a case-by-case assessment by an expert.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

The ownership of patents invented by AI devices is still being debated in Italy.

To date, there are no Italian rulings on the matter, although different jurisdictions have refused to recognise AI as an inventor of a patent based on the fact that the inventor must be a natural person and that AI's inventions do not possess the characteristics of creativity and originality necessary for specific protection. This approach is reflected in Law No. 132/2025 with regard to copyright, which provides that only works of human intellectual creation of a creative nature are protected, even where they are produced with the assistance of AI, provided that they constitute the result of the author's own intellectual effort.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The reference for government-funded inventions is Art. 65 of the IPC (see question 6.4), which applies to the inventions of researchers who work for a university or other public entity whose institutional purposes include research. Art. 65 of the IPC does not apply to research carried out within specific research projects funded by public entities other than the entity to which the researcher belongs.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

As far as we know, there are no specific decisions on this matter. However, with reference to intellectual property rights in the life sciences sector, we can recall the Italian Supreme Court decision No. 18372/2024. The Court clarified the scope of the Bolar exemption under Italian patent law, holding that activities carried out to obtain regulatory approval for a generic medicinal product (including clinical or experimental testing of a drug covered by another party's patent) do not constitute patent infringement, provided they are strictly limited to regulatory purposes. The decision reinforces the balance between patent protection and early market entry of generics, aligning Italian case law with EU principles.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

When dealing with collaborative improvements, the parties should consider that the link between the various subjects of the network is generally obtained with specific agreements that may have different legal nature, depending on the scope and purpose pursued, such as: consortia; contractual joint ventures; and partnerships between public and private entities; as well as licensing relationships if intellectual property is involved. It is recommended that a customised contractual model be prepared that is adapted for the specific project and its potential outcomes.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

The healthcare sector in Italy (as well as in the EU) is subject to strict rules to both protect health and encourage business development. Healthcare companies are structured to operate in compliance with detailed regulatory schemes, and also take part in self-regulatory organisation that provides for the extension of rules and principles in relation to companies with less restricted activities in other sectors. It is therefore fundamental to capitalise on the experience of healthcare companies in the business and contractual model in order to encourage efficient integration and cooperation.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

The main aspects that parties should consider are the ones connected to security and confidentiality of data. The federated learning system should be protected by adequate security measures, since a possible attack to the system could jeopardise the data and information of all the participants.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties should consider aspects connected to data privacy, liabilities in case of damages occurred by patients and intellectual property rights. Furthermore, it should be considered that the only subject entitled to make a decision is the physician, and so AI technology can be used only as a support (Art. 7, Law No. 132/2025).

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

In addition to the authorities already mentioned in question 2.1, it is important to mention: the Agency for Digital Italy (AgID), which oversees the use of AI within the public administration, focusing on technical standards, interoperability, and compliance with digital government rules; the Agency for Cybersecurity (ACN) which is responsible for the supervision, inspection and sanctioning activities of AI systems and for the promotion of AI with regard to cybersecurity aspects; and the Authority for Communications Guarantees (AGCOM), acting as the Digital Services Coordinator.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Laws and regulations already mentioned on data protection, intellectual property rights and copyright and medical devices shall apply (see questions 2.1–2.9, 4.1–4.7, 5.1–5.5 and 6.1–6.8).

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under Italian law, copyright protects works created through a human creative contribution. Algorithms or software improvements generated autonomously by AI/ML without active human involvement are not eligible for copyright protection as such, because the work under protection must be the result of the author's "intellectual work" (art. 1, Law No. 633/1941). In practice, rights typically vest in the person or entity that created or lawfully controls the original software, training framework, or parameters, to the extent human creativity can be identified upstream.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

A key issue is how to properly value intangible assets, such as ML datasets, using methods that may include cost-based approaches, income or royalty-based models, depending on the nature of the asset and the assessment context.

At the same time, data licensing must comply with data protection laws, requiring clear contractual terms on permitted use, duration, security measures, and allocation of liability for misuse or breaches.

These challenges are heightened for healthcare data, given its sensitive nature: licensing must ensure patient confidentiality, and where required, informed consent, often relying on aggregation or anonymisation and stricter ethical and regulatory safeguards, including limits on secondary uses.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

In Italy, regulators do not yet apply a fully separate, standalone regime for generative AI, but they do differentiate it in practice through EU-level frameworks, which Italian authorities are tasked with enforcing.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Generative AI raises specific legal and regulatory issues that include lawful use of training data, transparency and explainability, risk of bias, misinformation and content manipulation and unclear allocation of liability for AI-generated outputs. Recently, the Italian Data Protection Authority ordered an urgent ban of a generative AI service that "undresses" photos and videos converting images of clothed individuals into highly realistic nude representations without the individual's consent, resulting in serious violations of personal image, dignity and privacy (decision No. 574, 01/10/2025).

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Italy does not have a standalone "data disgorgement law" for AI, but GDPR remedies, reinforced by recent national legislation and the EU AI Act, allow authorities to effectively neutralise models trained on unlawfully used data.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Even in the context of telemedicine, the traditional approach should remain applicable, according to which the physician's obligation is one of means rather than result, thus requiring the physician to carry out an activity that is appropriate to curing or improving the patient's health condition.

A problematic issue is whether the use of telemedicine entails situations of "special technical difficulty", in which Article 2236 of the Italian Civil Code limits the physician's liability to cases of intent or gross negligence; this assessment must necessarily depend on the evaluation of the specific circumstances of each case.

Where an adverse outcome of treatment is attributable to the inadequacy or malfunctioning of medical equipment, liability may also be imposed on the physician who knew or should have known of the equipment's defect through a verification carried out in accordance with ordinary professional diligence.

With regard to cases involving the use of AI systems, Law No. 132/2025, under article 13, has introduced an obligation on professionals (among these we should include physicians) to clearly inform the recipient subject (including patients) whether and how AI is used in the management of their case.

9.2 What cross-border considerations are there?

It is possible that technological services involve multiple subjects in different countries, thus involving multiple legal systems. In order to avoid disputes upstream as regards interpretation issues on the competent jurisdiction and applicable law in the event of dispute between the user and supplier, it is wise to pay absolute attention and use maximum precision in the regulation of contractual relations between the parties.

With regard to cooperation between States in the field of AI, it is important to mention that the AI Act established a European Artificial Intelligence Board, composed of one representative per Member State as an advisory board to ensure the consistent and effective application of the Regulation across Member States.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

1. Informed consent: it is important to obtain updated informed consent, namely to ensure that the patient is informed that AI tools are used in the management of their care.
2. Training: it is necessary to provide comprehensive training, on the one hand, to healthcare professionals, so that they are as capable as possible of responding to any malfunctions of the system and, on the other hand, to patients themselves, so that they are fully aware of the operating methods and implications of the use of such tools.
3. Professional supervision: risks can be mitigated if the use of AI systems is subject to supervision by an expert.
4. Transparency: AI systems should be transparent in their operations, especially regarding decision-making processes. In healthcare, this transparency is crucial for professionals who need to understand AI-generated insights for clinical decision-making.
5. Product safety standards and risk assessment: by identifying and mitigating with adequate security measures the possible risks early, developers can reduce the chance of liability issues arising later. Following MDR standards is especially critical for digital health products that impact patient diagnosis and treatment.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Liability for the misuse of healthcare data in AI/ML models in digital health solutions may imply liabilities related to data protection and data subjects' rights violation, professional and medical liability, and liability for defective products.

Case law has not yet addressed the misuse of healthcare data included in AI models used in digital health solutions. However, a decision of the Administrative Court of Milan (No. 3348, 21/10/2025) concerning the use of incorrect data in the legal field processed by AI may be taken as a relevant example. The Court held that the citation of case law through AI tools without prior verification by counsel may result in a breach of the duty to conduct proceedings with loyalty and probity, by introducing potentially misleading elements into the adversarial process, and that responsibility for citing judicial authorities and verifying their accuracy rests with the signatory of the procedural submissions.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The main key issues are: the outsourcing of data management, which requires appropriate rules for the control; and the need for full security guarantees of privacy.

The quality of network connectivity is essential to the efficacy of the performances and to guarantee the continuity of system accessibility. Therefore, it is essential to choose a service provider with high-quality standards in order to minimise the risks, and the Cloud computing contract must cover all aspects that could represent critical or unknown factors such as to generate liability.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Non-healthcare companies should first assess whether their solution falls within regulated healthcare categories (e.g. medical devices or DTx), as this determines market-access requirements. They must ensure compliance with health-data protection rules under the GDPR and, where applicable, the EU Data Act and forthcoming European Health Data Space (EHDS). Clinical validation and evidence are often required to substantiate product claims, particularly for AI-driven solutions, which may also trigger obligations under the EU AI Act. Companies should carefully manage liability exposure, system integration with healthcare infrastructures, and ethical and trust considerations.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

These firms should assess whether the target's products are correctly classified under healthcare regulations and whether they have a credible path to regulatory compliance and market access. Particular attention should be paid to health-data governance, as well as to clinical validation and evidence supporting product claims. They should also evaluate exposure to product and professional liability, cybersecurity and data-breach risks, integration with healthcare systems, and the robustness of reimbursement, adoption and scalability models, which often determine long-term value creation.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The main barriers to the widespread adoption of digital health solutions in Italy stem from economic, organisational and structural factors. Public healthcare providers often lack sufficient funding to cover the costs of digital technologies. Organisationally, regional autonomy leads to fragmented governance, with differing regulatory frameworks, implementation models and welfare strategies across Regions, resulting in non-standardised and uneven national adoption. Access is further constrained by gaps in infrastructure and availability of digital devices among both patients and healthcare professionals. Finally, uncertainty around health and professional liability may discourage clinicians from fully integrating digital solutions into routine practice.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Italy, there is no formal certification by medical associations in accordance with an objective protocol of criteria and without misleading claims.

At most, the endorsement of products by medical associations can take place. In order to be lawful, this endorsement must be accompanied by a certification of quality from passing a specific approval procedure, and not a mere commercial agreement, against payment, of product sponsorship by the association.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

In Italy, no DTx are currently reimbursed under the public healthcare system. Nevertheless, many companies are actively investing in the development of DTx, reflecting a clear growth trend in anticipation of the definition of an appropriate reimbursement and market-access pathway.

On 12 January 2025, during a hearing before the XII Social Affairs Committee of the Chamber of Deputies, held in the context of the parliamentary examination of draft bills on "Provisions on Digital Therapeutics", it was acknowledged that the adoption of DTx – within a regulatory framework governing their reimbursement by the National Health Service (SSN) – could represent a significant opportunity to improve the management of chronic diseases. In this context, particular emphasis was placed on the role of healthcare professionals, including pharmacists, in supporting the safe and effective use of digital health tools by patients, strengthening community-based care and contributing to the efficiency and sustainability of the healthcare system.

As a general rule, full and stable public reimbursement requires inclusion in the LEA, following assessment at both national and regional level. In this respect, the 2023 update of the LEA introduced certain digital and assistive technologies within prosthetic care, such as eye-tracking communication devices, adaptive keyboards for individuals with severe disabilities, digital hearing aids, home-automation systems, and environmental control and command sensors, signalling an incremental approach to the integration of digital technologies into reimbursed healthcare services.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence often underestimates regulatory classification and scope creep, with insufficient scrutiny of whether software qualifies as a medical device, high-risk AI, or both. For AI/ML, diligence may inadequately cover AI Act compliance, transparency, explainability, bias mitigation, and human oversight. Finally, liability allocation, cybersecurity resilience, interoperability, and reimbursement readiness are often reviewed superficially, despite being critical to scalability and long-term value.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

Beyond the issues already discussed, a key factor is the PNRR-driven digital transformation of the Italian healthcare system, which is accelerating investment in national, but also increasing scrutiny on interoperability, governance and long-term sustainability once public funding phases out. The progressive implementation of the EHDS is expected to materially affect data access, secondary use, and cross-border scalability of digital health and AI solutions.

There is also growing attention to outcomes-based and value-based healthcare models, which may influence future reimbursement of digital tools, particularly DTx. From a regulatory perspective, the combined application of the MDR, AI Act and evolving liability regimes will raise compliance expectations and due diligence standards, especially for adaptive AI systems. Finally, increasing focus on cybersecurity, resilience and ethical AI, together with professional guidance from medical bodies and regional authorities, is likely to shape clinical trust and adoption patterns in the coming years.



Sonia Selletti graduated in law from the University of Pavia in 1991. She was admitted in Milan in 1994. She is a Supreme Court Barrister. After practising international law and after a period as Head of the internal legal office of an Italian pharmaceutical company, in 1995, Sonia joined Astolfi e Associati where she is a Partner and Head of the Life Sciences Group. She has 25 years of expertise in pharmaceutical and health legislation for medicinal products, cosmetics, medical devices and health supplements.
Sonia is a member of the Supervisory Bodies in sanitary and pharmaceutical companies pursuant to Legislative Decree No. 231/2001, aimed at preventing criminal liabilities of corporate entities.
She is the Director responsible for the specialist legal journal *Rassegna di diritto farmaceutico e della Salute*. She has authored various publications on legal topics concerning life sciences.
Sonia collaborates with the University of Pavia in administrative law courses on procedures for the access of medicines to the market. She also provides training courses in the healthcare and pharmaceutical field at CME events for health professionals.

Astolfi e Associati Studio Legale
Via Larga, 8, 20122, Milan
Italy

Tel: +39 02 885 561
Email: sonia.selletti@studiolegaleastolfi.it
LinkedIn: www.linkedin.com/in/sonia-selletti-b25953164



Claudia Pasturenzi graduated in law from the University of Pavia in 2010. She has been a member of the Pavia Bar Association since 2014. Claudia has been working with Astolfi e Associati since 2014 and mainly works in the field of pharmaceutical and healthcare law, in handling questions on the advertising of medicinal products and medical devices, also with regard to new communication channels (social media).
She is a member of the editorial board for the specialist legal journal *Rassegna di diritto farmaceutico e della salute*, as well as the author of several publications.

Astolfi e Associati Studio Legale
Via Larga, 8, 20122, Milan
Italy

Tel: +39 02 885 561
Email: claudia.pasturenzi@studiolegaleastolfi.it
LinkedIn: www.linkedin.com/in/claudia-pasturenzi-687032167



Chiara Screpanti graduated in law from the University of Trento in 2024. Chiara has been working with Astolfi e Associati since 2024 and mainly works in the field of pharmaceutical and healthcare law.
She is a member of the editorial board for the specialist legal journal *Rassegna di diritto farmaceutico e della salute*, as well as the author of several publications.

Astolfi e Associati Studio Legale
Via Larga, 8, 20122, Milan
Italy

Tel: +39 02 885 561
Email: chiara.screpanti@studiolegaleastolfi.it
LinkedIn: www.linkedin.com/in/chiara-screpanti-1600a3317

Astolfi e Associati Studio Legale was founded by Antonio Astolfi in 1955. Fostering his original interest in international trade law, he founded the law journal "*Diritto Comunitario e Degli Scambi Internazionali*" ("*EU Law and International Trade Law*"). Later, in the 1960s, he developed a strong interest in pharmaceutical and health law (life sciences) showing longsighted vision. In 1968, he founded the law journal "*Rassegna di Diritto Farmaceutico*" ("*Pharmaceutical Law*"), still edited today after more than 50 years, in its new version "*Rassegna di diritto farmaceutico e della salute*". This heritage is today the practice area of Astolfi e Associati, deployed from civil, labour, commercial and banking law to pharmaceutical, health and food law, proposing complementary and comprehensive services to clients to fully meet their needs for legal advice. Astolfi e Associati assists Italian and foreign clients in both extrajudicial and judicial matters.

www.studiolegaleastolfi.it

Japan



Masanori Tosu



Kenji Tosaki

Nagashima Ohno & Tsunematsu

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

In Japan, there is no clear legal definition of "digital health". It is generally used as a generic term for products and services related to medicine and healthcare that utilise digital technologies and data.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Regulatory approvals were granted with respect to various software as a medical device ("SaMD"), such as Artificial Intelligence ("AI") programs to assist in the diagnosis of diseases through images and smartphone applications to treat nicotine dependence and hypertension. Such software is being used in medical settings. Also, telemedicine is becoming popular due to deregulation and the difficulty of face-to-face medication during the COVID-19 pandemic. Various wearable devices and smartphone applications for general health promotion purposes outside of medical settings are also widely used.

1.3 What is the digital health market size for your jurisdiction?

We are not aware of any definitive data on the digital health market size in Japan.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

We are not aware of any definitive data on the comparative revenue of digital health companies in Japan.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

We are not aware of any definitive data on the comparative revenue of digital health companies in Japan.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The principal regulatory authorities for the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices ("PMD Act") are the Ministry of Health, Labour and Welfare ("MHLW"), the Pharmaceuticals and Medical Devices Agency ("PMDA") and local governments. The principal regulatory authorities for the Medical and Medical Practitioners Law are the MHLW and local governments. The principal regulatory authority for the Act on the Protection of Personal Information ("APPI") is the Personal Information Protection Commission ("PPC"). The principal regulatory authority for the Fair Competition Code is the Fair Trade Council. The principal regulatory authority for the Act Against Unjustifiable Premiums and Misleading Representations ("AUPMR") is the Consumer Affairs Agency.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The PMD Act applies to digital health devices including programs that meet the following criteria for medical devices: (i) the device falls under the devices listed in the Cabinet Order; and (ii) the purpose of use of the device is the diagnosis, treatment or prevention of diseases or is to affect bodily structures or functions. Class I programs are excluded from the definition of medical device. A regulatory notice issued by the MHLW entitled "Guidelines concerning Applicability of Medical Devices for Programs" provides more detailed criteria, including examples of programs not falling under medical devices. The PMD Act requires, among others, obtaining business licences and marketing authorisation for each product, complying with manufacture and quality control standards and conducting pharmacovigilance activities. In addition, false and exaggerated advertisements and advertisements of unapproved medical devices are prohibited. For the details of the regulations, please see the response to question 2.4.

Consumer healthcare devices or software that fall under the category of medical devices are subject to the regulations under

the PMD Act. Consumer healthcare devices or software that do not fall under the category of medical devices shall not be advertised as if they are intended to diagnose, treat or prevent diseases. In addition, any other advertisements or representations that falsely claim that the products or services are better than they actually are will be in violation of the AUPMR.

Under the Medical Practitioners Act and the Medical Care Act, medical practices such as the diagnosis, treatment and prevention of diseases may only be provided by physicians and other qualified healthcare professionals. In addition, previously, physicians and patients were required to meet face-to-face at medical institutions when providing medical treatment. However, the regulations have been gradually eased and currently, telemedicine services, in which patients are examined, diagnosed and provided with diagnostic results and prescriptions live through ICT devices, are increasingly permitted provided that the various requirements set forth in the "Guidelines for the Proper Implementation of Online Medical Treatment" published by the MHLW are met.

The application of the regulations under the APPI is a key issue with respect to data privacy and data compliance. For the details of the regulations, please see the responses to questions 4.1 through 5.5.

The prohibition of bribery under the Criminal Code is applicable when the physician is a (deemed) public official, and for certain manufacturers and distributors of medical devices, the regulations under the Fair Competition Code prohibit offering premiums (including money and other benefits) to doctors and medical institutions as a means of unfairly inducing them to trade in medical devices.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

As for the medical device regulations, the key enforcement areas are the determination of whether a program qualifies as a medical device and the regulation of device advertisements.

As for the data regulations, the key enforcement areas are the implementation of the necessary procedures for handling healthcare-related information and the implementation of the security control measures therefor, especially at medical institutions.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

In order to market SaMD in the Japanese market, it is necessary to obtain both business licences for the relevant entities/sites and a marketing authorisation for each product. As to the business licence, the company that markets the SaMD must obtain a marketing business licence. In addition, a manufacturing business licence must be obtained for each manufacturing facility and a sales business licence must be obtained for each sales office.

There are two pathways in respect of the marketing authorisation for SaMD products. Marketing Certification is the pathway for Class II or III medical devices for which the MHLW specified and published the evaluation and specification standards. Marketing Approval is the pathway for (a) Class II or III medical devices not subject to Marketing Certification, and (b) Class IV medical devices.

Clinical trials are usually required to be conducted for novel types of SaMD. When conducting clinical trials, medical device good clinical practice must be observed. Recently, the MHLW published evaluation indices for the safety and efficacy of SaMD that induces behavioural changes for disease treatment.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

The regulatory framework is essentially the same as that for SaMD. The MHLW published evaluation indices for the safety and efficacy of medical image diagnosis support systems using AI technology.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

An expert committee at the PMDA has discussed and published a part of recommended methods for the examination of adaptive AI devices that are intended to autonomously change their performance after being marketed. The relevant discussion will continue going forward.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data such as clinical trial data will be a material part of regulatory review for marketing approval for AI/ML-based digital health solutions, the same as other types of medical devices. If a medical device subject to regulatory review is not a noble type of medical device, clinical trial data may not be required.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There is currently no difference in regulations between the national and local levels.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

There is currently no noticeable difference in regulatory enforcement actions to digital health products and solutions.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Please see the response to question 2.1.
- **Robotics**
  If the product falls under medical device, the PMD Act shall apply.

- **Wearables**
  If the product falls under medical device, the PMD Act shall apply.
- **Virtual Assistants (e.g. Alexa)**
  If the product falls under medical device, the PMD Act shall apply.
- **Mobile Apps**
  If the product falls under medical device, the PMD Act shall apply.
- **Software as a Medical Device**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **Clinical Decision Support Software**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **IoT (Internet of Things) and Connected Devices**
  If the product falls under medical device, the PMD Act shall apply.
- **3D Printing/Bioprinting**
  If the product falls under medical device, the PMD Act shall apply.
- **Digital Therapeutics**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **Digital Diagnostics**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **Electronic Medical Record Management Solutions**
  If the product falls under medical device, the PMD Act shall apply.
- **Big Data Analytics**
  If the product falls under medical device, the PMD Act shall apply.
- **Blockchain-based Healthcare Data Sharing Solutions**
  If the product falls under medical device, the PMD Act shall apply.
- **Natural Language Processing**
  If the product falls under medical device, the PMD Act shall apply.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The "Safety Management Guidelines for Providers of Information Systems and Services that Handle Medical Information" issued by the Ministry of Economy, Trade and Industry ("METI") and the Ministry of Internal Affairs and Communications ("MIC") are applicable to providers of medical information systems and services. The guidelines contain stipulations such as the risk management process required upon the provision of medical information systems to medical institutions.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the APPI, personal information can only be used within the scope of the purpose specified in relation to the obtainment of personal information, and the principal's consent is required when such information is used for any other purpose.

In addition, personal information related to medical or health matters falls within the category of sensitive personal information and the consent of the principal is required for the obtainment of such sensitive personal information.

"Anonymously Processed Information" is the information that is processed so that it cannot be restored to re-identify a specific individual, and it is treated as non-personal information to which the above-mentioned limitation on the purpose of use does not apply. "Pseudonymously Processed Information" is the information that is processed so that a specific individual cannot be identified without cross-checking with other information, and it can be used for purposes other than those specified in relation to an obtainment without the principal's consent, provided that the modified purpose is publicly announced. These types of information are expected to be utilised in the fields of medicine and healthcare.

In addition to the APPI, when personal information is obtained and used for life sciences and medicine-related research, regulations based on Ethical Guidelines issued by the Ministry of Education, Culture, Sports, Science and Technology, the MHLW and the METI, such as Institutional Review Boards approval and informed consent, would also apply.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The amendment to the APPI, which integrates national and local government regulations on personal data, came into effect as of April 2023, and there is currently no difference in the regulation of health data use between the national and local levels.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The above-mentioned restrictions under the APPI do not apply to the use of personal information for academic research purposes by academic research institutions, such as universities (including university hospitals). For the difference of the regulation depending on the nature of data, please see the response to question 4.1.

4.4 How do the regulations define the scope of personal health data use?

Apart from certain exceptions stipulated in the APPI, the use of personal information including personal health data is limited to the specified purpose. Exceptions include cases where the use is particularly necessary for the improvement of public health and when it is difficult to obtain the consent of the principal. In a Q&A recently published by the PPC, it was indicated that the use by pharmaceutical companies for the purpose of research on rare diseases or the like may fall within this exception.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

In regard to the securing of comprehensive rights to use

personal information and data, the key point is to define the purpose as broadly as possible in the contract terms and privacy policy. Having said that, according to the guidelines published by the PPC, it is not sufficient to merely specify the purpose of use in an abstract or general manner, instead, it is desirable to specify the purpose in such a way that the principal can generally and reasonably assume the kind of business and the purpose the information will ultimately be used for.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The APPI stipulates that efforts must be made to keep personal data accurate and up to date. The APPI also prohibits the use of personal information in a manner that may encourage or induce illegal or unjustifiable acts, which include the use of personal information to illegally discriminate against a person.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Please see the response to question 5.4.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the APPI, apart from certain exceptions, such as outsourcing or joint use, personal data may not be provided to third parties without the consent of the principal. In obtaining consent for international transfer, information must be provided to the principal in advance regarding the personal data protection system in the country where the third party is located and the measures to be taken by such third party to protect the personal data.

Exceptions include cases where the use is particularly necessary for the improvement of public health and when it is difficult to obtain the consent of the principal. In a Q&A recently published by the PPC, it was indicated that the provision to pharmaceutical companies for the purpose of research on rare diseases or the like may fall within this exception.

Anonymously Processed Information may be provided to third parties without the consent of the principal, whereas the provision of Pseudonymously Processed Information to third parties is prohibited.

When providing personal data to a third party outside Japan, apart from certain exceptions, it is necessary to obtain consent from the principal even in the case of outsourcing or joint use.

The regulations based on Ethical Guidelines may also apply in the domains of life sciences and medicine-related research.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There is currently no difference in regulations between the national and local levels. Please see the response to question 4.2.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The above-mentioned restrictions under the APPI do not apply to the provision of personal data to academic research institutions or provision by academic research institutions to a third party for academic research purposes. For the difference of the regulation depending on the nature of data, please see the response to question 5.1.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Under the APPI, the provision/sharing of medical information to a third party (such as provision by a medical institution to a pharmaceutical company) requires the opt-in consent of the principal. However, the Next Generation Medical Infrastructure Act ("NGMIA") allows an opt-out process instead of opt-in consent for the collection and provision by a medical institution of medical information to a certified entity performing anonymous processing of medical information to enhance the utilisation of Anonymously Processed Information in medical fields. Since the 2023 amendment to the NGMIA, a similar regime also applies to Pseudonymously Processed Information in medical fields. It is expected that, in some respects, Pseudonymously Processed Information, where the deletion of outlier information is not required upon processing, may be more useful than Anonymously Processed Information in medical fields.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

In principle, healthcare data itself constitutes personal information and when such data is to be shared, the consent of the principal is required under the APPI. Even in respect of federated learning, where only parameters and/or learned models excluding personal information are to be shared with third parties, it is necessary to confirm whether the use of healthcare data for federated learning will be within the purpose of use that was presented to the principal.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under the Patent Act of Japan, inventions are classified into three categories: an "invention of a product"; an "invention of a method"; and an "invention of a method for producing a product". To obtain patent protection for digital health technologies, one can either seek patent protection for a system or program that utilises digital health technologies as an "invention of a product" or seek patent protection for information processing or services that utilise digital health technologies as an "invention of a method". In the case of an invention of a product, to act in such a way as to constitute direct patent infringement is to produce, to use, to "Assign, etc." (i.e. to assign or to lease, including, in the case where the product is a computer program, to provide through an electrical communication line), to export, to import or to offer to "Assign, etc." the product as part of one's business. For an invention of a method, on the

other hand, to act in such a way as to constitute direct patent infringement is to use the method as part of one's business. In the case of an invention of a method for producing a product, to act in such a way as to constitute direct patent infringement is to use the method as part of one's business or to use, to "Assign, etc.", to export, to import or to offer to "Assign, etc." the product produced by the method as part of one's business. When the allegedly infringing product or method meets all the elements of the patented invention, the above-mentioned acts constitute acts of literal patent infringement. Even when a part of a patent claim does not correspond to the allegedly infringing product and the product does not literally fall within a patent claim, the scope of protection of the patent claim extends to the product under the doctrine of equivalents if (i) the non-corresponding part is not the essential part of the patented invention, (ii) the purpose of the patented invention can be achieved by replacing this part with a part in the product and an identical function and effect can be obtained, (iii) a person skilled in the art could easily come up with the idea of such replacement at the time of the production of the product, (iv) the product is not identical to the technology in the public domain at the time of the patent application or could have been easily conceived at that time by a person skilled in the art, and (v) there were no special circumstances such as the fact that the product had been intentionally excluded from the scope of the patent claim in the course of the prosecution. A patent owner can seek injunctive relief and/or compensation against an infringer through court proceedings.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Software, screen displays and instruction manuals used in digital health technologies may be eligible for copyright protection. A copyright includes a right of reproduction, a right of stage performance, a right of musical performance, a right of on-screen presentation, a right of transmitting to the public, a right of recitation, a right of exhibition, a right of distribution, a right of transfer, a right to rent out and a right of adaptation. A copyright owner can seek injunctive relief and/or compensation against an infringer through court proceedings.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Information used or generated by businesses utilising digital health technologies may be protected as trade secrets. In general, the wrongful acquisition, use and disclosure of "Trade Secrets" are regarded as "Unfair Competition" under the Unfair Competition Prevention Act of Japan ("UCPA"). "Trade Secrets" are defined as "technical or business information useful for business activities, such as manufacturing or marketing methods, that are kept secret, and are not publicly known". A person who wrongfully acquired, used or disclosed "Trade Secrets" may be enjoined from using and/or disclosing the "Trade Secrets" and/or be held liable for damages by the court under the UCPA.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Technology licensing organisations ("TLOs") are organisations that transform the results of research by university researchers into patents and transfer the results to private companies. TLOs can submit plans for the implementation of their technology transfer businesses to the Ministry of Education, Culture, Sports, Science and Technology and the METI and seek their approval. Approved TLOs will be eligible for a discount of annual patent fees. Further, when approved TLOs take out a loan for their approved businesses, an Incorporated Administrative Agency will guarantee the debts incurred by these TLOs.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

An invention of software can be patented. If an invention of software to be used for a medical device is patented, the scope of patent protection is the same as that for other patents. Please see the response to question 6.1 on the general scope of patent protection. Further, software can be considered as works of computer programming under the Copyright Act of Japan. The scope of copyright protection for works of computer programming is the same as that for other works. Please see the response to question 6.2 on the general scope of copyright protection.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No, an AI device cannot be considered an inventor of a patent under Japanese law. Under Japanese law, only a "person" can own a right and an AI device is not a "person". As an AI device cannot own a right to obtain a patent, an AI device cannot be named as an inventor. On May 16, 2023, in the litigation where the applicant of a patent application for an invention titled "Food Container and Devices and Methods for Attracting Enhanced Attention" allegedly autonomously generated by an AI device called "DABUS" sought the revocation of the dismissal of the patent application by the Commissioner of the Japan Patent Office, the Tokyo District Court dismissed the action, holding that an "inventor" is limited to natural persons. The applicant filed an appeal, and on January 30, 2025, the Intellectual Property High Court ("IPHC") affirmed the judgment by the Tokyo District Court.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The scope of intellectual property ("IP") rights provided to the government for government-funded inventions is the same as that for other inventions. With respect to certain IP rights that are associated with the results of government-contracted research and development, or of government-contracted software development, the national government may decide not to acquire such rights in a situation where the contractor promises that (i) if such results have been obtained, the contractor will report them to the national government without delay, (ii) the contractor will grant the national government the right to use such rights free of charge if the national government requests the contractor to do so while making it clear that the reason for doing so is that it is particularly necessary for the sake of the public interest, (iii) the contractor will grant a third party the right to use such rights if the contractor has

not used such rights for a considerable period of time and does not have a legitimate reason for not having used such rights for a considerable period of time, and if the national government requests the contractor to do so while making it clear that the reason for doing so is that it is particularly necessary to facilitate the use of such rights, and (iv) when intending to transfer such rights, the contractor will obtain the approval of the national government in advance.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

In providing services utilising digital health technologies, servers located outside of Japan may be used. In such cases, the territoriality of IP rights can be an issue. With respect to the principle of territoriality, the Supreme Court rendered two judgments addressing this issue on March 3, 2025. In one case, the patentee of a patent covering an invention of a program titled "Display Device, Method of Displaying Comments, and Program" sued defendants who transmitted their program from a server located in the United States to users in Japan. Article 2(3)(i) of the Patent Act of Japan sets forth the definition of "working" of an "invention of a product" and pursuant to that definition, in the case of an invention of a program, "providing through a telecommunication line" is included in "working". On July 20, 2022, the IPHC held that in the case of an invention of a program that may be transmitted via a network, "an act of transmitting a program can be considered to constitute 'providing' under the Patent Act of Japan when such transmission can be evaluated as having been performed within the territory of Japan from a substantive and overall perspective". The Supreme Court found that the transmission was performed as part of the information processing activities when providing the services in Japan; the transmission ensured that the effect of the patented invention was obtained at terminals located in Japan, and in relation to obtaining the effect, the fact that the location of the server is outside of the territory of Japan has no particular significance, and it could not be said that the transmission had no economic impact on the patentee, and held that the act of transmitting the program fell under "providing through a telecommunication line". In the other case, the patentee of a patent covering an invention of a system titled "Comment Delivery System", which is the plaintiff in the first case, sued defendants who transmitted files used for the defendants' services from a server located in the United States to user terminals in Japan, which are the same defendants as in the first case. Pursuant to the definition of "working" set forth in Article 2(3)(i) of the Patent Act of Japan, "producing" is included in "working". On May 26, 2023, the IPHC held that even if a server, which is part of the components of a network-type system, is located outside Japan, newly producing that network-type system constitutes the act of "producing" under Article 2(3)(i) of the Patent Act of Japan when such production can be considered to have been performed within the territory of Japan. The Supreme Court found that making of the system by the transmission was performed as a part of the information processing when providing the services in Japan; the transmission made the system containing terminals located in Japan and ensured that the effect of the patented invention was obtained at terminals located in Japan, and in relation to obtaining the effect of the system, the fact that the location of the server is outside of the territory of Japan has no particular significance, and it could not be said that the transmission and the system made as a result had no economic impact on the patentee, and held that the act of making the system fell under "producing". The rulings in these two judgments are highly fact-specific, but they have significant influence on other potential cases where the territoriality of patents is at issue.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

In general, when conducting collaborative development or improvements, it is important to stipulate in the contract, among others, the roles and cost allocation of each party, the rights and licence of the deliverables, and the confidentiality obligation. If the rights of one party are restricted during and after the collaboration (e.g., restriction on a similar development), antitrust issues may arise. When collaborating with academia, compensation for non-execution and publication procedure may also be negotiation points.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Although there is nothing special to note, it would be helpful to note that healthcare companies are highly regulated and the contents of agreements may be affected by applicable regulations.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

The purpose of use of the AI models provided by AI developers to the data holders should be limited to the purpose of federated learning. In addition, it would be preferable for the AI developers not to limit the purpose of use of the learned AI models provided by such data holders to such AI developers to the extent possible in order to eliminate restrictions on business development. It would also be important to provide representations, warranties and covenants regarding compliance with data privacy regulations.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

It should be noted that, if the personal information to be used by a generative AI contains sensitive information such as medical data, the consent of the principal is required to obtain and provide such data to a third party under the APPI. In addition, since the output from the generative AI cannot be controlled in principle, it would be necessary to take care in respect of the risk of the output rising to a level where it would constitute a diagnosis, which could lead to issues regarding the generative AI unintentionally constituting a medical device and/or medical service.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is no regulatory authority that is comprehensively in charge of regulations related to AI/ML in Japan and the governmental agencies that oversee each industry are in the process of organising their respective policies and guidelines on AI/ML-related regulations.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Please see the responses to questions 2.4 to 2.7.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

If there is no active human involvement in the software development at all, no IP rights will arise. However, if the development of the software falls under the act of "adaptation" of an original work, the copyright holder of the original work holds rights on the developed software including the right of reproduction, the right of transmitting to the public and the right of adaptation. This means that, for example, the developed software cannot be reproduced without obtaining a licence from the copyright holder of the original work.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

In transactions of licensing data, the following issues should be considered: (i) rights to deliverables; (ii) liability for defective data; (iii) losses derived from licensed data; and (iv) limitations on the purposes of use.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

There is currently no specific difference in regulations between standard AI and generative AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Among the various issues, the issues under the Copyright Act and the APPI are important. The issues under the Copyright Act include (i) whether a copyright infringement occurs when a generative AI uses a work for learning, (ii) the risk of an AI-generated product infringing on a third party's copyright, and (iii) whether the AI-generated product itself constitutes a copyrighted work. The various discussions related thereto are ongoing. With respect to the APPI, it is important to check whether the principal consented to certain uses of personal information by a generative AI for learning. It is also important to check whether the input of prompts containing personal information into a generative AI constitutes (a) a purpose other than those that were presented to the principal, or (b) the provision of such personal information to a third party (in both cases (a) and (b), the principal's additional consent is required). The PPC has issued a warning related thereto.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

While there is no clear precedent to date, such disgorgement by trained AI/ML models without appropriate data rights may constitute a violation of the APPI.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

In general, liability can arise in tort (either under the Civil Code or under its special law, the Product Liability Act ("PLA")) or under contract. Since "products" for which a claim under the PLA can be asserted are limited to movable property, a claim based on the PLA cannot be filed for an adverse outcome caused by programs unless there exists a device in which such program is incorporated and a defect in the program leads to a defect in the device itself.

An administrative notice recently issued by the MHLW provides that even when a patient is treated using a program that provides AI-based diagnosis and treatment support, the physician is responsible for the final decision for those acts.

9.2 What cross-border considerations are there?

Under the conflicts of laws principle in Japan, the governing law of a tort is the law of the place where the adverse consequence of the tortious act occurred. On the other hand, the parties' agreement takes precedence over the decision of the governing law of the contract.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

It would be advisable to include provisions regarding limitation of liability in the terms and conditions for the use of the generative AI. It would also be advisable to include appropriate disclaimers to avoid any misunderstanding about the nature of the subject device/service for digital health solutions using a generative AI.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Misuse of healthcare data may constitute a violation of the APPI and a civil tort that would result in damage compensation liability.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The PMD Act regulations of SaMDs would apply to the medical programs provided in a form that allows only the right to use the program in the Cloud without transferring ownership of the program.

In addition, providers of Cloud-based services that handle medical information would be subject to the METI/MIC guidelines described in the response to question 3.2.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

When entering the digital health product market, whether the PMD Act is applicable or not is the key issue. When entering the digital health service market, it is necessary to keep in mind that private companies are not allowed to provide services that fall under medical practice.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

As the healthcare sector, including digital health, is highly regulated, it is advisable for venture capital and private equity firms to conduct due diligence carefully, especially on regulatory and compliance matters. In addition, as IP would be a key asset for digital health ventures, it is also advisable to carefully examine IP-related matters in due diligence.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barrier is the low predictability of applicable regulations regarding medical devices and medical practice. The MHLW is working to ensure the foreseeability of the applicability to medical device regulation to programs by establishing a consultation service and publicising consultation cases.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The clinician certification body in Japan is the MHLW. Having said that, the Japan Medical Association, a voluntary membership organisation for medical doctors, may have a certain influence on the policy making regarding the clinical adoption of digital health solutions.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Digital health solutions may be reimbursed under the National Health Insurance ("NHI") system. To be eligible for reimbursement, a digital health solution provider needs to apply to the MHLW for inclusion on the NHI Price List and to undergo a review process by the MHLW.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

When conducting due diligence on the digital health solution, especially data-driven products such as AI/ML-based solutions, it is crucial to review the subject products not only from the pharmaceutical/medical regulation perspective but also from the data privacy/protection regulation perspective.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

As the next amendment to the APPI is currently being discussed, it is necessary to closely monitor how it will affect the digital health field.



Masanori Tosu is a partner at Nagashima Ohno & Tsunematsu. He provides services in a wide range of matters, including mergers and acquisitions, licensing, collaborative research and development, and various other transactions, as well as regulatory and governmental affairs, for clients both inside and outside Japan, with a focus on the life science, pharmaceutical and healthcare fields.
He also worked for the Ministry of Health, Labour and Welfare (MHLW) from 2019 to 2021. While at the MHLW, he was involved in various life science and healthcare-related policies and administrative actions and, among others, in various measures taken by the Japanese government to the COVID-19 pandemic.

Nagashima Ohno & Tsunematsu
JP Tower
2-7-2 Marunouchi, Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 3 6889 7245
Email: masanori_tosu@noandt.com
URL: www.noandt.com/en/lawyers/masanori_tosu



Kenji Tosaki is a partner at Nagashima Ohno & Tsunematsu. His practice focuses on dispute resolution. He specialises in IP litigation and complex commercial litigation, and he also covers the area of TMT, including data protection matters.
In the area of IP litigation, he handles both IP infringement litigations and IP invalidation litigations before the IP High Court, the Supreme Court, District Courts and the Japan Patent Office. His IP expertise includes a wide variety of IP matters (patents, copyrights, trademarks, design rights, unfair competition and trade secrets) in many areas, such as telecommunications, electronics, social games and pharmaceuticals. He also provides pre-litigation counselling, including infringement/invalidity analysis.
In the area of complex commercial litigation, he gives advice on matters such as securities law and cross-border contracts.

Nagashima Ohno & Tsunematsu
JP Tower
2-7-2 Marunouchi, Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 3 6889 7206
Email: kenji_tosaki@noandt.com
LinkedIn: www.linkedin.com/in/kenji-tosaki-8b084311

Nagashima Ohno & Tsunematsu, based in Tokyo, Japan, is widely recognised as a leading law firm and one of the foremost providers of international and commercial legal services. In representing our leading domestic and international clients, we have successfully structured and negotiated many of the largest and most significant corporate, finance and real estate transactions related to Japan. The firm has extensive corporate and litigation capabilities spanning key commercial areas such as antitrust, intellectual property, labour and taxation. We are known for path-breaking domestic and cross-border risk management/corporate governance cases, such as fraud investigations and white-collar criminal defence, and for handling insolvency and restructuring proceedings including large-scale corporate reorganisations. In order to deliver optimal service and value to our clients, the over 600 lawyers of the firm, including about 50 experienced lawyers from various jurisdictions outside Japan, work together in customised teams to provide the expertise and experience specifically required for each client matter.
The firm has a vast network of relationships with foreign companies and law firms that provide it with a unique perspective when representing clients in international deals. Our overseas network includes locations in New York, Shanghai, Singapore, Bangkok, Ho Chi Minh City, Hanoi, Jakarta* and London. The firm also maintains collaborative relationships with prominent local law firms across Asia and other regions. We regularly advise on and coordinate complex cross-border matters across multiple Asian jurisdictions. As a pioneering Japanese law firm with an established presence in New York, we are significantly and rapidly expanding our activities in the United States, across the Americas, and in Europe. The firm strives to meet the needs of both its international clients operating in Japan and Asia and its domestic clients operating outside Japan or seeking to expand their operations overseas.
(*Associate office)

www.noandt.com

NAGASHIMA

Korea


Jin Hwan Chung


Eileen Jaiyoung Shin


Sungil Bang

Lee & Ko

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

No statutory definition has yet been established. However, "digital health" is generally understood as the combination of healthcare services and information and communication technology, which includes telemedicine, mobile health, health information technology and hospital digitalisation systems, such as electronic medical records (EMRs) and electronic health records (EHRs).

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Beyond traditional PACS and EMR systems, the most prominent emerging areas include digital therapeutics (DTx), generative AI-based medical services, remote patient monitoring, health-data brokerage, cloud-based transitions of hospital information systems (HIS, PACS, LIS), and integrated healthcare platforms that connect medical institutions with wearable devices. Notably, insomnia-treatment apps (such as Somzz and WELT-I) have received regulatory approval for the first time and are now being prescribed, and LLM-based medical-record summarisation and diagnostic-support solutions are also gaining rapid traction.

1.3 What is the digital health market size for your jurisdiction?

No official data is available. However, according to the *2023 Korea Digital Healthcare Industry Survey* published by the Korea Digital Health Industry Association on February 25, 2025, the total revenue of the domestic digital healthcare industry was reported to be KRW 6.493 trillion (approximately USD 4.81 billion; 1 USD = 1,300 KRW).

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

There is still no official ranking data available. However, based on revenue size, major players are generally considered to include EMR companies such as UBicare and BIT Computer, as well as publicly listed medical AI companies such as VUNO and Lunit.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

No official data is available.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

With the full implementation of the Digital Medical Products Act on January 24, 2025, the Ministry of Food and Drug Safety (MFDS) has become the primary regulatory authority overseeing all digital health products. The MFDS exercises review and supervisory authority across the entire lifecycle – covering approval and certification, clinical trial authorisation, manufacturing and quality control, modification control for AI-based products, and post-market surveillance – for product groups that have now been clearly reclassified, such as digital medical devices, digital-convergence pharmaceuticals, and digital medical/health-support devices.

The Ministry of Health and Welfare (MOHW) effectively determines whether a technology can be used clinically through the new health technology assessment (nHTA) and decisions on national health-insurance coverage and non-coverage. It also determines whether a digital health service constitutes a medical act under the Medical Service Act.

The Health Insurance Review & Assessment Service plays a practical gatekeeping role by conducting reimbursement assessments, coding, and post-market monitoring, all of which significantly influence market access.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The MFDS has authority over regulatory approval of medical devices, AI, generative AI, SaaS, SaMD and combination products. However, obtaining regulatory approval from the MFDS does not necessarily mean that the digital health technology can immediately be used in medical settings. Certain new digital health technologies are required to undergo the nHTA under the Medical Service Act (enforced by the MOHW) before being used at medical sites. Furthermore, as explained in

question 2.1 above, approval from the MOHW is required for national medical insurance reimbursement eligibility.

The Personal Information Protection Act (PIPA), which imposes strict data privacy protection obligations, plays an important role in the digital health field. In developing and providing digital health services to customers, it is necessary for a manufacturer or service provider to have access to patients' health data without violating the data privacy regulations in Korea; however, these restrictions are not easy to fully comply with from the industry's perspective.

If a digital health product is classified as a medical device under the Medical Devices Act or a drug under the Pharmaceutical Affairs Act, anti-kickback restrictions, which prohibit a manufacturer, importer or distributor of medical devices or drugs from providing economic value to healthcare professionals for the purpose of promoting medical devices or drugs, will apply as well.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The most critical area of enforcement is the implementation of the Digital Medical Products Act, which took effect on January 24, 2025. Regulators are focusing on clearly reclassifying previously ambiguous product categories into digital medical devices, digital-convergence pharmaceuticals, and digital medical/health-support devices, and on establishing category-specific approval and post-market oversight systems.

An emerging enforcement area is the Act on Fostering the AI Industry and Establishing a Trust-Based AI Environment (AI Framework Act), scheduled to take effect in 2026. The Act defines "high-impact AI" as AI systems that may significantly affect human life, physical safety, or fundamental rights, and it imposes heightened obligations on high-impact AI operators, including establishing and publishing risk-management plans, conducting impact assessments, and maintaining documentation supporting their mitigation measures.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Essentially, market authorisation must be obtained from the MFDS under the Digital Medical Products Act. Furthermore, even after obtaining market authorisation, to be used in medical settings, the product must undergo administrative procedures related to national health insurance reimbursement coverage.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Please refer to the response for question 2.4.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

The MFDS, which holds the authority for market authorisation, continues to update its regulations and guidelines related to approvals in order to reflect advancing technologies.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

The role of clinical validation data in the regulation of AI/Machine Learning (ML)-based digital health solutions is crucial, as it is considered a key element in ensuring the safety and efficacy of the technology. In Korea, such clinical validation data serves as an important criterion in the regulatory approval process.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Korea, digital health products and solutions are regulated at the national government level.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Please refer to the response for question 2.6.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Korea's Medical Service Act had, in principle, prohibited telemedicine. However, during the COVID-19 pandemic, limited telemedicine was temporarily permitted, and even after the pandemic ended, it continued to be allowed on a restricted basis through a pilot programme. With the National Assembly's passage of the Medical Service Act amendment on December 2, 2025, telemedicine is now formally permitted on a limited basis. Telemedicine is principally limited to clinic-level medical institutions, and a prior in-person clinical record is generally required.
- **Robotics**
  Robotic surgery equipment is widely used in Korea; however, as far as digital health is concerned, no significant issues are being discussed.
- **Wearables**
  Many wearable devices are introduced in Korea as wellness products or medical device products, the latter of which will require MFDS's market approval. As medical services can be provided only by healthcare professionals under the Medical Service Act, wearable devices are not permitted to provide information or services that can be deemed medical services as defined by relevant Supreme Court precedents. In this regard, the MOHW provides guidelines on the health information that can be provided through wearable devices.
- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants draw relatively less attention in Korea; however, similar issues as in the case of wearable devices can apply.
- **Mobile Apps**
  Mobile apps are one of the hottest areas in Korea, and the MFDS has established the Safety Management Guideline for Medical Mobile Apps in this regard.

- **Software as a Medical Device**
  Software-based medical devices are classified as "digital medical devices" under the Digital Medical Products Act and are subject to a separate approval and review framework. A key regulatory issue in this area is cybersecurity. Because of the inherent risk of hacking or data manipulation in software products, the MFDS requires strict compliance with security standards, such as communication security and data encryption, at the approval and review stage.
- **Clinical Decision Support Software**
  A significant portion of software-based medical devices approved by the MFDS fall under clinical decision support software. The key regulatory issue in this area is determining whether a product qualifies as a medical device. Under MFDS guidelines, software that merely provides simple medical information retrieval or general medical knowledge is not considered a medical device. However, software that analyses a patient's biometric signals or medical images to predict the presence or status of a disease or to suggest treatment directions is classified as a medical device.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  AI/ML-powered digital health solutions can also require MFDS's market approval if the product is deemed a medical device. According to the MFDS guideline, AI-based medical imaging software that can be deemed a medical device are as follows: (i) those that analyse medical data to diagnose, predict, monitor or treat diseases; and (ii) those that analyse medical data to provide clinical information necessary for the diagnosis or treatment of a patient.
- **IoT (Internet of Things) and Connected Devices**
  There are no specific guidelines regulating IoT and connected devices in the digital health field. However, given the nature of these technologies, more emphasis may be imposed on the protection of personal data.
- **3D Printing/Bioprinting**
  The government classifies 3D printing/bioprinting as one of the innovative medical devices under the Act on Nurturing the Medical Devices Industry and Supporting Innovative Medical Devices.
- **Digital Therapeutics**
  The Digital Medical Products Act systematically manages the safety and efficacy of DTx and outlines measures to support market entry and commercialisation.
- **Digital Diagnostics**
  In the field of digital diagnostics, such as radiology and electrocardiography, numerous products have been developed and received approval from the MFDS. However, these products are not intended to replace the judgment of a physician but have received approval as items that assist in the physician's judgment.
- **Electronic Medical Record Management Solutions**
  The most significant recent development in the EMR sector is the integration of voice AI and generative AI. "Voice EMR" solutions – systems that convert physician–patient conversations into text (STT) and use LLMs to summarise the content into standard medical-record formats – are currently being developed and deployed.
- **Big Data Analytics**
  Under the "pseudonymised information"-related provisions of the PIPA, pseudonymised medical data may be used without the data subject's consent for purposes of statistical analysis, scientific research, and public-interest record preservation. The government has issued the Healthcare Data Utilization Guidelines outlining safe pseudonymisation procedures, and initiatives such as K-CURE, which provides access to public medical datasets including cancer data, are actively underway.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain technology is gaining attention in Korea for its potential to enhance interoperability of EMRs and the security capabilities of healthcare data. However, there are no specific regulations governing its use as of now.
- **Natural Language Processing**
  No particular development has been made from a regulatory or governmental policy perspective.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The most critical issue is whether a digital healthcare platform's activities conflict with the prohibition on for-profit patient solicitation or inducement under Article 27(3) of the Medical Service Act. If a digital health platform recommends specific hospitals to patients or receives fees in connection with appointment booking, there is a significant risk that such conduct will be deemed unlawful.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In Korea, personal health data is classified as sensitive information under the PIPA, and therefore strengthened protection measures and heightened consent requirements apply across all stages of collection, use, and disclosure. Pseudonymised data may be used without consent for research and statistical purposes, but safeguards to prevent re-identification and the use of an accredited data-combination institution are mandatory. Medical records held by healthcare institutions are subject to confidentiality and retention obligations under the Medical Service Act, and explicit patient consent is required before such records may be provided externally. In addition, genetic information is regulated under the Bioethics and Safety Act and typically requires Institutional Review Board (IRB) approval for its collection or use.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There is comprehensive regulation at the national government level.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The regulation of personal health data usage varies depending on the nature of the data (e.g., sensitive information,

pseudonymised information) and the entities handling it (e.g., medical institutions, corporations). Personal health data classified as sensitive information is strictly protected under the PIPA and the Medical Service Act, requiring patient consent for external provision by medical institutions. Pseudonymised information can be used for research or statistical purposes without consent, but security measures are required to prevent re-identification.

4.4 How do the regulations define the scope of personal health data use?

The scope of personal health data usage is defined through various laws and guidelines, such as the PIPA, the Medical Service Act and the Bioethics Act. Emphasis is placed on balancing secure data utilisation with the protection of data subjects. For detailed information, please refer to the response for question 4.1 above.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

It is necessary for a researcher or a company to collect patients' health/medical data to develop new digital health technology. In this regard, the condition and extent of the collection and use of pseudonymised or anonymised personal data has become one of the key issues.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The current PIPA and relevant laws do not stipulate explicit regulations with respect to data inaccuracy, bias and/or discrimination.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Safe collection and use of personal health data are supported through laws such as the PIPA and the Medical Service Act, as well as the My Healthway platform (government-initiated health data platform) and healthcare data utilisation guidelines. Focus is put on striking a balance between data protection and promoting research.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In Korea, personal health data is classified as sensitive information under the PIPA, and data sharing is generally categorised into either third-party provision or outsourcing. Third-party provision requires the data subject's explicit consent, and the consent form must specify the recipient, purpose of use, data items provided, and retention period. For outsourcing, a written contract and appropriate management and supervisory measures are required.

With the expansion of the government's healthcare data-utilisation policy in 2025, the use of pseudonymised data, data combination, and joint use for research and statistical purposes have been increasing. Pseudonymised health data may be shared without consent only for statistical, research, or public-interest purposes, although strict conditions apply, including re-identification prevention measures, use of an accredited data-combination institution, and enhanced security requirements. In addition, unless the data subject has consented, the overseas transfer of pseudonymised health data is, in principle, not permitted.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal health data sharing is regulated under unified laws and regulations at the national government level.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Regulations governing the sharing and utilisation of personal health data vary depending on the entities handling the data (e.g., medical institutions, corporations) and the nature of the data (e.g., patient data, pseudonymised data). Medical institutions, under the Medical Service Act, cannot provide data to third parties without patient consent, and the use of data for research purposes requires approval from an IRB. Companies may utilise pseudonymised data under the PIPA, but its use is often restricted to research and public interest purposes rather than commercial objectives.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please refer to the responses for questions 4.1, 5.1 and 5.3 above.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

While patient medical and health data are strictly protected under the Medical Service Act and the PIPA, technological advancement and the shift in healthcare focus from treatment to health management and preventive care, along with the emphasis on precision medicine, have raised awareness of the need for healthcare data sharing. Accordingly, the MOHW and the Korea Health Information Service are developing a Korea-specific technical standard (KR Core) based on Fast Healthcare Interoperability Resources and promoting integration with EMR and personal health record systems to support domestic standardisation. In response to these societal changes, the government is formulating and implementing policies as explained above.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under the current Korean Patent Act, in principle, medical practices cannot be patented due to their industrial use not being recognised for public policy reasons. It is considered that medical practices should contribute to the sustention of life and well-being of humanity rather than being protected by patent rights for the promotion of intellectual property interests of specific persons.

For example, an invention that has the human body as a direct component, such as a surgical method, treatment method or diagnostic method, is not recognised as an industrial use invention (provided, however, the mode of operation or method of measurement of a medical device, which does not use the interaction with the human body or a particular medical practice as its component, may be protected by patent rights as its industrial use will be recognised). As an exception, in the case of a medical practice in which the human body is an indirect component or a non-medical practice in which the human body is a direct component, then industrial applicability is recognised and a patent may be obtained.

In the case of software, patent protection is applicable only when the information processing carried out by the software is concretely realised using hardware. Patent protection in this case can cover the information processing system that operates with the software, the method of operation, a computer-readable medium containing the subject software, and the program stored on the medium.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

For digital health solutions, the software may be protected as copyright or the database itself may be protected under copyright if it meets the requirements for a database under the Copyright Act (a compilation that systematically arranges or organises materials so that the particular materials may be accessed or searched). Copyright under the Korean Copyright Act arises from the time its subject is created and does not require any separate procedures or formalities. However, copyright registration has its benefits as it is presumed that the work was created and made public at the time of copyright registration, the registered author is presumed to be the true author, and the person who infringes upon a registered copyright is presumed negligent in the act of infringement. Thus, copyright registration makes it easier to prove infringement in case of a dispute, and it is relatively easier to protect against infringement even after the author's death. The duration of a copyright continues through the life of the author and for a period of 70 years after the author's death.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

According to the Korean Unfair Competition Prevention and Trade Secret Protection Act, three conditions must be met in order to be protected as a trade secret: (i) non-disclosure; (ii) manageability of confidentiality; and (iii) usefulness. Non-disclosure means that the content of the information is not publicly known. Confidentiality means that such information must be managed and kept by the holder of said information in confidence. Usefulness means that the information must be useful and hold independent economic value. Meanwhile, even if a trade secret is protected, unlike with patents, there is no effect of excluding a third party from independently developing and using such trade secret.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

The Technology Transfer and Commercialisation Promotion Act applies to, or regulates the transfer of technology developed by academic institutions. According to Article 2(2) of the Act, technology transfer includes the transfer of technology from the technology holder to others through means of transfer, licensing, technical advice, joint research, joint venture, or merger and acquisition. Academic institutions often conduct research by receiving research and development funding from the government, and in such cases the state or public institution will make efforts to secure intellectual property rights for the results of such research. In such situations, the state or public institution may vest the results to the joint research institution, and may even grant permission for its use to a third party for a royalty.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Medical device software in itself cannot be protected by a patent, but information processing devices (e.g., medical devices) that operate in conjunction with medical device software, the method of operation, and medical device software saved onto storage devices can be protected by a patent. In addition, medical device software may also be protected as a copyright.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

According to Article 33(1) of the Patent Act, those eligible to receive a patent are limited to "natural persons" who have made the invention or their successors. Since AI does not belong to the category of natural persons, the general principle, which is recognised by the court as well, is that AI cannot be recognised as the inventor for the purpose of obtaining a patent.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

In Korea, the National Research and Development Innovation Act regulates inventions and results of research conducted through government funding. This statute and its subordinate regulations regulate the ownership, management and utilisation of inventions and other output (including software, products and publications, as well as intellectual property rights such as patents) developed with support from the government. A research and development institution that generates profits from the outcome of such research and development must pay a certain percentage of the amount of profits to the state.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Key examples include the precedent described in question 6.6 above, where AI was not recognised as an inventor, and cases where the Patent Office and related industries established patent examination guidelines to keep pace with the rapid growth of digital healthcare technologies. These include efforts to prepare and discuss specific guidelines for drafting specifications and defining the scope of rights.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Two things may be taken into consideration with priority: (1) to whom an intellectual property belongs; and (2) the method of profit sharing.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

There is no general rule; however, it would be helpful to consider the following: (1) non-healthcare companies may not have an understanding of the applicable regulatory scheme (e.g., the requirements under the Medical Service Act); and (2) medical institutions are not permitted to conduct for-profit activities in principle under the Medical Service Act.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

As explained above, under the current PIPA, data sharing is permissible only for the purposes of statistical compilation, scientific research and public interest record preservation. Furthermore, to engage in data sharing, one must go through the procedures set forth by the PIPA, such as internal review processes within the institution that holds the information.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

As explained in question 2.3, the AI Basic Act passed the National Assembly plenary session on 26 December 2024. Korea is the second country in the world to establish a basic law on AI. The potential impact of the Enforcement Decree of the AI Basic Act, which has been publicly notified in draft form, should also be carefully analysed.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

The main regulatory authorities enforcing AI/ML-related regulations and their scope of enforcement are as follows, and these organisations collaborate to establish a balanced regulatory system that ensures the safety and ethical use of AI technologies while also supporting industry growth.

The Ministry of Science and ICT:

- leads the advancement of AI technology through the AI Basic Act (scheduled for implementation in 2026);
- defines high-impact AI and generative AI as regulatory targets, establishes obligations for transparency and safety, and outlines the responsibilities of operators;
- supports AI safety and reliability verification and certification; and
- formulates a National AI Master Plan every three years and promotes the AI ecosystem, including the development of AI data centres and clusters.

The MFDS:

- pursuant to the Digital Health Products Act, is responsible for the approval, review, quality management and clinical trial approval of AI-based medical devices; and
- supports ongoing updates through AI medical device change management plans and evaluates the safety and effectiveness of medical devices.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

As described in question 8.1 above, the AI/ML-related regulatory framework in Korea is built around the AI Basic Act and the Digital Health Products Act.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under the current Korean Patent Act, the inventor is limited to natural persons. Under the current Korean Copyright Act, in principle, authors are limited to natural persons, but corporations and organisations can also become authors as exceptions.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Various commercial considerations should be taken into account when licensing data for ML. In such cases, ML is not to produce output by using the data itself, but to produce an algorithm or model that is output through training by using

the data, thus the fact that this is different from conventional methods of data usage should also be considered.

For example, the method of using the data, the scope of the data provided, the type of data and its content, the form of data, and the extent to which the data is used (including temporal, regional and human scope), the right to products of ML using the data, and the right to sublicense should all be considered.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

The AI Basic Act, scheduled to take effect in 2026, provides a clear legal distinction between "generative AI" and general AI systems. General AI is defined as an electronic implementation of intellectual abilities possessed by humans, such as learning, reasoning, perception, judgment, and language comprehension. In contrast, generative AI is defined as an AI system that generates text, sound, images, video, or other types of outputs by mimicking the structure and characteristics of input data.

Generative AI operators are required to clearly indicate to users that the output has been generated by AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

The AI Basic Act requires that when an AI business operator provides products or services based on generative AI, they must notify users in advance that the product or service is operated using generative AI. Additionally, the AI business operator must indicate that the outcome of the product or service was generated by generative AI. When providing results such as virtual sounds, images or videos that are difficult to distinguish from reality, the operator must notify or indicate in a way that ensures users can clearly recognise that the result was generated by an AI system.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Laws such as the PIPA and the Copyright Act are used to regulate the improper use of data. However, Korea does not have a particular disgorgement law like the one in the U.S.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

General tort liability and contractual liability doctrines established under the Civil Code will apply in principle. In addition, the Product Liability Act may also apply. However, if the damage occurs within the scope of adverse events or warnings disclosed or stipulated in the package insert prepared pursuant to the Medical Devices Act with the review of the MFDS, the aforementioned liability of the manufacturer or supplier of the subject medical device may be exempted.

9.2 What cross-border considerations are there?

The international cross-certification system has not been introduced in Korea.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Currently, most terms of service for generative AI include disclaimers regarding intellectual property infringement, specifying that users of the AI are responsible for any liability arising from intellectual property infringement. Therefore, to minimise infringement liability, it seems necessary to review potential intellectual property infringement risks associated with the particular results generated by the generative AI.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

In cases where AI/ML models misuse medical data, various legal responsibilities may apply, including those pursuant to the PIPA, the Medical Service Act, Civil Law (tort liability) and the Product Liability Act. Companies and healthcare institutions need to strengthen data protection measures and ensure strict compliance with ethical and legal standards in the design and operation of AI/ML solutions.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The following issues are discussed in connection with the protection of personal data: (i) whether the consent of the data subject is required; (ii) cross-border transfer of personal data; and (iii) data security.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

As to the provision of medical services to patients, two requirements are satisfied under the Medical Service Act: (i) only licensed healthcare professionals are allowed to provide medical services; and (ii) medical services should be provided at medical institutions through *vis-à-vis* diagnosis or treatment, in principle. That said, non-healthcare professionals may provide general health information (not replacing physician's diagnosis or treatment of patients) to customers without violating the Medical Service Act. Further, the developer of digital health technologies should take into consideration reimbursement eligibility under the National Insurance Act as well as MFDS's market approval.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Digital health is one of the fastest-growing markets and the government also has a strong desire to nurture the digital health industry. However, easy access to healthcare services with a low-cost burden under the national health insurance system may be a challenge to the commercial success of a digital health product or service in the market.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

It is difficult for a digital health solution to replace traditional medical services under the Medical Service Act, which requires that the medical service be provided by a licensed healthcare professional at a medical institution. Further, given the universal national insurance system in Korea, it would be necessary for a digital health solution to be eligible for the national health insurance reimbursement so as to be widely used by medical service providers.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

No significant guidelines have been provided by major clinician certification bodies.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

With regard to private insurance, it depends on each insurance company's policies, and no significant general policy consensus has yet been established in the industry. However, as far as the national health insurance is concerned, the following processes are required: (i) the MFDS's product approval or certification under the Medical Devices Act; (ii) nHTA under the Medical Service Act if a new health technology is to be adopted; and (iii) review and determination of reimbursement eligibility under the National Health Insurance Act.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Korea's digital health ecosystem has several gaps, including issues related to data quality and standardisation, algorithmic bias and regulatory uncertainty.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The government has a firm view that the digital health sector is one of the key industries that will lead national growth in coming decades.



Jin Hwan Chung is a partner in the Corporate Practice Group at Lee & Ko, and the co-head of the Healthcare/Life Sciences Team of Lee & Ko. For many years, Jin Hwan has provided legal representation and counsel to numerous leading pharmaceutical and medical devices companies, as well as medical institutions including Archigen Biotech, AstraZeneca, Baxter, BMS, Bayer, Berna Biotech (Crucell), CSL Behring, CSL Seqirus, Daiichi Sankyo, Eisai, Johnson & Johnson, Janssen, Merck & Co., Mundipharma, Novartis, Novo Nordisk, Takeda, UCB, Boston Scientific, Fresenius Medical Care, GE Healthcare, Hologic, Intuitive Surgical, Johnson & Johnson Medical, Medtronic, MerzAesthetics, Samsung Medical Center, Seoul National University Medical Center, and Yonsei Medical Center in connection with various transactions and compliance issues. As a corporate lawyer, Jin Hwan has been involved in many mergers and acquisitions, and has advised his domestic and foreign clients on anti-trust and anti-corruption issues as well. Jin Hwan is one of the highest regarded experts in the area of healthcare compliance and is also a popular lecturer on this area of law.

Lee & Ko
63 Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4711
Email: jinhwan.chung@leeko.com
LinkedIn: www.linkedin.com/in/jin-hwan-chung-9a533719



Eileen Jaiyoung Shin is a partner in the Corporate Practice Group and the Healthcare/Life Sciences Team of Lee & Ko. Her practice focuses primarily on the health industry, including the pharmaceutical and biotechnology products, medical devices, food, nutritional supplements, cosmetics, tobacco and public healthcare sectors. Eileen has advised many multinational companies in the healthcare industry on a broad range of regulatory, corporate and competition law issues. In addition, with respect to the pharmaceutical industry in particular, Eileen regularly advises multinational clients on new drug pricing and after-launch life-cycle management with the firm's active market-access practice.

Lee & Ko
63 Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4831
Email: eileen.shin@leeko.com
LinkedIn: www.linkedin.com/in/eileen-shin-7294b026



Sungil Bang is a partner in the IP Practice Group and the Healthcare/Life Sciences Team of Lee & Ko. His practice at Lee & Ko focuses on legal issues in the areas of healthcare and intellectual property, with a special emphasis on medical device, pharmaceuticals, food and cosmetics. In addition to his legal credentials, Sungil has an extensive background in pharmaceutical and medical sciences, including earning both a B.S. in pharmacology and an M.S. in medical science at Kyunghee University. As a result, Sungil has a particularly excellent contextualised understanding of pharmaceutical and medical technology and intellectual property, as well as the full range of legal and regulatory concerns in the pharmaceutical and medical business sectors in Korea.

Lee & Ko
63 Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 6386 6685
Email: sungil.bank@leeko.com
LinkedIn: www.linkedin.com/in/sungil-bang-973356240

Lee & Ko is a premier full-service law firm in Korea that has been actively servicing multi-national clients since its establishment in 1977. Lee & Ko comprises more than 700 professionals organised into eight practice groups with 40 specialty teams. We pride ourselves on providing a true one-stop service for all legal needs, based on efficient collaboration among our highly specialised teams. Our reputation for trustworthiness and reliability is based on a proud "Lee & Ko tradition" that emphasises the essentials of an excellent law firm practice: specialisation; professionalism; and full consideration for each client's particular needs. We are committed to doing our utmost to, at all times, conduct ourselves in the role of Korea's leading law firm in a socially responsible and positive way.

www.leeko.com

Lee & Ko

Lithuania


Raminta Matulytė


Irma Kunickė


Dovydas Gudžiūnas


Marijus Dingilevskis

Sorainen

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Lithuanian law does not provide a general definition of "digital health". However, it does provide a definition of an "e-health system", which is a set of measures designed to promote healthcare through the use of information and communication technologies.[1]

In addition to this, the Minister of Health has set the objectives for the development of the digital health system. These objectives aim to increase the effectiveness and efficiency of the healthcare system by integrating health information resources into an ecosystem based on uniform principles, modernising electronic health elements, introducing new digital technologies that enable healthcare providers, patients and decision-makers to strive for better accessibility, quality and innovation of healthcare services.[2]

Based on this objective, it can be concluded that digital health in Lithuania is a combination of information resources integrated into an ecosystem based on uniform principles, electronic health elements and new digital technologies, enabling better healthcare accessibility.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Information system (ESPBI IS) – this information system is designed for the centralised collection, storage, and administration of information related to healthcare services provided in Lithuania. This system collects both medical and administrative information related to the providers and recipients of these services. This information system also has, *inter alia*, the following subsystems: (i) **e-prescription subsystem** designed for the issuance, storage, and implementation of electronic prescriptions for medicines and medical aids in pharmacies; (ii) **the Remote Sales of Prescription Medicines and Medical Devices Subsystem (NPRVP IS)**, designed for initiating and executing remote sales of prescription medicines and/or medical devices; and (iii) **the e-health mobile app** that allows users to monitor their health data, view e-prescriptions and medical history, register with doctors, and view referrals and other documents provided by doctors.

The Advance Patient Registration System (IPR IS) is an information system that allows patients to find all their appointments with doctors in one place, reserve appointment times, receive notifications and reminders about scheduled visits to the doctor, cancel visits to the doctor, and monitor the history of all their planned and completed visits online.

Artificial intelligence (AI) – the Ministry of Health highlights that AI has broad potential in personal healthcare, including disease diagnosis, patient data management, support for treatment planning, assessment of patient needs, and clinical consultations.

Telemedicine – key priorities include developing a centralised platform, establishing security and confidentiality standards, ensuring integration with the IPR IS, and enabling clinicians to access relevant information from patients' electronic health records.[3]

1.3 What is the digital health market size for your jurisdiction?

There are currently no official statistics available that would provide a clear overview on this matter. However, Lithuania's per-capita investment in health information and communications technology in 2023 was EUR 1.5 million per 100,000 residents.[4]

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

It is not possible to make a blanket statement in this regard. However, we note that the notable players in the Lithuanian market are Kilo grupė, Medical Score, Mano Daktaras, Skaitmeninės Lankos and Nortal.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

See our response to question 1.4.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Ministry of Health is the main institution responsible for developing and implementing legislation related to digital health in Lithuania. It coordinates and supervises the implementation of the ESPBI IS information system, adopts plans for the development of digital health in Lithuania, etc.

The State Accreditation Service for Health Care Activities under the Ministry of Health (State Accreditation Service) is an institution that supervises, licenses, and controls healthcare activities in Lithuania, including medical devices.

National Health Insurance Fund under the Ministry of Health is the main institution in Lithuania that administers the Compulsory Health Insurance Fund and ensures that insured persons are reimbursed for healthcare services, medical devices and medicinal products.

The State Data Protection Inspectorate is an independent personal data protection supervisory authority that supervises the application of the General Data Protection Regulation (EU) 2016/679 (**GDPR**) and other privacy laws.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Digital health products often qualify as medical devices or *in vitro* diagnostics and, therefore, fall within the scope of the Regulation (EU) 2017/745 on medical devices (**MDR**) or Regulation (EU) 2017/746 on *in vitro* diagnostics (**IVDR**). As EU regulations, the MDR and IVDR are directly applicable in Lithuania and do not have to be transposed into national law. The regulations are complemented by the Law on the Health System of the Republic of Lithuania and its implementing legal acts.

Also, GDPR and the Law on Legal Protection of Personal Data of the Republic of Lithuania (**Law on Legal Protection of Personal Data**) are highly relevant to digital health products and services. Digital health companies must ensure that patient data are processed in compliance with these legal frameworks and safeguarded against unauthorised third-party access.

In addition, certain issues related to digital health are regulated by Regulation (EU) 2023/2854 (Data Act), Regulation (EU) 2024/1689 (**AI Act**), Regulation (EU) 2022/2065 (Digital Services Act) and Regulation (EU) 2022/868 (Data Governance Act).

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Lithuania's digital health enforcement landscape is mainly shaped by EU regulatory convergence, national digitalisation priorities, and growing cybersecurity obligations.

Key areas cluster around eHealth governance, GDPR/health data protections, medicines information systems, and operational oversight by state authorities.

Emerging areas reflect EU-level regulatory expansion (NIS2, DORA, eIDAS), modernisation of state information systems, and rising supervision of AI, cloud, and digital infrastructure providers.

The topic of medical devices – particularly those incorporating AI software – remains a key and emerging area, especially with respect to determining whether a product should be classified as a medical device or not.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

If the software were to be considered a medical device, it would have to comply with the requirements of the MDR or IVDR. State supervision of medical devices is carried out by the State Accreditation Service.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Lithuanian lawmakers have not yet adopted legislation specifically regulating products powered by AI or ML technologies. However, AI/ML-powered medical devices are subject to the same regulations as any other medical device. This means they must comply with the MDR or IVDR for safety, while also complying with data protection and cybersecurity laws.

Depending on the nature of the solution, the AI Act might also be applicable for such devices/software.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

In its digital health development plan, the Ministry of Health of the Republic of Lithuania expresses its intention to implement innovative solutions using AI in order to have a positive impact on healthcare institutions, healthcare professionals and patients. The Ministry of Health already sees and recognises the benefits of AI/ML in optimising the work of medical professionals.

However, in terms of legal regulation, medical devices developed using AI/ML technology are not viewed in isolation in Lithuania and related issues will be addressed together with other pressing AI/ML issues.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

When AI/ML systems act as medical devices, the MDR/IVDR demand strict clinical evaluation and solid validation data.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Such products are predominantly regulated on an EU level with certain national-level laws ensuring the implementation of EU legislation.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

As of the time of writing, enforcement actions are not being specifically tailored to digital health products and solutions and general regulation principles apply.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  The protection of patients' personal data while providing telemedicine services (including prevention of data breaches).
- **Robotics**
  Robotics are machines capable of partially substituting healthcare professionals and will, in most cases, qualify as medical devices.
- **Wearables**
  Wearables, such as smartwatches or smart glasses, often have multiple functions and their primary purpose may not be medical. However, when wearables include health-related features, they may qualify as medical devices and require CE certification.
- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants are generally not designed with health-specific functionalities and are therefore not considered medical devices.
- **Mobile Apps**
  Mobile apps with health-related features can be classified as medical devices and thus may fall under the regulations of medical devices.
- **Software as a Medical Device**
  In case software is considered as a medical device, it is subject to the regulations of medical devices.
- **Clinical Decision Support Software**
  In case software is considered as a medical device, it is subject to the regulations of medical devices.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  A key challenge of such health solution is the protection of patients' personal data while providing solution with real-world evidence.
- **IoT (Internet of Things) and Connected Devices**
  Connected devices in most cases are considered as medical devices and thus require CE certification.
- **3D Printing/Bioprinting**
  The use of 3D templates for prosthetics and tissues can cause intellectual property (**IP**) and licensing issues.
- **Digital Therapeutics**
  Depending on the solution, such therapeutics can fall under the legal category of medical devices.
- **Digital Diagnostics**
  Depending on the solution, such diagnostics can fall under the legal category of medical devices.
- **Electronic Medical Record Management Solutions**
  The protection of patients' personal data while providing healthcare services (including the prevention of data breaches).
- **Big Data Analytics**
  The protection of patients' personal data while using big data analytics (including the prevention of data breaches).
- **Blockchain-based Healthcare Data Sharing Solutions**
  The current e-health infrastructure is not based on blockchain technology but instead relies on traditional solutions.
- **Natural Language Processing**
  The protection of patients' personal data while using natural language processing (including the prevention of data breaches).

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Digital platform providers must ensure compliance with GDPR, i.e. patients' health and other personal data should be processed in accordance with GDPR principles and requirements.

Compliance with cybersecurity regulations is also crucial to ensure the protection of sensitive health data from hacking, unauthorised access or cyberattacks.

Also, the unclarity remains whether international telemedicine services can be provided in Lithuania; specifically, when foreign companies provide telemedicine services to Lithuanian hospitals (for example, radiology), since only Lithuanian established companies can receive access to the ESPBI IS system, which is mandatory for the health data exchange between the service provider and service recipient.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the GDPR, health data is considered a special category and its processing is prohibited unless lawful bases under Articles 6 and 9 exist. Moreover, the entity responsible for the processing is subject to the following requirements:

- inform the individuals how their data is processed;
- maintain records of processing activities;
- ensure rights of data subjects;
- apply enhanced technical and organisational safeguards; and
- when necessary, conduct data protection impact assessments – this will often apply to digital health applications that involve health data and new technologies.

Where health data is anonymised in a manner that irreversibly prevents the identification of individuals, GDPR no longer applies, though organisations must ensure that anonymisation is robust and reidentification risks remain low.

Pseudonymised health data continues to be treated as personal data, meaning that all obligations remain in force, although pseudonymisation is encouraged as a risk-reduction measure.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Protection of health data is primarily regulated by the GDPR and it is supplemented by the local Law on Legal Protection of Personal Data.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

Healthcare providers (like hospitals and clinics) are usually data controllers and must comply with strict GDPR rules for processing special categories of data. Cybersecurity requirements are also crucial.

Public authorities and state health information systems must follow both GDPR and specific Lithuanian legislation on state information systems, cybersecurity, which impose additional obligations on security, and institutional data exchange.

Private digital health and AI solution providers may hold both roles, i.e., if entities operate on behalf of healthcare institutions and follow their instructions, they will be considered data processors, and if health data is needed for the development of the entities' own products or for the provision of their services, they will act as data controllers. Accordingly, depending on the role, particular GDPR requirements will apply. In all cases, it is critically important to comply with cybersecurity requirements.

As personal health data is a special category under GDPR, its processing is prohibited by default unless lawful bases under Articles 6 and 9 exist.

4.4 How do the regulations define the scope of personal health data use?

Under the GDPR, "processing" means any operation that is performed on personal data, including health data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

It is essential to define the roles of the parties with respect to the processing of personal data:

- Where one party processes personal data on behalf of another, a data processing agreement must be concluded in accordance with Article 28 of the GDPR.
- Where two or more parties jointly determine the purposes and means of processing, they are required to enter into a joint controller arrangement pursuant to Article 26 of the GDPR.
- In scenarios involving independent controllers, the GDPR does not mandate specific contractual provisions; however, contractual limitations on data reuse may be appropriate to mitigate the risk of non-compliance.

If personal health data is being transferred outside the EEA, such transfers can take place only if the conditions laid down in Chapter V of the GDPR are complied with, e.g. standard data protection clauses adopted by the Commission should be signed by parties.

Liability and indemnification are key contractual considerations in all cases and warrant particular attention where health data is processed, given the increased exposure to significant administrative fines under the GDPR.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

At present, data accuracy is not a primary enforcement priority for the data protection authority. Moreover, given the restrictions imposed by the GDPR on automated decision-making, the risk of bias or discriminatory outcomes arising from profiling and data use remains comparatively low.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

- GDPR.
- Regulation (EU) 2025/327.
- Law on Legal Protection of Personal Data.
- Law on the Reuse of Health Data of the Republic of Lithuania.
- Law on the Rights of Patients and Compensation for the Damage to Their Health (**Law on the Rights of Patients**).

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Data sharing is one of the operations performed on personal data. Therefore, personal health data sharing is governed by the GDPR together with the Law on Legal Protection of Personal Data.

As personal health data is classified as a special category, its processing, including sharing, is generally prohibited unless lawful bases under Articles 6 and 9 exist. Moreover, if health data is being transferred to a third country outside the EEA, the conditions laid down in Chapter V of the GDPR should be met, e.g. standard data protection clauses adopted by the Commission should be signed. Moreover, a transfer impact assessment must be performed to assess whether the receiving country ensures GDPR-equivalent data protection, identify risks and determine if extra safeguards (technical, contractual, organisational) are needed.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal health data sharing is primarily regulated by the GDPR and it is supplemented by the local Law on Legal Protection of Personal Data.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Healthcare providers (such as hospitals, clinics and general practitioners) act as data controllers when sharing patient health data and must ensure that any disclosure complies with GDPR requirements for special-category data, including, if relevant, entering data processing agreements with their data processors, concluding standard contractual clauses for data transfers outside the EEA, etc. Cybersecurity requirements are also crucial.

Public authorities and operators of state health information systems typically act as data controllers when sharing patient health data and obligations for data controllers under the GDPR are applicable. Additionally, it is necessary to ensure compliance with Lithuanian rules governing state information systems, cybersecurity, which impose additional obligations on security, and institutional data exchange.

Private digital health companies, telemedicine platforms, cloud service providers, and AI developers may hold both roles, i.e., if entities operate on behalf of healthcare institutions and follow their instructions, they will be considered data processors, and if health data is needed for the development of the entities' own products or for the provision of their services, they will act as data controllers. Accordingly, depending on the role, particular GDPR requirements will apply. In all cases, it is critically important to comply with cybersecurity requirements.

As patient data includes health data, which is a special category under GDPR, processing, including sharing, of health data is prohibited by default unless lawful bases under Articles 6 and 9 exist.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

First, GDPR is applicable for sharing healthcare data, under which it is a special category requiring a lawful basis under Article 6, and a special condition under Article 9(2) (e.g., necessity to protect the vital interests of the patient or explicit patient consent).

In Lithuania, the sharing of healthcare data is mainly regulated by the Law on the Rights of Patients. The law establishes that a patient's private life is inviolable and health information may be collected or used only when necessary for diagnosing, treating, or nursing the patient. Health information is strictly confidential during life and after death. It may be shared only:

- with the patient's written consent, specifying the purpose, scope and recipients;
- with persons involved in treatment or care, but only to the extent needed to protect the patient's interests;
- with legally authorised institutions, based on a written request stating the legal basis and purpose;
- with close relatives in limited circumstances when the patient cannot express their will; or
- in specific mandatory cases, such as notifying law enforcement about injuries possibly caused by crime.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

See our response to question 4.7.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

According to the Law on Patents of the Republic of Lithuania (**Law on Patents**), general rules of invention patentability apply to digital health technologies, meaning that digital health technologies are patentable if they are new, involve an inventive step and are industrially applicable. Notably, the interpretation of these concepts in Lithuania is largely harmonised with the EPO Guidelines for Examination, which means that applicants can expect a similar approach to assessing technical character, inventive step and the permissibility of claims related to digital health technologies (e.g., in respect to patenting software-related inventions in the field of digital health).

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The Law on Copyright and Related Rights of the Republic of Lithuania establishes that copyright protection applies to any original result of a person's creative activity expressed in an objective form, regardless of its artistic, scientific or practical value. This means that digital health technologies are protected insofar as they are expressed in a material form. For instance, written content such as various texts and computer code, visual works such as drawings, schemes, and graphic user interfaces are protected. However, ideas, methods, processes or data (except for data bases) remain outside the scope of copyright protection.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected under the Law on the Protection of Commercial Secrets of the Republic of Lithuania and the Civil Code of the Republic of Lithuania, which together define the scope of confidential information and prohibit unlawful use or disclosure. This protection can be strengthened and extended through contractual confidentiality obligations, which usually define the scope of what qualifies as a trade secret between the parties.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

In Lithuania, academic technology transfer is primarily carried out through licensing mechanisms. Academic institutions usually have their internal policies and practices concerning the licensing of various IP to interested parties.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Software as a medical device is protected primarily as a work. The protection applies automatically as of the moment of the expression (creation) of the software's source code. Patent protection is not granted to software "as such", but a software-implemented medical invention may be patentable if it meets general patentability requirements (see question 6.1).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

AI cannot be named as an inventor because the Law on Patents explicitly requires that an inventor be a natural person. Article 2(8) of the law defines "inventor" as "a natural person who creates an invention", which excludes non-human entities such as AI systems.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The scope of IP rights granted to the government for publicly

funded inventions is not comprehensively regulated; therefore, general rules regarding appearance of ownership apply, meaning that the person who created the copyrightable object owns the economic and moral rights.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

The Supreme Court of Lithuania applies the transfer-minimum principle, under which only those IP rights that are expressly identified in an IP transfer agreement are considered transferred or licensed. Therefore, it is essential to describe the transferred or licensed rights in the agreements related to digital health innovations as comprehensively and specifically as possible, ensuring that no intended rights remain unlisted.

Another key precedential guidance comes from Lithuanian Court of Appeals decisions in drug-patent disputes related to the application of injunctions. The courts in drug-patent cases tend to calculate the urgency requirement for injunctions by reference to the European Medicine Agency registration date of the allegedly infringing medicinal product. This precedent is significant for digital health innovation, as it highlights that rights holders must act promptly to protect their patent rights, since delays may restrict access to urgent protection essential for safeguarding fast-moving health technologies.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Collaborative work in the digital health sector demands detailed and well-structured contracts. These contracts should clearly set out how the parties will handle IP and future commercial use of the results, while also defining who is responsible for meeting regulatory requirements and managing any risks linked to the product.

In such contracts it is also recommended to clearly attribute data protection responsibilities, such as data processing roles, etc.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Non-healthcare companies working with public healthcare organisations should avoid offering any advantages or perks when concluding the commercial contract. Any services exchanged must be genuinely equivalent in value, with payments set at fair market price. Benefits must never appear to influence purchasing, prescribing or treatment decisions. They should have a clear, legitimate purpose and remain fully separate from commercial interests.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

When companies enter federated learning healthcare data-sharing agreements, they must ensure that health data processing complies with GDPR (see sections 4 and 5). The agreement must also comply with the Law on the Rights of Patients, which requires strict confidentiality, written documentation of disclosures, and prioritising the patient's interests. Parties should also allocate IP ownership, define rights to improvements, ensure fair commercial terms and set clear responsibilities for regulatory compliance, liability and governance throughout the collaboration.

It must also be evaluated whether processing of such patients' data does not amount to biomedical research (trials), which would require special permits from the state authorities and consents from the patients.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Digital health solutions developers must navigate a staged rollout of requirements, which involves training staff in AI literacy, avoiding banned or high-risk practices, passing conformity checks, maintaining transparency, and forming a legal strategy for IP. Also, integrating generative AI into medical technology requires a rigorous focus on data privacy and protection standards.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is no single authority dedicated solely to regulating AI/ML use. Instead, different public bodies supervise AI/ML systems depending on the area in which they are used. The State Data Protection Inspectorate oversees compliance where AI processes personal data, whereas the Communications Regulatory Authority supervises compliance with the AI Act. Sectoral regulators such as the Bank of Lithuania supervise AI/ML within their fields. Other regulatory authorities may intervene where AI affects consumer protection or competition.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

See question 8.1. Regarding AI/ML in healthcare, AI-based medical technologies usually fall under the category of medical devices and therefore fall under the supervision of the State Accreditation Service, which oversees their compliance with medical device requirements, including safety, performance and proper clinical evaluation.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

There are no special rules assigning IP rights to improvements of algorithms generated autonomously by AI/ML; therefore, general copyright and contract-law principles apply. AI/ML cannot hold authorship. If the prompt of an AI/ML-generated

algorithm was original as per the standard originality threshold, the generated algorithm would likely be owned by a person who wrote the prompts or by their employer if created in the course of employment.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

No special regulations regarding the licensing of data for AI/ML exist in Lithuania. The general text and data mining exceptions apply. If licensing agreements are concluded, it is important to define the scope and aims of the licence very clearly.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Institutions do not distinguish standard AI from generative AI in their current practice.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Generative AI differs from traditional AI systems because, rather than performing rule-based or narrowly defined predictive tasks, it uses ML models to analyse data, detect patterns and create new outputs that resemble human-produced content.

Lithuania currently does not have regulatory instruments that apply specifically to generative AI technologies. At present, generative AI is treated under the same general legal framework as other AI systems, without separate statutory rules or differentiated supervision. From 2 August 2026, generative AI deployed in Lithuania will become subject to the AI Act, which will apply in full and introduce risk-based obligations for all AI systems, including generative AI models. Initiatives at the national level focus on preparing institutions for the EU framework rather than developing standalone Lithuanian rules for generative AI.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Lithuania does not have any legislation specifically addressing situations where trained AI/ML models contain data for which the developer lacks appropriate rights. In such cases, general legal frameworks apply.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Either contractual or tort liability can be applied for the adverse outcomes in digital health solutions depending on the circumstances. When it comes to the provision of health services, the special liability regime applies.

9.2 What cross-border considerations are there?

Liability is primarily determined by the national laws of EU Member States, while in cross-border situations the applicable law is identified under Regulation (EU) 593/2008 (Rome I) and Regulation (EU) 864/2007 (Rome II).

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Digital health providers should ensure compliance with regulatory frameworks while implementing strong data-protection measures, maintaining transparency, safeguarding patient rights, and establishing solid governance, risk-management, and contractual structures. They must also maintain human oversight, ensure secure and responsible data use, and continuously monitor AI/ML system performance to detect errors, bias or performance drift.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Misuse of healthcare data incorporated into trained AI/ML models may result in administrative liability under GDPR and the Law on Legal Protection of Personal Data. Civil liability, defined in question 9.1, may also be applied.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

- **Compliance with GDPR**: Cloud-based digital health solutions must meet strict GDPR requirements when processing health data, which is classified as special-category data under Article 9 (see sections 4 and 5).
- **Cybersecurity risks**: Cloud environments introduce heightened security challenges; the NIS2 Directive imposes enhanced cybersecurity obligations on healthcare providers and cloud service providers, including risk management, incident reporting and supply-chain security controls.
- **Subcontracting risks**: Reliance on external cloud providers raises issues of control, ensuring adequate technical and organisational measures and verifying the provider's compliance with EU standards.
- **Business continuity and resilience**: Healthcare data hosting must ensure high availability, disaster recovery and resilience, as system failures can directly impact patient care.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

- **Highly regulated sector**: Health is one of the most strictly regulated areas in the EU/Lithuania, requiring

compliance with sector-specific rules far beyond those applicable to ordinary digital services.

- **Enhanced data protection obligations**: Health data qualify as special-category data under GDPR, triggering stricter processing conditions and security requirements.
- **Regulatory approvals and certifications**: Many digital health tools may fall under the MDR or require registration with competent authorities, adding significant compliance burdens.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

From a legal perspective, before investing in digital healthcare ventures, venture capital and private equity firms should assess their compliance with pharmaceutical law requirements and data protection laws (if personal data is used by a product). Additionally, investors should make sure that all IP is concentrated within a company and that other legal matters concerning competition, corporative law and employment are well managed within a company.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Lack of a dedicated (and clear) regulatory framework for digital health, meaning providers and developers must rely on general EU and national rules (e.g., GDPR, MDR, health service regulations, etc.), which creates legal uncertainty and increases compliance burden. Also, unclear and limited reimbursement pathways within the public healthcare system.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Lithuania, the Ministry of Health shapes the environment for digital health by setting national health policy, preparing legislation and issuing rules that determine how digital solutions may be used in clinical practice. The State Accreditation Service licences and accredits healthcare providers, oversees compliance and acts as the main supervisory body, which in practice determines whether new digital tools can be introduced in accredited services. Professional medical associations also influence adoption through clinical guidelines and expert recommendations, although these are advisory rather than regulatory.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Digital health solutions do not have a clear reimbursement pathway in Lithuania, neither for patients nor specialists. Therefore, the reimbursement of such solutions generally falls under the reimbursement schemes of healthcare services or medical devices.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

The main due-diligence gap in Lithuania is the absence of a dedicated regulatory framework for digital health technologies, meaning that assessments must rely on general data protection, cybersecurity, medical device and health-sector rules, which were not designed with data-driven or AI/ML solutions in mind.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

This is not applicable.

Endnotes

1 Law on the Health System of the Republic of Lithuania, Article 2, p. 2.

2 Order No. V-878 of 18 July 2017 of the Minister of Health of the Republic of Lithuania "On the Approval of the Action Plan for the Development of the Digital Health System for 2023–2027", p. 6.

3 Order No. V-878 of 18 July 2017 of the Minister of Health of the Republic of Lithuania "On the Approval of the Action Plan for the Development of the Digital Health System for 2023–2027", p. 5.4.2.

4 OECD/European Observatory on Health Systems and Policies (2025), *Country Health Profile 2025: Lithuania. State of Health in the EU*, OECD Publishing, Paris/European Observatory on Health Systems and Policies, Brussels, p. 15.



Raminta Matulytė is an Associate with the firm's Competition and Regulatory team. Raminta specialises in the field of data protection law, advising clients on issues related to national and European Union data protection laws. Raminta also assists local and international clients on intellectual property and state-regulated matters. As a member of the Startup sector group, Raminta focuses closely on development in this sector.

Sorainen
44A Gedimino Ave
LT-01110 Vilnius
Lithuania

Tel: +370 61 062 865
Email: raminta.matulyte@sorainen.com
LinkedIn: www.linkedin.com/in/raminta-matulyt%C4%97



Irma Kunickė is a Counsel with the Competition and Regulated Industries team and Head of the Data and Tech team in Lithuania, focusing on data privacy, cybersecurity and IT law.

Sorainen
44A Gedimino Ave
LT-01110 Vilnius
Lithuania

Tel: +370 66 377 166
Email: irma.kunicke@sorainen.com
LinkedIn: www.linkedin.com/in/irma-kunick%C4%97-72224ab1



Dovydas Gudžiūnas is a Senior Associate with the Competition and Regulated Industries team and Head of the Life Sciences sector group in Lithuania, focusing primarily on pharmaceutical law. In providing legal services to clients, Dovydas helps to ensure that the actions of pharmaceutical and other companies comply with the requirements set out in legislation both in Lithuania and across the European Union. Dovydas is also an officer at the Healthcare and Life Sciences Law Committee of the International Bar Association.

Sorainen
44A Gedimino Ave
LT-01110 Vilnius
Lithuania

Tel: +370 65 891 982
Email: dovydas.gudziunas@sorainen.com
LinkedIn: www.linkedin.com/in/dovydas-gudžiūnas-208313128



Marijus Dingilevskis is a Senior Associate in the Competition and Regulated Industries team, with a primary focus on intellectual property law. His practice covers the full spectrum of intellectual property work, including complex intellectual property transactions, litigation, and intellectual property prosecution. In addition to his advisory and contentious work, Marijus is an attorney-at-law and a national patent attorney, bringing a unique combination of legal and technical insight to matters involving trademarks, copyrights, patents, and technology-driven innovation.

Sorainen
44A Gedimino Ave
LT-01110 Vilnius
Lithuania

Tel: +370 62 905 540
Email: marijus.dingilevskis@sorainen.com
LinkedIn: linkedin.com/in/marijus-dingilevskis-a92501212

Sorainen is an international business law firm that operates as an integrated team across its offices in Estonia, Latvia and Lithuania.
Founded in 1995, the firm has successfully handled numerous significant mandates for both international and local clients. With 46 partners and over 270 lawyers and tax specialists, Sorainen possesses the necessary resources to provide comprehensive support to clients on all matters related to business law and taxation in the region.
The core purpose of Sorainen is to promote the growth of prosperity in the region by assisting more than 15,000 clients in achieving business success. The firm upholds a set of corporate values that guide its operations, which include a focus on clients' needs and business-mindedness, striving for excellence and innovation, fostering teamwork and knowledge sharing, as well as maintaining ethics, respect, reliability, integrity and honesty in all interactions.
Operating as a unified ecosystem, Sorainen's offices adhere to ISO 9001-certified quality management systems and ISO 27001-certified information security management systems. The firm utilises cutting-edge technology to facilitate the sharing of expertise and know-how among its offices, teams and sector groups. This enables its lawyers to leverage the extensive experience held by Sorainen across all jurisdictions, allowing them to spend less time on research and dedicate their focus to crafting tailored legal solutions for clients' specific needs.
Sorainen also embraces modern legal technologies and AI solutions: Luminance, an AI technology streamlining mergers and acquisitions due diligence processes; xLaw, a knowledge management system enhancing lawyer efficiency; and Crespect, an intelligent cloud-based legal practice management software.

www.sorainen.com

SORAINEN

Mexico


Carla Calderón


Marina Hurtado Cruz


Daniel Villanueva


Carlos Vela Treviño

Baker McKenzie Abogados, S.C.

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

The term digital health is traditionally associated with any application of information technologies to the provision of health services and products.

In the last couple of years, there have been some law initiatives, including proposals to amend the General Health Law ("GHL") and specific Technical Standards (Mexican Official Standards – "NOMs") to expressly regulate some applications of digital health. However, none of these have been successfully passed until a structural amendment to the GHL was approved on December 10, 2025 (the "Amendment"). The amendment published in the Official Gazette of the Federation on January 15, 2026, elevates digital health as a matter of public health and includes a full chapter on digital health, including its first legal definition: "*Digital health refers to the application of information and communication technologies in health services, such as, among others, telehealth, telemedicine, mobile health, electronic medical or health records, and wearable devices.*" It also establishes the purposes of digital health, which include to: (i) facilitate the provision of medical services remotely, allowing care for the population without the need for travel; (ii) optimise the use of human and technological resources in healthcare; (iii) expand the coverage of health services, especially in communities with limited access to medical infrastructure; (iv) provide support and advice to healthcare professionals through inter-consultations with specialists; (v) implement educational programmes using digital tools aimed at healthcare personnel and the general population for disease prevention; (vi) digitise the patient's medical information to facilitate access, updating, and secure data exchange among professionals and healthcare facilities, ensuring continuity of medical care; and (vii) analyse large volumes of data to identify patterns, optimise diagnoses, personalise treatments and improve hospital management.

While the legal definition of digital health and its purposes included in the Amendment to the GHL are aligned towards the provision of health services and public health applications, the development and implementation of further regulations for the applications of digital health is expected to follow in secondary regulations and Mexican official regulations or NOMs. At the same time, from the entry into force of the Amendment, all public health institutions must integrate digital health into their programmes and services.

Digital health has also been defined in the Global Strategy for Digital Health 2020–2025 by the World Health Organization ("WHO") as "*the field of knowledge and practice associated with the development and use of digital technologies to improve health*". According to the WHO's Global Strategy, digital health can be further conceptualised as either eHealth or mHealth.

On the one hand, eHealth encompasses the use of ICT by healthcare providers and patients to aid in prevention, diagnosis and treatment.

On the other hand, mHealth: "*[E]xpands the concept of eHealth to include digital consumers, with a wider range of smart and connected devices. It also encompasses other uses of digital technologies for health such as the Internet of Things, advanced computing, big data analytics, artificial intelligence including machine learning, and robotics.*"

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Telemedicine has experienced significant growth in Mexico, with health platforms reporting over 3 million virtual consultations in the past year. This development has enabled individuals in rural areas to access quality medical care from home. The adoption of electronic health records has also advanced, particularly among private hospitals, where 57% now use digital systems for patient registration and prescriptions, streamlining processes and reducing errors. Mexico's medical device ("MD") market exceeds MXN $16 billion, with leading companies such as Medtronic, GE Healthcare and Roche operating plants in the country and exporting products like pacemakers, insulin pumps, and imaging equipment to the United States and Latin America. Additionally, collaborations between hospitals, insurers and technology companies have yielded innovative solutions, such as AXA and Sofía Salud's digital insurance offering unlimited video consultations. The subscription-based healthcare model has quickly gained traction, reaching over 200,000 users in 2024. These trends highlight telemedicine, electronic health records, MDs and digital insurance as key emerging subsectors in Mexico's digital health landscape.

1.3 What is the digital health market size for your jurisdiction?

Mexico stands as the second largest digital health market in Latin America, trailing only Brazil. In 2024, the market value reached USD $2.86 billion, with projections indicating growth to USD $3.56 billion by 2025, as reported in HealthTech in Mexico 2025. These estimates are corroborated by Statista, which forecasts a similar market size of USD $2.31 billion for

2025. Together, these sources highlight the robust expansion and significant scale of Mexico's digital health sector.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

WeeCompany, an InsurTech, has reached MXN $16.2 million in revenue, positioning itself as a significant player in the market. Eden, also reporting MXN $16.2 million, focuses on diagnostics and improving patient care, with a strong emphasis on medical imaging and digital tools to transform the healthcare system. MarfilMexico, with MXN $14.6 million in revenue, is a Mexican company specialising in comprehensive health services, including medical assistance and home care. Welbecare, generating MXN $8.8 million, is a workplace health platform that helps companies enhance employee well-being, productivity and healthcare through technology. Mamotest, with MXN $6.7 million in revenue, is a healthtech company dedicated to early breast cancer detection using artificial intelligence ("AI"), telemedicine and digital infrastructure.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Doctoralia and Sofía Salud have reported more than 3 million virtual consultations in the past year, highlighting their rapid growth in Mexico's digital health sector. Medsi recently raised MXN $3 million in a funding round, which it will use to enhance its AI-driven solution focused on health metrics and biomarkers. Reliv currently manages over 80,000 hospital admissions each month and aims to increase this figure to 200,000, demonstrating impressive expansion. Dentity AI offers an all-in-one platform that connects dentists and patients, provides access to medical records, and leverages data to develop algorithms recommending the best dental products and treatments for clinics. These companies represent the five fastest-growing digital health companies by revenue in Mexico, reflecting the sector's dynamic innovation and increasing adoption of digital solutions.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Federal Commission for the Protection against Health Risks ("COFEPRIS") is the federal authority in charge of health regulation, control and promotion of several regulated products, MDs, cosmetics and healthcare services. COFEPRIS issues market authorisations ("MAs") for MDs and manages health authorisations for healthcare services. It also performs health inspections to the regulated actors to verify compliance with applicable regulations. In 2024, COFEPRIS published GRRUPI, an Advertising Guide for Influencers in connection with healthcare services, drugs, MDs, cosmetics and dietary supplements with the intent to capture these actors' activities that are currently not regulated.

The Secretariat of Anti-Corruption and Good Governance, through its General Directorate of Personal Data in the Private Sector ("SABG"), is the data protection regulator in Mexico. In November 2024, a Constitutional amendment ordered the disappearance of seven autonomous entities tasked with overseeing government compliance in diverse areas, including the previous regulator, the National Institute for Transparency, Access to Information and Protection of Personal Data ("INAI"). The SABG recently replaced the INAI and has taken over the objective of disseminating knowledge for the right to the protection of personal data, promote its exercise and oversee the due observance of the provisions of the corresponding laws and regulations. In this capacity, the SABG can perform audits, request documentation and information, as well as enforce the rights of access, correction, cancellation, opposition, and revocation on public and private entities. This new entity is responsible for managing archives, the National Transparency Platform and sanctions related to personal data protection.

The Federal Consumer Protection Authority ("PROFECO") is responsible for promoting and protecting the rights and interests of consumers and for ensuring fairness and legal certainty in relations between suppliers and consumers. Such mandate includes the oversight of marketing and misleading advertising, e-commerce regulations and product/services warranties. In 2023, the PROFECO issued *The Advertising Guide for Influencers* to emphasise that influencers' activities on social media are considered advertising. The PROFECO is particularly active in sectors where there may be substantial risk for individuals or vulnerable groups, which includes health services and products.

Meanwhile, the Mexican Institute of Intellectual Property ("IMPI") is the competent authority for the protection and enforcement of IP rights.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Mexico does not currently have a comprehensive and dedicated regulation for digital health products such as MDs, AI, SaaS and Software as a Medical Device ("SaMD"). However, the health regulatory framework applies to many product and services categories, which capture digital health applications. As mentioned earlier, once the amendment to the GHL enters into force we can expect that secondary regulations will be likewise amended to include dedicated regulatory schemes for digital health products. Only telehealth is captured by the Amendment, and the focus lies on the conditions and considerations for public health institutions rendering these services.

The framework law is the GHL, from which stem several Secondary Regulations that set forth rules for: (i) products, including drugs and MDs; (ii) establishments, including manufacturing plants, warehouses, pharmacies, hospitals and doctor offices; and (iii) activities, such as research and advertisement. More detailed subjects are regulated in the NOMs, including labelling, techno vigilance and good manufacture practices.

Noteworthy, the product category of MD is very relevant for digital health applications. MDs include the sub-categories of medical equipment, prostheses, diagnostic tools, dental products, surgical and healing products, and hygienic products.

NOM-241-SSA1-2021 on Good Manufacturing Practices for Medical Devices ("NOM-241") contains the concept of SaMD. On July 26, 2024, a draft amendment for NOM-241 was published, which, among other modifications, expands the

definition of SaMD and delegates regulation of the manufacturing of SaMD to the Mexican Pharmacopeia.

The Mexican Pharmacopeia also contains technical requirements that are relevant for digital health. On the one hand, its *Supplement on Establishments* contains key requirements for accepting e-prescriptions in pharmacies. On the other hand, the recently amended *Supplement on MDs* introduced a full Appendix on SaMD which contains detailed rules for the definition of SaMD, classification of the risk level, quality system, clinical evaluation and mobile apps. To date, this is the most detailed legal instrument for the regulation of digital health applications. The General Constitution (the "Constitution") sets forth the basic privacy rules and rights. From there, the Federal Law on the Protection of Personal Data held by Private Parties ("FDPL" or the "Law") and the General Law on the Protection of Personal Data held by Government Agencies ("GLPPD" or the "Law"), provide detailed rules for private and government entities in connection with the basic privacy rules considered by the Constitution. The SABG is permitted to issue secondary regulation and is entitled to enforce the Law. However, other agencies, such as the Ministry of Economy, may also issue privacy-related rules under the umbrella of the FDPL. Such laws regulate the processing of personal and sensitive data, which includes the complete cycle of such data, from its collection, storage, transfer and deletion. Different from other jurisdictions, in general, privacy laws in Mexico are omni-sectorial; therefore, there are no particular regulations for health data. Instead, data protection is regulated by the laws mentioned herein, across all sectors and industries. Other laws, such as the Federal Law for Consumer Protection, provide guidance for e-commerce, which has been complemented by a NOM and a Code of Ethics on e-commerce, a NOM for e-signatures, as well as regulations for financial institutions and payments processors. An imminent amendment to the Secondary Regulations of Medical Products has been in the works since 2023. It is expected that it will include regulations on the e-commerce of medical products, which may include SaMD.

While Mexico has two different regulations for data protection, one for the private sector and one for public entities, both supply protection for the processing of personal data and sensitive personal data which includes past, present and future health data. Further to the principal requirements for the processing of personal data, which require the delivery of a privacy notice to the data subjects, the law considers monetary fines for the misuse of personal data, which are double the regular amount, when sensitive personal data is involved. Such regulatory compliance and the risk of misuse of sensitive personal data, which may result in fines, impose a big legal issue for the development of digital health in Mexico. In addition, because of the nature of digital health services, it is important for companies involved in the sector to consider having privacy by design in their concepts, as well as to conduct privacy impact assessments prior to their implementation. While it may be debatable that privacy impact assessments are mandatory, the INAI had publicly recommended their implementation, a trend that is likely to continue with the SABG's recent appointment. Also, the latent risks of being involved in a data breach or being subject to cybercrime activities increase the possible legal and reputational issues in Mexico.

Depending on the technology used in digital health services, there may be other regulatory issues, such as compliance with technical standards, considered by the NOMs or other laws and regulations such as the Federal Law of Telecommunications, particularly for the use of radio spectrum and the provision of telecommunication services.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

In the context of digital health, the most relevant regulatory category would be that of MDs, which includes the subcategories of medical equipment, prostheses, diagnostic tools, dental products, surgical and healing products, hygienic products and SaMD.

From a health regulatory perspective, digital health applications may constitute a product, a service or both. Once a regulatory category is triggered, a significant number of different obligations and requirements become binding.

On the one hand, if a digital health product is found to constitute a MD, for example, not only would the obligation to obtain a MA be triggered, but also other regulatory requirements, including (i) product-related requirements, such as advertising rules, (ii) establishment-related requirements, such as rules for good distribution practices, or (iii) company-wide requirements, such as operating a techno-vigilance system.

On the other hand, if a digital health application is found to constitute a healthcare service, a variety of requirements are triggered, including (i) filing a notice of operation for at least a consulting room (or clinic or hospital), (ii) having a licence to practise for the physician, and (iii) operating the consulting room in full compliance with other technical requirements.

From a data protection perspective, this can be addressed by looking at sanctions and fines. The health sector and related industries have been one of the most fined. Regardless of the industry, the list of activities that are grounds for most sanctions has stayed the same as previous years, including: (1) processing personal information against the principles of the law; (2) collecting or transferring personal information without the consent of the data subject; and (3) omitting any of the minimum mandatory informational elements in the privacy notice. The INAI was a highly active regulator as is shown in its latest report for the first semester in 2023, with 91 recorded proceedings and having concluded 74 of them, which derived in total MXN $46 million in fines (approx. USD $2.3 million). The INAI also began 293 Right Requests to confirm compliance with the law, from which 155 relate to the access right, five to rectification, 122 to cancellation and 79 to opposition. In addition, the INAI encouraged companies with respect to the processing of biometric data and had lately taken the position in different scenarios that biometric data must be considered sensitive personal data; therefore, it should be processed as such, including a heightened level of diligence and security, since the fines derived from the misuse of sensitive personal data are double of the amount considered for misuse of non-sensitive personal data. Such position will likely continue with the SABG.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

NOM-241 incorporated as a sub-category the notion of SaMD and the Supplement on Medical Devices of the Pharmacopeia, which was amended in 2023 to introduce a full Appendix X on SaMD, and are the applicable regulations to SaMD and its approval for clinical use.

This Appendix establishes six objectives: (i) establishing harmonised definitions (including input data, output data, algorithm, definition statement and real-world performance data); (ii) establishing key considerations of the life

cycle process (including requirements, design, development, testing, maintenance and use); (iii) providing guidance on the application of quality management system practices; (iv) standardising the terminology used for the software industry and integrating regulatory concepts to software engineering activities; (v) establishing a common understanding of clinical evaluation to demonstrate the safety, effectiveness and performance; and (vi) providing guidance on mobile applications.

This regulatory instrument is based heavily on the regulations developed by the International Medical Device Regulators Forum, which created the term SaMD, and the last section on Mobile Apps is heavily based on regulatory concepts adopted by the US Food and Drug Administration ("FDA"), such as listing certain apps in relation to which the FDA would reserve its discretion to exercise regulatory powers.

Apart from those category-specific provisions, the whole regulatory framework for MDs would be applicable to SaMD, including the GHL, the Secondary regulations for Medical Products, NOM-137-SSA1-2008 on the labelling of MDs and NOM-240-SSA1-2012 on techno vigilance. Noteworthy, SaMD requires a MA for its commercialisation in Mexico, which is valid for five years after which, the MA holder shall apply for an extension for another five years. Once the Amendment enters into force, the extension will be valid for 10 years.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Mexico still has no AI/ML-specific law in force for healthcare technologies. AI-enabled MDs and SaMD are approved and supervised under existing health and MD rules administered by COFEPRIS; privacy/automated decision-making duties now sit under Mexico's overhauled data protection regime (LFPDPPP 2025). A national, horizontal AI law is being actively drafted in the Senate with a risk-based approach but is not yet enacted.

The Senate's AI Commission (chaired by Senator Rolando Zapata Bello) held six multi-stakeholder forums and drafted elements of a flexible, horizontal AI framework that would integrate AI principles across sectoral laws (including the GHL), explicitly citing EU-style risk tiers. As of late 2025, sources suggest discussion/approval targeted into 2026; no final AI statute has entered into force yet.

The INAI had published its Recommendations For The Processing Of Personal Data Arising From The Use Of Artificial Intelligence, which aim to disseminate knowledge and the relationship of AI/ML with the fundamental right to the protection of personal data, to promote the appropriate and ethical use of personal data through the different technologies that use AI/ML for their operation and compliance with the obligations of the duty of security of personal data, for those responsible for the private and public sector that develop or use AI products or services.

The foregoing should not undermine the importance that those responsible for the processing of personal data must also comply with the other principles and duties established in the applicable legal frameworks. Similarly, this approach will likely continue with the SABG.

AI-enabled devices and SaMD must be approved under COFEPRIS MD rules (sanitary registration, GMP/QMS per NOM-241-SSA1-2025, and techno vigilance under NOM-240), with 2025 reforms introducing consolidated procedures and an Abbreviated Pathway that recognises IMDRF/MDSAP approvals. Separately, the FDPL overhauled privacy oversight and added automated decision-making transparency and human-involvement requirements, enforced under the Secretariat of Anti-Corruption and Good Governance (post-INAI). A risk-based General AI Law is being developed by the Senate AI Commission but has not yet been enacted.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

See question 2.5 above.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

See question 2.5 above.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Regulation of medical products, which encompasses the regulatory category of MDs such as SaMD, are regulated at a federal level. As mentioned above, NOM-241 and Appendix X of the Mexican Pharmacopeia are the only specific provisions for digital health products and solutions, which are applied together with the general regulatory framework of MDs. Likewise, once the amendment to the GHL enters into force, we can expect further regulations for digital health products and solutions to be developed with a top-to-bottom approach.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

See question 2.4 above.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  From a health regulatory perspective, the absence of specific rules for telemedicine means that this is regulated through the existing general rules applicable to medical consulting rooms, which presuppose a brick-and-mortar establishment. This can be difficult to understand by new players proposing digital platforms. The Amendment introduced a legal definition of telehealth establishing that it refers to *the use of information technologies to offer patient-centred health services at a distance, which may include, among others, medical orientation, medical attention, health education or health research*. The Amendment further establishes that telehealth services shall: be provided by personnel designated and trained for this purpose; use reliable and trustworthy systems that warrant confidentiality, protection of personal data, integrity and availability of medical

information for authorised personnel; integrate mechanisms to obtain informed consent for the rendering of at-a-distance health services; and ensure adequate documents and records of medical attention provided through digital platforms.

From an information technology regulatory perspective, the core issues include the processing of personal and sensitive personal data and the challenge of having to comply with the mandatory regulations, including having to obtain express consents, such as those necessary for: (i) the processing of sensitive personal data, including health data; and (ii) transferring the personal data to a third party (with some exceptions).

- **Robotics**

  From a health regulatory perspective, there are no major issues, as robotics could constitute medical equipment, a sub-category of MDs.

  Rather, challenges may exist in relation to IP protection. Further to the protection granted for the mechanical parts and configuration, there may be challenges regarding patenting software. While software can be protected as a copyright, the rapid change in its code sometimes makes it not worth having copyright registrations for the same and rely on the automatic protection for copyrights. Nonetheless, there are situations where registration is required for other situations, such as government grants, and it is always a good practice where possible. When developing robotics in Mexico, companies must make sure to secure ownership of the developments by having the correct contractual frameworks with their employees and/or contractors.

- **Wearables**

  Wearables may be considered MDs, depending on whether they serve a medical purpose. Many of them often act as diagnostic tools.

  With respect to privacy, it is important to consider privacy by design and privacy impact assessments, as well as to always consider that data subjects in Mexico are entitled to a reasonable expectation of privacy. In addition, it must be considered that when data controllers desire to use Cloud services for the processing of personal data, and the data controller simply adheres to the Cloud services terms and conditions, the Cloud services provider must comply with certain minimum mandatory requirements. Otherwise, in theory, the data controller would be prevented from contracting with such Cloud services provider.

- **Virtual Assistants (e.g. Alexa)**

  The main challenges relate to privacy, in the same terms described above.

- **Mobile Apps**

  Mobile apps would fall within the same regulatory category of SaMD, thus sharing the same challenges and regulation. It is often the case that there is a blurred frontier between wellness apps and medical apps. Regulatory definitions are key to draw distinctions (e.g., definition of mental health) and the new Supplement on Medical Devices of the Mexican Pharmacopeia has certainly shed light in this regard, but we are yet to see COFEPRIS's interpretation of these definitions.

- **Software as a Medical Device**

  A full set of provisions for SaMD have been recently introduced, as mentioned in questions 2.2 and 2.4. The main challenges are the same described above.

- **Clinical Decision Support Software**

  On the one hand, the provision of healthcare services, including mental healthcare, is legally conceived as being provided by licensed healthcare professionals, not machines or software. Therefore, clinical decision support software may be used as an auxiliary to the decision-making process of the healthcare professional. At the same time, under the new product sub-category of SaMD, a clinical decision support software could constitute a MD, requiring a prior MA.

  On the other hand, professional liability for medical negligence can only arise from acts or omissions committed by a healthcare professional, assessed against *lex artis*; in contrast, product liability would arise where a product did not perform according to its announced, intended or approved function.

- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**

  The most relevant regulatory category would be regarding MDs, thus the same challenges described above for other digital health applications would apply. At the same time, under the new product sub-category of SaMD, this would constitute a MD, requiring a prior MA. At the same time, there are issues related to the collection of real-world data from patients. This kind of data is not yet fully incorporated in the Mexican regulatory framework. For instance, it is not clear whether it can be used to support approval decisions.

  On the other hand, there is significant uncertainty in relation to the learning aspect, which requires the constant use of performance data from the user. If this is considered clinical research, it would be subject to an ethics and regulatory approval of the research protocol.

  The same challenges with respect to IP, data protection and privacy, as mentioned above, also apply.

- **IoT (Internet of Things) and Connected Devices**

  The same challenges with respect to IP, data protection and privacy, as mentioned above, also apply. Currently, there are no regulatory guidelines, although this may change at any time.

- **3D Printing/Bioprinting**

  Mexico has not yet issued regulations on 3D printing or in relation to bioprinting, although this may change at any time. Due to the absence of rules, product classification issues may arise regarding the bioprinting of tissues or organs. Noteworthy, ultimately, the place where the printing takes place will be considered the manufacturing site and would have to comply with applicable establishment requirements.

- **Digital Therapeutics**

  Mexico has not yet issued regulations on digital therapeutics. Although in some jurisdictions the relevant product categories for digital therapeutics would include both MDs and medicines, it is likely that in Mexico, they would be framed as a MD.

- **Digital Diagnostics**

  As with all digital health applications, there are no specific regulations for digital diagnostics, hence providers are bound to comply with regulation applicable to a physical version of the model. This includes the same challenges as telemedicine and further adds that healthcare professionals engaged in the diagnostic must be licensed by competent Mexican authorities.

  Nonetheless, the same challenges would apply with respect to data protection and privacy, including the

regulation for the processing of personal data through automated decision-making technologies.

- **Electronic Medical Record Management Solutions**
  The same challenges with respect to data protection and privacy, as mentioned above, also apply. Currently, there are certain regulatory guidelines, although this may change at any time. NOM-004-SSA3-2012 establishes the mandatory scientific, ethical, technological and administrative criteria for the preparation, integration, use, management, filing, preservation, ownership, title and confidentiality of a clinical record.
- **Big Data Analytics**
  The same challenges with respect to data protection and privacy, as mentioned above, also apply. Currently, there are no regulatory guidelines, although this may change at any time. Nonetheless, companies must consider the regulation for the processing of personal data through automated decision-making technologies, which may be applicable to some extent.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The same challenges with respect to intellectual property, data protection and privacy, as mentioned above, also apply. Currently, there are no regulatory guidelines, although this may change at any time.
- **Natural Language Processing**
  Natural language processing has not yet been discussed by the health regulator in Mexico. However, the same challenges, described above, for other digital health applications would apply.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

As mentioned in question 3.1, due to the absence of specific rules for digital platform providers in the digital health space, these providers are regulated through the existing general rules applicable to digital health applications (i.e. products, services or establishments), which presuppose in-person interactions and/or a brick-and-mortar establishment. This can be difficult to understand by new players proposing digital platforms.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The key issues to consider for use of personal data are: (1) the processing of personal information in accordance with the principles of the Law; (2) collecting or transferring personal information only with the consent of the data subject; and (3) delivering and complying with the minimum mandatory informational elements in the privacy notice. However, there are others that should also be considered, such as considering the nature of the data (whether it is personal data or sensitive personal data), the reasonable expectation of privacy, implementing privacy by design, conducting privacy impact assessments, and having a privacy officer or similar function within the company that may address any data subject request. These issues are expected to continue having a substantial impact with the SABG.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As mentioned above, privacy laws in Mexico are omni-sectorial; therefore, there are no regulations for health data.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

While both the public sector and private sector laws are omni-sectorial, their application depends on whether the entity is public or private. Other than such distinction, the considerations do not change depending on the nature of the entities involved.

4.4 How do the regulations define the scope of personal health data use?

"Processing" is defined as the collection, use, disclosure or storage of personal data, by any means. Use encompasses any action of access, handling, use, exploitation, transfer or disposal of personal data.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Contractual obligations may vary depending on the agreement's nature. For data transfers to a data processor, the agreement must show the existence, scope and content of the processing activities. In particular, it should also address the principal obligations for data processors: (i) to process personal data only in accordance with the instructions of the data controller; (ii) to refrain from processing the personal data for purposes other than those instructed by the data controller; (iii) to implement security measures in accordance with the Law; (iv) to maintain confidentiality with respect to the personal data processed; (v) to delete the personal data processed once the legal relationship with the data controller has been fulfilled or upon instructions from the data controller, provided that there is no legal provision requiring a retention period for personal data; and (vi) to refrain from transferring the personal data except where the controller so determines, the communication derives from subcontracting, or when so required by the competent authority.

For transfers to a third party as a new data controller, the agreement between the transferor and recipient must show that the transferor communicated to the recipient the conditions under which the data subject consented to the processing of the personal data. International transfers must consider at least the same obligations to which the controller transferring the personal data is subject, as well as the conditions under which the data subject consented to the processing of his or her personal data. There is a special regime for transfers between entities that belong to the same corporate group, where the transfers do not require consent to the extent that such entities run under the same data protection policies, where such policies are aligned with the principles of the Law.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

From a data protection perspective, personal data must always be complete and correct, imposing an obligation for data controllers to comply with such requirements. While bias and/or discrimination have not been formally addressed in connection with information technology, the Mexican government has provided, particularly for AI, that:

"AI actors must respect the rule of law, human rights, and democratic values throughout the lifecycle of data within the AI system. These include freedom, dignity and autonomy, privacy and personal data protection, non-discrimination and equality, diversity, equity, social justice, and internationally recognized labour rights."

This was also quoted by the INAI in its Recommendations for the Processing of Personal Data Arising from the Use of Artificial Intelligence.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The law applies to entities located in Mexico and to entities located abroad; specifically, under the implementing regulations of the Law, the regulation applies to entities located abroad: (i) if the data is processed in the place of business of the data controller located in Mexico; (ii) if the data is processed by a data processor (regardless of location) who is acting on behalf of a data controller located in Mexico; or (iii) if the data controller is not located in Mexico, but uses means located in Mexico to process personal data, unless such means are used only for transit purposes. While no definition of "means" is provided by the Law, this provision is likely to be interpreted broadly. In that regard, entities that are subject to the application of the law must primarily: (i) deliver a privacy notice that complies with the minimum mandatory information under the Law, the implementing regulations and the privacy notice guidelines; and (ii) obtain consent which must be express for the processing of sensitive personal data and financial data but may be tacit where no such special categories are processed.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Please see question 4.5.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As mentioned above, privacy laws in Mexico are omni-sectorial; therefore, there are no regulations for health data.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Other than the considerations in question 4.5, because of the omni-sectorial nature of the law, these are not altered depending on the nature of the entities involved.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

The most like a governmental initiative to establish a standard regarding the sharing of health information is NOM-024-SSA3-2012. This NOM regulates Information Systems of the Digital Health Record and establishes the mechanism for healthcare providers to record, exchange and consolidate information. However, even though NOM-024-SSA3-2012 entered into force in 2012, we are still waiting to see implementation on a large scale.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Companies that share any personal data, including health data, must either: (i) have the data subjects' express consent for the transfer, having informed the data subjects in the corresponding privacy notice about the identity of the recipient and the purpose of the transfer, if the transfer is made on a controller-to-controller basis; or (ii) execute an agreement with the recipient, as described in question 4.5, if the transfer is made on a controller-to-processor basis, where the recipient only processes the personal data on behalf of the controller and once the relationship is over, the recipient deletes the data.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patents protect inventions, including those related to digital health technologies. The Mexican Federal Law for the Protection of Industrial Property ("FLPIP") states that an invention is any human creation that allows the transformation of matter or energy that exists in nature, for its use by humans to cover their specific needs. Inventions can be products or processes.

Not all human creations can be considered inventions. The FLPIP establishes some exceptions (Art. 47), such as the following: discoveries, scientific theories or their principles; mathematical methods; literary, artistic works or any other aesthetic creation; the schemes, plans, rules and methods for the exercise of intellectual activities, for games or for economic-commercial activities or to conduct business; computer programs as such; the ways of presenting information; the biological material as found in nature; and the combination of known products or inventions unless their combination cannot function separately or that the characteristics of the same are modified to obtain an industrial result or use not obvious for a person skilled in the art.

Furthermore, the FLPIP states that inventions in all fields of technology, including digital health technologies, that are

(i) new (i.e. are not in the state of the art), (ii) the result of an inventive activity (i.e. results are not deduced from the state of the art in an obvious way for a person skilled in the art), and (iii) capable of industrial application (i.e. the invention can be produced or used in any branch of economic activity) shall be patentable (Art. 48).

The initial term of protection of a patent is 20 years. Supplementary Certificates are available for patents filed in Mexico from July 1, 2020, when there are unreasonable delays in the prosecution of the patent attributable to the IMPI, that are translated in a period of more than five years, between the filing date in Mexico and the granting date. Regarding computer programs as such, these are excluded from patent protection; however, computer-implemented inventions related to digital technologies, that involve the use of a computer, computer network or other programmable apparatus, can be patented if they meet the patentability requirements and contain technical features.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyrights cover literary and artistic works. Computer programs as such, including those related to digital health technologies, are protected as Copyrights.

The Mexican Federal Copyright Act ("FCA") establishes that the works protected are those of original creation capable of being disclosed or reproduced in any form or medium (Art. 3 FCA).

Protection is granted to works from the moment they have been fixed on material support, regardless of merit, destination or mode of expression. Fixation is the incorporation of letters, numbers, signs, sounds, images and other elements in which the work has been expressed, or of the digital representations of those, that in any form or material medium, including electronic ones, allow their reproduction (Arts 5 and 6 FCA).

The recognition of copyright and related rights does not require registration or documents of any kind, nor will it be subject to the fulfilment of any formality (Art. 5 FCA). However, it is recommended to voluntarily register the art works with the Copyright Institute as a preventive action to have a precedent of the existence of this right.

In accordance with Art. 14 of the FCA, the following are not subject to copyright protection: the ideas themselves, formulas, solutions, concepts, methods, systems, principles, discoveries, processes and inventions of any kind; the industrial or commercial use of the ideas contained in the works; the schemes, plans or rules to carry out mental acts, games or businesses; the letters, digits or isolated colours, unless their stylisation is such that it is converted into original drawings; among others.

Copyrights grant their holders moral rights and economic rights. The first are inalienable, imprescriptible and unseizable. The second are valid during the life of the author and up to 100 years after his/her death.

Unlike patents, copyrights protect the expression, not the ideas or the technical features. Therefore, referring to computer programs of digital health technologies, copyrights protect the software whether in source or object code.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

The FLPIP defines trade secret as any information of industrial or commercial application, including information related to digital health technologies, that keeps the person who legally controls its confidentiality. This information represents for its owner the obtaining or maintenance of a competitive or economic advantage over third parties in carrying out economic activities and in respect of which it has adopted sufficient means or systems to preserve its confidentiality and restricted access to it.

Information regarding a trade secret may be contained in documents, electronic means or magnetic, optical discs, microfilms, films or in any other medium known. A trade secret owner shall adopt sufficient means to keep the confidentiality of the information and restrict access to it.

It shall not be considered a trade secret if the information is in the public domain, the information turns out to be known or is easily accessible to persons within the circles in which that information is used, or if it must be disclosed by legal provision or by court order.

The FLPIP entered into force in 2020, strengthening the protection of trade secrets and providing more legal certainty on this area. The FLPIP states a new definition of trade secret, indicated in the paragraphs above, as well as a definition for misappropriation and misappropriation infringement and offences. Similarly, it includes additional defences excluding certain information from being considered a trade secret.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

There is no general IP framework for academic technology transfer; general IP and contractual laws apply. Additionally, each Higher Education Institution has its own regulation that shall be considered, including specific restrictions on IP ownership and royalties. When collaborating with a university or institution, it is highly recommended to previously review any restrictions and agree the conditions in which intellectual property will be developed and protected to avoid future conflicts.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

There is no specific regulation for the IP protection of SaMD, so the general rules apply. In this way, the software, whether in source or object code, can be protected as copyright. If the software is related to a computer-implemented invention that meets the patentability requirements established by the FLPIP and that has technical features, it could be subject to patent protection.

In addition to the above, it is important to mention that, for example, the animated sequences and graphical interfaces of a MD application can be protected as industrial drawings.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No. Under the FCA, only individuals can be considered authors. Similarly, under the FLPIP, only individuals can be considered inventors. Therefore, currently under Mexican laws, only individuals can be considered creators.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

There is no general regulation related to government-funded inventions in Mexico. However, public health institutions are subject to a different set of administrative law rules, which may contain IP-relevant provisions, which need to be studied on a case-by-case basis. Similarly, the rules regarding issues of ownership or licensing of government-funded inventions may vary depending on the specific programme, so terms and conditions should also be reviewed on a case-by-case basis. For general patent protection issues, the general rules under the FLPIP would be applicable.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

We are yet to see IP issues related to AI/ML applied to digital health litigated in the Courts. However, a recent resolution in Mexico has confirmed that copyrights created by an AI are not protectable under Mexican copyright law. This decision is based on the principle that only human creators can be considered authors under current legislation. The ruling emphasised that intellectual creations require a human element of creativity and originality, which an AI, as a non-human entity, cannot provide. This resolution underscores the need for clear legal frameworks to address the growing presence of AI in creative fields.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

There must be a written agreement describing the scope of the collaboration and the obligations for each party. It must be agreed beforehand whether the resulting intellectual property can be used by each participant independently or if there should be a collective agreement from all or part of the same. Similar rules must be agreed for the transfer (licensing or assignment) of any resulting intellectual property. In addition, it must be considered that neither the FDPL nor GLPPD consider the existence of a co-controller status. Therefore, only the entity that decides on how the processing takes place would be considered as the data controller. Further to this, the transfer of personal data to a third party that is not another entity part of the same corporate group of the data controller or a data processor would require the data controller to obtain express consent from the data subject prior to the transfer. Lastly, certain collaborative improvements may constitute technical modifications to MDs that warrant either a modification to an existing MA or a new MA. The agreement shall also consider who will be the MA holder, and in the event of termination of the agreement, who will maintain the MA.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

General considerations regarding confidentiality, data privacy, intellectual property, damages, liability and warranties would apply to agreements between healthcare and non-healthcare companies. On the other hand, business models in healthcare typically require addressing technical issues such as quality control and post-commercialisation vigilance obligations, which may require supplementary agreements. At the same time, it must be considered that regulatory approvals constitute intangible assets, the ownership of which needs to be defined in the related contracts. Also, it is important to remember that certain regulatory categories carry certain restrictions to the business model. For instance, the regulatory approval for a MD cannot be held by a foreign company, as it occurs with medicines, thus a local legal entity, most likely a distributor, would have to be the owner and responsible for the product approvals.

Considerations more specific to digital healthcare developments include considering the background of the two industries that converge in this sector. Healthcare companies come from a highly regulated industry and are therefore used to the burden of obtaining health authorisations from innovation to post-marketing. Moreover, they expect their return on investment in a much longer time frame, where the trial-and-error process from molecule to medicine takes several years.

In contrast, digital companies have emerged in a context of the absence of regulation, where innovations can be introduced to the market with little or no regulatory barriers and return on investment can be made much faster.

Therefore, it is important to manage the expectations of digital health companies regarding the time frames for introduction to the market of digital health developments and the time frame for obtaining a return on investment.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

When collecting health data for ML purposes, caution must be had since this may likely constitute health-related research and require health authorisations from an Ethics Committee and the approval of a research protocol from the COFEPRIS. Likewise, if the application is considered an experimental product, concerning which data is collected to prepare a dossier for obtaining a MA in Mexico, then it would certainly require a MA for its commercialisation. The agreement should therefore consider the obtention of the required health authorisations and allocate the responsibility in relation thereto.

Companies that share any personal data, including health data, must comply with the requirements described in question 4.5.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

As mentioned above, digital health solutions may require health authorisation. Before entering the Mexico market, it is highly recommended to consult with a local legal expert regarding whether a specific digital health solution triggers a regulatory framework.

In Mexico, only licensed health professionals may provide healthcare services. Thus, a limitation of a digital health

solution could be that it may claim to assist licensed health professionals in providing healthcare services but may not claim or pretend to perform or render these services in and of itself.

In relation to intellectual property, it is important to review the terms and conditions of the tool used to obtain generative AI to determine the ownership and licensing rules for IP rights. Likewise, it is important to consider that there is a risk of invading the IP rights of third parties.

From a data protection perspective, companies using generative AI in the provisioning of digital health solutions must consider the rules for processing personal data with Cloud service providers, as described in question 10.1. In addition, companies must consider that the data controller remains the sole party responsible for compliance with Mexican data protection laws, even in the case that the misuse of personal data may come from the service provider.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Please see questions 2.1, 2.2 and 2.5.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Please see questions 2.1, 2.2 and 2.5.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under Mexican copyright law, only individuals can be considered authors. Similarly, under the FLPIP, only individuals can be considered inventors. Therefore, currently under Mexican laws, only individuals can be considered creators.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

The commercial considerations are whether the data includes personal data and having to comply with the data transfer requirements set forth herein. However, from an IP perspective, to the extent that the data is embedded on a database, it would be necessary to address the requirements of the Copyright law and regulate ownership of any derivative works.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Please see questions 2.1, 2.2 and 2.5.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Please see questions 2.1, 2.2 and 2.5.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In Mexico, the legal landscape surrounding trained AI/ML models that may include data for which the developer lacks appropriate data rights is evolving. Currently, there are no specific data disgorgement laws directly addressing this issue. However, general principles of data protection and IP law apply.

Mexican copyright law stipulates that only individuals can be considered authors and inventors. Thus, individuals are the only recognised creators under the law. This principle extends to the development and improvement of AI/ML algorithms.

When it comes to using data for AI/ML, commercial, contractual and strategic considerations are paramount, particularly when licensing data. For healthcare data, these considerations are even more stringent due to the sensitive nature of the information and compliance with data transfer requirements as per the Mexican data protection regulations.

From an IP perspective, if the data is embedded in a database, it is subject to the requirements of the Copyright law, and ownership of any derivative works must be clearly regulated in licensing agreements.

As for regulatory oversight, there is no clear differentiation between standard AI and generative AI technologies by the regulatory bodies in Mexico. However, ongoing initiatives aim to develop and refine regulations specific to generative AI, ensuring that the unique challenges and legal issues posed by these technologies are addressed appropriately.

In summary, while Mexico does not have explicit data disgorgement laws for AI/ML models, the existing framework of data protection and IP laws provide a basis for addressing unauthorised use of data. Continued development and refinement of regulations will be crucial as the use of AI/ML technologies expands.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

From a health regulatory perspective, health-related "product liability" is not well developed in Mexico. The most explicit rules relate to liability from clinical trials, where the only clear provision creates an obligation for the sponsor to cover for the medical treatment required to address medical complications directly related to the clinical research, although it is not as clear in relation to a wider notion of damage.

In turn, in relation to health-related "services", the notion of liability falls squarely in the field of medical negligence, where it is physicians (physical individuals) who may be subject to professional liability for acts or omissions assessed against

the *lex artis*. Under the Amendment, the National Commission for Medical Arbitration is the authority tasked with issuing recommendations, opinions, agreements, rulings and arbitral awards.

Alternative dispute resolution methods for controversies in health services, including telehealth or telemedicine, are: (i) immediate resolution; (ii) conciliation; (iii) mediation; and (iv) arbitration.

In terms of general rules of damages, in Mexico there is contractual and non-contractual liability. Within non-contractual liability, there are different scenarios:

(a) Objective liability for inherently risky goods – This takes place: (i) under the consumer protection regime, when the supplier fails to deliver the Instructions of Use; and (ii) under the civil code regime, unless it is demonstrated that the damage occurred due to fault or inexcusable negligence of the victim.

(b) Subjective liability – This requires an illegal conduct and takes place unless it is demonstrated that the damage occurred due to fault or inexcusable negligence of the victim.

At the same time, under the regime that controls technical standards, manufacturers must comply with quality control systems, which will be crucial when assessing the standard of care under the subjective liability system.

Finally, Class Actions were introduced in Mexico in 2011; and although healthcare was not explicitly included, the private healthcare market falls within the scope of the consumer protection law, which applies to the relationship between suppliers and consumers. However, in 14 years there has not been any Class Action in the healthcare sector.

9.2 What cross-border considerations are there?

Digital health has a cross-border nature, materialising the possibility of supplying healthcare services not only at a distance, but from another country. This at once begs the question of whether the digital healthcare provider should be licensed in his/her place of residence or in the patient's place of residence? Would health import permits be required for digital health applications such as SaMD? Likewise, the absence of international harmonisation in the regulation of digital health means that digital health companies must follow different sets of regulations for the same product or service, in the different countries where they may have presence.

Cross-border data sharing is another relevant consideration (see question 4.5), as well as the possibility to file for patents or register trademarks in other countries, under the Patent Cooperation Treaty or the Madrid System.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

To minimise liability risks in the use of generative AI in the provisioning of digital health solutions, before entering the Mexico market it is recommended to consult with a local legal expert to establish whether a certain solution triggers a regulatory framework and which, if any, health authorisations are required. Likewise, care must be taken with the claims of the digital health solution since it may exclusively assist healthcare professionals in their role but is precluded from providing healthcare services. From a data protection perspective, companies using generative AI must assess and confirm that the terms and conditions of the AI provider comply with the rules for processing personal data with Cloud service providers.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Under Mexican law, the misuse of healthcare data in AI/ML models can invoke several liability theories, including breaches of the FDPL due to improper consent or protection and civil liability for damages resulting from unauthorised use or disclosure of health information. Companies must comply with regulations set by health authorities like COFEPRIS, and non-compliance can lead to fines and mandatory corrective actions. To minimise liability, companies should implement robust data protection measures, obtain explicit consent for data use, regularly update data protection policies and ensure AI/ML models comply with ethical guidelines even if there are no particular AI laws that provide a mandatory application.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

If the data processor is a Cloud-based services provider, and the data controller merely adheres to a contract, certain minimum requirements must be included in the standard-terms contract. Otherwise, Mexican companies are prevented by law from contracting such providers. The SABG published minimum guidelines regarding contracting Cloud service providers.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Key issues that non-healthcare companies should consider before entering the digital healthcare market are that healthcare products with medical purposes typically require a longer process to market, since they need to generate clinical information, especially compared to tech companies' disruptive product cycle.

There is no specific regulation related to government-funded inventions in Mexico. The rules regarding issues of ownership or licensing of government-funded inventions may vary depending on the specific programme, so terms and conditions should be reviewed on a case-by-case basis. For general patent protection issues, the general rules under the FLPIP would be applicable.

Regulatory schemes of healthcare products with medical purposes require specific authorisations and not following the healthcare regulations can bring forth fines, as well as the application of safety measures such as temporary closure of the establishment.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

For the reasons mentioned in question 10.2, the commitment of

venture capital and private equity firms to invest may require a longer period to generate return on investment.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

From a regulatory perspective, key barriers holding back widespread clinical adoption of digital health solutions in Mexico are the absence of updated and clear regulations, leading to the application of traditional rules to digital health solutions that do not respond to emerging business models. Also, a regulatory backlog from the healthcare regulator, COFEPRIS, is another barrier across healthcare products. At the same time, there is a risk of over-regulating digital health. Some of the law initiatives being discussed right now at the Federal Congress are proposing to create new authorisations for the digital version of certain activities, whereas the risks involved between the digital and physical versions of the activities may be the same. This may create market barriers or create unintended monopolies.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Healthcare providers (physicians) must be licensed by a Medical School jointly with Mexico's Ministry of Education. Currently, there are no specific certification bodies for digital health applications in Mexico.

The National Centre for Health Technology Excellence has been proposed in draft law initiatives as a certifying body for digital healthcare providers, but it is not within its current scope.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

The provision of public healthcare services in Mexico are not provided through a reimbursement scheme. Rather, there is a system of public procurement of goods and services.

Only around 10% or so of the Mexican population has access to private medical insurance where a reimbursement scheme would apply in combination with a direct pay scheme. There is no straight answer for whether patients who use digital health solutions are reimbursed, since this depends on each insurer's policies and level of insurance protection. Noteworthy, most insurers will not cover medical experimental treatments in clinical phases. For instance, some specific insurance policies consider robotic surgery as experimental treatment and thus it would not be covered, unless it is for brain surgery.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

The main gap in the healthcare ecosystem for analysing digital health solutions is that current provisions for the regulation of digital health are generally fragmented and there is no comprehensive or dedicated legal framework for these applications.

For data-driven products, including AI/ML solutions, the same challenges would apply.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

Before the Amendment, which impact we have described above, the last development regarding the regulation of SaMD was the publication on December 2023 of the Application Guide for Medical Devices Market Authorization issued by COFEPRIS. This Guide provides an in-depth overview of MA applications for MDs, along with comprehensive guidance for digital health applications that either incorporate a sensor or transducer to monitor physiological parameters or are installed on smartwatches. This reflects the prevailing regulatory trend in digital health, where a bottom-up approach allows for swifter regulatory action through administrative channels rather than formal parliamentary processes. However, as previously discussed, this trend is anticipated to shift direction. Once the relevant Amendment takes effect, it is expected that secondary regulations will be updated to expand on the subject matter covered by the Amendment, thereby moving towards a more structured and detailed regulatory framework.

There have been several draft law initiatives submitted in the Federal Congress in the last three years, which focus on different aspects of digital health, mainly telemedicine and health applications of AI. The themes included have been telemedicine, electronic health records, e-prescription, medical apps, AI and neuro-rights.



Carla Calderón is the Head of the Healthcare & Life Sciences Practice at Baker McKenzie Mexico and one of the leading regulatory lawyers in pharmaceuticals, medical devices, and digital health in Mexico. With more than a decade of experience advising multinational companies operating in highly regulated sectors, she is recognised for her strategic, business-oriented approach to navigating complex and evolving legal frameworks governing market access, commercialisation, technology adoption, and regulatory compliance in Mexico's life sciences ecosystem. Carla's practice combines deep regulatory expertise with multidisciplinary capabilities across administrative law, data privacy, intellectual property, government relations, and commercial contracting. She routinely advises clients on the full product and service lifecycle – including manufacturing, import, distribution, labelling, advertising, post-market vigilance, and public procurement of medicines, medical devices, diagnostics, food, cosmetics, and emerging digital health technologies.

Baker McKenzie
Edificio Virreyes, Pedregal 24, 12th Floor
Lomas Virreyes/Col. Molino del Rey
Mexico City, 11040
Mexico

Tel: +52 55 5351 4105
Email: carla.calderon@bakermckenzie.com
LinkedIn: www.linkedin.com/in/carla-calderon



Marina Hurtado Cruz leads Baker McKenzie's Patent Practice in Mexico. With two decades of experience handling sophisticated IP matters, she advises on a broad range of areas, including prosecution, licensing and litigation of patents, utility models, industrial designs and trade secrets. In addition to this, Marina has extensive experience in the areas of Health Care & Life Sciences, Advertising and Consumer laws. In October 2019, Marina was appointed by the Secretary of the Mexican Ministry of Foreign Affairs, as *ad honorem* external advisor on IP issues to collaborate in the development of IP public policies in Mexico. In 2023, Marina was appointed as Vice President of the IP Committee of ICC Mexico.

Baker McKenzie
Edificio Virreyes, Pedregal 24, 12th Floor
Lomas Virreyes/Col. Molino del Rey
Mexico City, 11040
Mexico

Tel: +52 55 5279 2900
Email: marina.hurtado@bakermckenzie.com
LinkedIn: www.linkedin.com/in/marina-hurtado-544863104



Daniel Villanueva collaborates with clients across various industries, focusing on the intersection of intellectual property and technology. He assists technology companies in cross-border transactions, drafting and negotiating commercial agreements, including software and technology licences. Daniel's expertise extends to advising software developers, AI developers, hardware manufacturers, video game creators, social networks, e-commerce platforms and internet companies globally.
His advisory services cover a wide range of areas, including regulatory restrictions, intellectual property, data privacy and security. Daniel provides guidance on global data privacy, data protection, cybersecurity, digital media, and other legal and regulatory issues.

Baker McKenzie
Av. Paseo Royal Country 4596, Torre Cube 2, 16th Floor
Fracc. Puerta de Hierro, Zapopan, Jalisco 45116
Mexico

Tel: +52 33 3848 5387
Email: daniel.villanueva-plasencia@bakermckenzie.com
LinkedIn: www.linkedin.com/in/daniel-villanueva-plasencia-655bbab



Carlos Vela Treviño is the Lead Partner of the Telecommunications, Media and Information Technology Practice at Baker McKenzie. Carlos's practice operates at the intersection of the digital economy, regulation, information technology and human rights. Carlos advises highly disruptive companies in all sectors of the digital economy on a daily basis; his practice involves regulatory and contractual aspects of communications, digital media, copyright, software and cloud transactions, technology disputes, relations with regulators, privacy and cybersecurity.

Baker McKenzie
Edificio Virreyes, Pedregal 24, 12th Floor
Lomas Virreyes/Col. Molino del Rey
Mexico City, 11040
Mexico

Tel: +52 55 5279 2911
Email: carlos.vela-trevino@bakermckenzie.com
LinkedIn: www.linkedin.com/in/carlos-vela-trevi%C3%B1o-96290b2

Baker McKenzie is a top-tier full-service firm with a front-running position in the life sciences market in Mexico and the United Kingdom. The healthcare and life sciences industry group are active on matters throughout the whole life cycle of products, from research and development to manufacturing and commercialisation. The team is noted for advising clients on regulatory matters, particularly medical devices, digital health and pharmaceuticals. The team is also actively involved in legal and trade associations that have life sciences focus or working groups. The strong regulatory practices of health law, information technologies and intellectual property provide the solid bases for an experienced and highly recognised practice on digital health.

www.bakermckenzie.com

Singapore


Gloria Goh


Koh En Ying


Tham Hsu Hsien


Alexander Yap

Allen & Gledhill LLP

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Whilst there is no formal definition of "digital health" under Singapore law, the Health Sciences Authority ("**HSA**") has referred to digital health as "the usage of connected devices, wearables, software including mobile applications and artificial intelligence to address various health needs via information and communications technologies".

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging digital health subsectors in Singapore are presently in the areas of artificial intelligence ("**AI**"), data analytics/predictive preventative care, and digitised and integrated healthcare systems.

The Ministry of Health ("**MOH**") is responding to increasing pressure on Singapore's healthcare system from Singapore's ageing population and a rise in chronic illnesses associated with a modern lifestyle by leveraging technological developments to transform the healthcare sector. The MOH has identified certain key digital health technologies for study and funding, and such efforts can be expected to spur the growth of these subsectors.

AI is expected to play a pivotal role in the transformation of Singapore healthcare systems, driven by initiatives being taken in public healthcare institutions. Efforts are underway to identify proven and impactful AI use cases, with a view towards eventually scaling them into system-wide, national initiatives. Current plans include the ongoing implementation of generative AI tools to automate routine tasks such as updating/summarising of patient records to free up healthcare workers' time and provide better service to patients, as well as implementing AI in diagnosing and treating patients in multiple fields, including radiology, ophthalmology and oncology. Legislative changes may also be part of the efforts to optimise the regulatory framework to allow for scaling up of the use of AI solutions. For example, the Health Products (Medical Devices) Regulations 2010 presently provide exemptions to the licensing regime under the Health Products Act 2007 ("**HPA**"), and this includes that specified healthcare service licensees that develop standalone software (also known as "software as a medical device" or "**SaMD**") with AI ("**AI-SaMD**") are exempted from the general requirement for product registration and a manufacturer's licence if the AI-SaMD is used only for the licensee's own patients. However, as the key developers of AI-SaMDs in the public healthcare sector span multiple healthcare services licensees, such AI-SaMDs fall outside the scope of the said exemption and cannot be easily deployed across public healthcare. The HSA is therefore exploring the possibility of expanding the exemption to create a regulatory sandbox that facilitates the deployment of AI-SaMDs developed by public healthcare institutions for use across other public healthcare institutions.

As regards data analytics/predictive preventative care, it is recognised that AI can also be used to deliver predictive preventative care. This is done through the implementation of disease prediction models based on parameters such as health status, lifestyle and socio-economic status, and access to genomic data will further strengthen this. In line with this, the government had in late 2024 announced plans to invest S$200 million over the next five years to support public healthcare institutions in ramping up preventive care through the use of AI tools and genomic data. An example of such an initiative is the national familial hypercholesterolaemia genetic testing programme, launched by the MOH on 30 June 2025. Under this programme, Singapore citizens and permanent residents with abnormally high cholesterol levels may be referred by doctors for genetic testing, thereby enabling at-risk persons to be counselled to adopt healthier lifestyles and be started on cholesterol-lowering therapies with a view to reducing/avoiding future heart disease and cardiovascular complications. Immediate family members of patients with familial hypercholesterolaemia are also encouraged to undergo genetic testing (i.e., cascade screening), to allow timelier intervention. This programme is part of a broader strategy to enhance preventative care in Singapore, and success is likely to encourage the expansion of a similar approach towards the management of other major severe diseases such as cancer, kidney failure, stroke and heart attack.

Additionally, the National Precision Medicine program collects genomic data with a view to promoting health outcomes through precision medicine (i.e., rather than treating all patients with a particular condition in the same way, individual variations in genetics, environmental and lifestyle factors are taken into account to allow greater precision in predicting the efficacy of treatment and prevention strategies for particular groups of patients). The program is particularly valuable for its ability to collect data from the Asian population, which is presently underrepresented in global genomic research. Ultimately, the program seeks to facilitate the implementation of precision medicine in Singapore on a large scale by 2030.

Concurrently, platforms for digitised and integrated health systems (such as the National Electronic Health Record

("**NEHR**") and the Health Hub mobile application) continue to be progressively implemented to facilitate the consolidation, digital management and sharing of patients' information and records across both the public and private sectors. Presently, the NEHR has been fully adopted by all public healthcare institutions, and all nine private hospitals in Singapore are anticipated to contribute to the NEHR by about mid-2026. The Health Information Bill ("**HIB**"), which was passed in Parliament on 12 January 2026, is intended to take effect from early 2027 and will mandate the contribution of specified key health information by healthcare providers.

Finally, on 31 October 2025, Synapxe Pte Ltd ("**Synapxe**") (the national health-tech agency formerly known as Integrated Health Information System (IHiS)) launched two new national standards: (i) SS719:2025 Guidelines on Data Standard (Terminology) to Support Interoperability of Healthcare System Records, which provides guidance on how clinical information should be structured and exchanged across different healthcare systems; and (ii) SS720:2025 Remote Clinical Monitoring, which supports the integration needs of a growing range of remote clinical monitoring solutions through prescribing a standards-based application programming interface for remote monitoring solutions to record and transmit data in a standardised manner. These standards are intended to better equip health-tech startups and healthcare providers to manage and transmit health information, with the ultimate aim of a more connected, secure and efficient healthcare ecosystem.

1.3 What is the digital health market size for your jurisdiction?

We are not aware of definitive data on the digital health market size in Singapore. However, as an indication, Statista reports that the revenue generated by the digital health market in Singapore (including the digital fitness and well-being, online doctor consultations, and digital treatment and care markets) is projected to reach US$1,018.55 million in 2026.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

We are not aware of definitive data on the comparative revenue of digital health companies in Singapore.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Please see the response to question 1.4 above.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The key healthcare regulatory schemes related to digital health in Singapore involve the regulation of healthcare service providers and healthcare professionals, digital health devices, and cybersecurity and data protection.

The regulation of healthcare services is overseen by the MOH, which is the government ministry responsible for monitoring the accessibility and quality of healthcare services provided in Singapore. Healthcare services are regulated under the Healthcare Services Act 2020 ("**HCSA**") and its subsidiary legislation. Under the HCSA regime, providers of licensable healthcare services are required to obtain a licence, and may provide the licensable healthcare service through at least one of four Modes of Service Delivery ("**MOSD**"). One such MOSD available to certain licensable healthcare services (such as outpatient medical services) is remote provision; this entails the provision of care to a patient who is not physically present in the same place as the healthcare service provider through the Internet or any other kind of technology for facilitating communication (commonly referred to as "telemedicine").

Specific healthcare professionals involved in the supply of digital healthcare are each regulated by their respective professional bodies. For example: doctors are regulated by the Singapore Medical Council ("**SMC**") under the Medical Registration Act 1997; and nurses are regulated by the Singapore Nursing Board under the Nurses and Midwives Act 1999. Each professional body also typically promulgates its own code of ethics and/or ethical guidelines.

As regards devices used in the delivery of digital health solutions, health products (which include medical devices) are principally regulated by the HSA, a statutory board under the MOH, whose remit includes regulating the import, manufacture, export and supply of medical devices in Singapore, and ensuring that drugs, therapeutics, medical devices and health-related products are regulated and meet safety, quality and efficacy standards. The HSA administers and enforces the HPA and its subsidiary legislation, and also promulgates related guidelines. Telehealth products, such as wellness devices, that do not fall within the definition of medical devices are also subject to scrutiny by the HSA (see the Regulatory Guideline for Telehealth Products (April 2019)), although they do not generally require registration and licensing.

As regards data protection and cybersecurity, the Personal Data Protection Commission ("**PDPC**") and the Cyber Security Agency of Singapore ("**CSA**") serve as the key authorities with oversight over the personal data protection regime under the Personal Data Protection Act 2012 ("**PDPA**") and its subsidiary legislation and guidelines (including the PDPC's Advisory Guidelines for the Healthcare Sector), and the cybersecurity regulatory framework under the Cybersecurity Act 2018 and its subsidiary legislation and guidelines respectively.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Please see the response to question 2.1 above.

In addition, the increased usage of digital health records by healthcare institutions and the advent of mandatory contribution of patient data to digitised integrated healthcare systems like the NEHR shines a spotlight on the need for a robust cybersecurity and data protection regime. In this regard:

- The data protection and cybersecurity regimes overseen by the PDPC and the CSA are the critical regulatory schemes which are presently in force.
- The MOH also promulgates its own guidelines in consultation with the aforementioned regulators, such as the Cyber and Data Security Guidelines for Healthcare Providers (December 2023). The latter is currently undergoing revision, and the revised guidelines will be published in the first quarter of 2026.

- Finally, the HIB will add significant new cyber and data security requirements for health and relevant information (as defined in the HIB) when it takes effect. This includes requirements relating to: (i) the implementation of reasonable safeguards and controls to ensure secure processing of this information; (ii) the retention, disposal and destruction of such information; (iii) cybersecurity requirements for computer systems used to process such information; (iv) notification of cybersecurity incidents and data breaches in relation to such information; (v) compliance with emergency measures or requirements in response to threats and incidents affecting such information; and (vi) the portability of health information in electronic form.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The key areas of enforcement generally mirror the areas of regulation in respect of medical devices, healthcare services and healthcare professionals, including registration, dealers' licensing, quality control, advertising, post-market obligations of record keeping and reporting, and the security of patients' medical and health information. As new subsectors of digital health emerge, regulations and enforcement relating to these areas will need to be updated to keep pace with new technologies.

The remote provision of healthcare services continues to be closely watched by the MOH. The National Telemedicine Guidelines have provided guidance for telemedicine providers since 2015, and following a period in which telemedicine and mobile medicine providers were permitted to operate in a "regulatory sandbox" while the MOH sought to better understand the risks of these service delivery models, the remote provision of outpatient medical services has (since 2023) been formally regulated under the HCSA. Further, doctors who practice telemedicine are subject to the SMC's Ethical Code and Ethical Guidelines (2016) ("**ECEG**"). In December 2024, following MOH investigations into the practices of a telemedicine provider (which resulted in revocation of the provider's licence to provide outpatient medical services and disciplinary investigations into the medical practitioners involved), the regulatory obligations and professional standards applicable to providers of telemedicine services were re-emphasised in a joint MOH-HSA-SMC circular.

The advent of the HIB (which is intended to take effect from early 2027) will additionally bring regulation and enforcement concerning health information and the NEHR to the fore. While the MOH is already enforcing the security of health information in the NEHR through practical measures such as system-level controls to limit unauthorised access and regular audits, the further legislative controls introduced by the HIB will include the regulation of matters such as the sharing of relevant information (as defined in the HIB), security of health information and relevant information, the notification of cybersecurity incidents and data breaches and the portability of health information in electronic form.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Where software falls within the definition of a medical device, this is regulated under the HPA regime (see the response to question 2.1). Such software includes software embedded in medical devices, SaMD, standalone mobile applications and web-based software. The HPA and its subsidiary legislation, such as the Health Products (Medical Devices) Regulations 2010, set out the requirements for, amongst other things, registration, manufacturing and supply of SaMD. Unless exceptions (such as a special access route) apply, registration is generally required before the SaMD can be put to clinical use.

Key HSA guidelines relevant to SaMD include: (i) the Regulatory Guidelines for Software Medical Devices including Medical Learning-Enabled Medical Devices – A Life Cycle Approach (December 2025) ("**Guidelines for Software MD**"); (ii) the Guidelines on Risk Classification of Software as a Medical Device (SaMD) and Qualification of Clinical Decision Support Software ("**CDSS**") (July 2025); and (iii) the Regulatory Guideline for Telehealth Products (April 2019).

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In Singapore, there is no omnibus legislation (akin to the European Union's Artificial Intelligence Act), single consolidated framework or regulatory authority for the regulation of AI/ML-powered digital health devices or software solutions. However, where these fall within the definition of a medical device, these are generally regulated under the HPA regime (see the response to question 2.1).

Beyond the HPA, regulatory oversight is generally effected through guidelines promulgated by relevant authorities and professional bodies to guide organisations in the deployment of AI medical devices ("**AI-MD**"). These include Part 9 of the HSA's Guidelines for Software MD, as well as the Artificial Intelligence in Healthcare Guidelines ("**AIHGle**") (October 2021), which were co-developed by the MOH, the HSA and Synapxe, and endorsed by the Academy of Medicine, College of Family Physicians, Infocomm Media Development Authority ("**IMDA**") and PDPC. The PDPC has also articulated a technology- and sector-agnostic AI governance approach to AI, known as the *Model Artificial Intelligence Governance Framework* (2nd ed., January 2020) ("**Model AI Framework**").

More recently, the growing prevalence of generative AI and the advent of agentic AI (i.e., systems that use AI agents to plan across multiple steps to achieve specified objectives) have seen an associated need to consider and manage the risks associated with their use. This includes the need for improved AI governance. In this regard, the IMDA and AI Verify Foundation (a not-for-profit foundation launched under the IMDA to gather contributions of the global open-source community in developing AI testing tools, in support of responsible AI use) have published a *Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem* (May 2024) ("**Model GenAI Framework**"), setting out a framework to address generative AI concerns while continuing to facilitate innovation. The IMDA has also released a *Model AI Governance Framework for Agentic AI* (January 2026) ("**Model Agentic AI Framework**") to provide organisations with a structured overview of the risks of agentic AI and emerging best practices to manage these risks.

Big data and AI have also enabled processing and analysis of large amounts of data beyond what traditional data processing methods could manage. Such technology is valuable in biomedical research, but comes with challenges and risks such as: concerns relevant to ML; the way that big data is captured, analysed and interpreted; privacy and data security;

and ownership issues. The Bioethics Advisory Committee (a policy advisory body established in 2000 to, amongst other things, examine ethical, legal and social issues arising from research on human biology and behaviour and its applications, and develop and recommend policies to the Singapore government) has released a report on *Ethical Use of Big Data and Artificial Intelligence in Biomedical Research* (February 2025), identifying ethical principles and recommendations to guide the use of big data and AI in biomedical research in Singapore.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Where AI/ML-based digital health solutions fall within the definition of "medical devices" under the HPA, they are regulated as such under the HPA regime (see the response to question 2.1). The processes of obtaining registration and dealers' licences in respect of such AI-MD would thereby follow the general processes applicable to medical devices in Singapore, unless suitable exemptions apply (see the response to question 2.1 for an example of a possible prospective exemption).

On our understanding that the reference to the "*dynamic nature of AI/ML-based digital health solutions*" refers to the fact that AI-MD have continuous learning capabilities, the regulator has taken this into account in the relevant guidelines. For example, Part 9 of the HSA's Guidelines for Software MD sets out guidelines targeted at AI-MD. These include that at the pre-market registration stage, information regarding the ML model used in the AI-MD must be submitted and if the AI-MD has continuous learning capabilities and can change its behaviour post-deployment, the learning process must be defined by the manufacturer of the medical device, and appropriate measures implemented to control and manage the learning process. After deployment in the market, AI-MDs are also subject to continuous monitoring of real-world clinical performance where data is collected to verify that the software continues to meet safety and effectiveness claims and allow for timely detection of new and evolving risks arising from the use of the AI-MD (see further details in the response to question 2.7). Finally, a Change Notification must be submitted if there is any change to a registered medical device that affects: (i) the particulars provided upon registration; or (ii) the safety, quality and efficacy of the medical device pursuant to the Health Products (Medical Devices) Regulations 2010. Bearing in mind that AI-MDs are particularly susceptible to change due to their continuous learning capabilities, further guidance on when a Change Notification is required in relation to AI-MDs is set out in Part 9.4 of the Guidelines for Software MD. The AIHGle also contains similar recommendations at paragraph 6.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Post-market monitoring of AI/ML-based digital health solutions is an important part of the Singapore regulatory regime. The HSA's Guidelines for Software MD and the AIHGle provide further details about the role played by clinical validation data. For instance, developers and distributors of deployed AI-MD are expected to collaborate with the implementers and users of AI-MD so as to ensure software traceability, and to monitor and review the performance of AI-MD. Developers are also expected to introduce protocols to log factors that cause changes to the model to ensure traceability. This is considered especially pertinent for AI-MDs with continuous learning algorithms, to ensure that the AI-MD remains accurate and to prevent concept drift. Developers are also expected to apply appropriate control measures on any findings after deployment. In addition, periodic post-market reports are also to be submitted to the HSA, to enable the HSA to intervene in a timely manner if necessary.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Singapore is a single-state jurisdiction with no distinction between state/regional and federal/country regulation.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Digital health products and solutions are generally regulated as medical devices and the regulator's enforcement powers are therefore those available in respect of medical devices (see Part 10 of the HPA).

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

The following paragraph relates to the following technologies: telemedicine/virtual care; robotics; wearables; virtual assistants (e.g., Alexa); mobile applications; SaMD; CDSS; AI/ML-powered digital health solutions; Internet of Things and connected devices; 3D printing/bioprinting; digital therapeutics; digital diagnostics; electronic medical record management solutions; big data analytics; blockchain-based healthcare data sharing solutions; and natural language processing.

The following issues generally apply to all the above technologies: (i) categorisation of the relevant devices as medical devices under the HPA, and if so, determining the applicable risk classification (which has an impact on registration and licensing requirements); (ii) data protection and security; (iii) obtaining informed consent from patients to the use of such technologies; and (iv) maintaining standards of healthcare that are comparable to traditional modes of delivery.

Technologies that involve AI/ML and continuous learning capabilities, in particular, raise the need to ensure that the deployment of AI in decision making is done in a way that ensures that the decision-making process is explainable, transparent and fair, and that the use of AI solutions prioritises the well-being and safety of the humans it affects.

Technologies that involve the processing, sharing and management of confidential patient data in a digitised form also raise issues of the consent required for the collection, use and disclosure of patient data, as well as the need for regulation to ensure that data is not only kept secure from inadvertent data leaks and cyberattacks, but also kept accurate and safe from tampering or corruption. For example, under the HIB, all persons that may interact with or process health and relevant information (as defined in the HIB) will be required to comply with certain cyber and data security requirements. See

further comments on this and related issues in the responses to question 2.2, section 4 and question 9.4.

Under the Cybersecurity Act 2018, acute hospital care services and services relating to disease surveillance and response have been identified as essential services. Therefore, information technology systems relevant to the provision of such services could potentially be designated as critical information infrastructure and require compliance with the obligations under the Cybersecurity Act 2018.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Please see the response to question 3.1.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key issues to be considered, arising from the application of the PDPA, include transfers of personal data outside of Singapore (if the digital health technology provider stores personal data outside of Singapore), ensuring the security of users' personal data and the purposes to which such personal data will be put beyond providing the service or product to users (e.g., whether the personal data will be used for health/clinical research by a third party).

In relation to the use of personal health data:

- the HCSA contains prescriptions on safeguards to be implemented to protect healthcare records and ensure their confidentiality, integrity and availability;
- the Health Products (Clinical Trials) Regulations 2016 require appropriate consent to be obtained from, and sufficient information on intended uses of personal health data to be provided to clinical trial participants;
- the Human Biomedical Research Act 2015 requires appropriate consent to be obtained from, and sufficient information on intended uses of personal health data to be provided to, human biomedical research participants, or a tissue donor for the removal, donation or use of human tissue; and
- when it comes into force, the HIB will mandate the contribution of selected key health information to the NEHR and limit access to such information to specified users and approved users for clearly defined care-related purposes, regulate the sharing of relevant information (as defined in the HIB) through approved data sharing arrangements for specific use cases, and mandate certain cyber and data security requirements for all persons that may interact with or process health and relevant information.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Singapore is a single-state jurisdiction with no distinction between state/regional and federal/country regulation.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The considerations change if one entity is acting as a data intermediary (e.g., data storage provider) of another entity (e.g., product owner) that collects the users' personal data. A data intermediary is an entity that processes personal data on behalf of another entity under a contract. It has fewer obligations under the personal data protection regime and is only required to: protect the personal data in its possession or under its control with reasonable security arrangements; cease to retain documents containing personal data (or remove the means by which personal data can be associated with individuals) if the purpose for which the personal data was collected is no longer served by the retention and there are no legal or business purposes for the retention; and notify the entity that it is processing personal data on behalf of any occurrence of a data breach. In contrast, the entity for whom the data intermediary processes personal data is responsible for the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the entity itself.

The considerations also change depending on the nature of data – for dealings with personal health data, depending on the context, entities may have additional obligations to comply with under the personal health data-related legislation mentioned in the response to question 4.1. In particular, the HIB contains the cyber and data security requirements that specifically apply in relation to health and relevant information (as defined in the HIB) (see the response to question 2.2). The MOH is also expected to issue guidelines on the appropriate uses and access to the NEHR, that will provide for the designation of sensitive health information, to which additional safeguards and handling regulations will apply. Further, while the PDPA does not prescribe any additional legal requirements for information that may be considered sensitive, the sensitivity of data may simply be a factor for consideration in the application of the requirements under the PDPA, e.g., personal health data should be safeguarded by a higher level of protection and data breaches involving personal health data may attract higher penalties.

4.4 How do the regulations define the scope of personal health data use?

The HIB will mandate the contribution of selected key health information to the NEHR and regulate the sharing of relevant information (as defined in the HIB) through approved data sharing arrangements for specific use cases. Depending on the context, the other personal health data-related legislation mentioned in the response to question 4.1 may additionally affect the scope of personal health data use (e.g., where specific consent is sought from a research subject for human biomedical research).

Generally, in other contexts, the regulations do not define the scope of data use. This depends on the nature of the digital health technology and the purposes for the collection, use and disclosure and whether users consent to the purposes. However, there are certain purposes for which consent of users is not required, and this list was expanded in 2021. Accordingly, if the scope of data use falls within such purposes, the regulations could be said to affect the scope of data use, assuming separate consent cannot be obtained.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The types of personal data collected, used and disclosed, the purposes for which the personal data collected will be used and disclosed, and the parties to whom the personal data will be disclosed to should be clearly identified when obtaining consent from users. If there is to be any cross-border transfers of personal data, relying on contractual terms to comply with relevant data protection requirements is common, and this should be considered when entering into/preparing the relevant contract. Depending on the context, contractual terms may also provide that an entity will comply with relevant additional obligations under the personal health data-related legislation mentioned in the response to question 4.1. Further, pursuant to the HIB, entities sharing relevant information (as defined in the HIB) for specific use cases will need to enter into a data sharing agreement containing specified terms.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Data inaccuracy, depending on the cause of the inaccuracy, is potentially a breach of the obligation under the personal data protection regime in Singapore, as well as regulations applicable to healthcare services providers and healthcare professionals to ensure that personal data and patient records are accurate. The PDPC has the power to investigate any complaints of potential breaches and impose fines, if it is of the view that there was a breach. The HIB empowers the Minister, if satisfied that a relevant person has contravened a relevant obligation, to give directions to the person to ensure compliance.

Where the technology concerned is regulated as a medical device, data inaccuracies would have implications under the medical device regulatory regime (e.g., adverse event reporting, field-safety corrective actions, product recalls). The same risks identified may similarly apply in relation to data bias and/or discrimination that give rise to errors or safety issues, particularly for digital health solutions that are regulated as medical devices.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Please refer to the personal health data-related legislation mentioned in the response to question 4.1.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key issues to be considered, arising from the application of the PDPA, include whether the users have consented to the sharing of their personal data, the purpose for which the personal data is shared and whether any exceptions are applicable. If the sharing of personal data involves data transfers out of Singapore, the requirements for data transfers under the PDPA must be complied with. If there is any sharing of relevant information (as defined in the HIB) for specific use cases, the requirements of the HIB must be complied with.

Patient confidentiality is another key issue, and healthcare service providers and healthcare professionals need to be particularly cautious when allowing patients' medical information to be shared, including not to run afoul of ethical duties. For example, doctors need to be mindful of the provisions of the SMC's ECEG regarding medical confidentiality. Further, a breach of patient confidentiality could attract civil liability as a breach of confidence.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Singapore is a single-state jurisdiction with no distinction between state/regional and federal/country regulation.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The considerations change if an entity is a data intermediary. Please see the response to question 4.3.

The sources, expression and nuances of the obligations of patient confidentiality may be different depending on the nature of the entities/persons in question (e.g., different professional bodies may articulate obligations of confidentiality differently), although the gist of the obligations are unlikely to vary hugely between healthcare service providers and healthcare professionals generally.

The considerations also change depending on the nature of data – for dealings with personal health data, depending on the context, entities may have additional obligations to comply with under the personal health data-related legislation mentioned in the response to question 4.1, in particular, the HIB.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please refer to the personal health data-related legislation mentioned in the response to question 4.1, as well as the last paragraph of the response to question 1.2 (on the NEHR and HIB).

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Please see the response to question 10.8 – when it comes into effect, the HIB will facilitate greater integration of the healthcare ecosystem.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patent protection is available for an invention that is new,

involves an inventive step and is capable of industrial application. Under the patent examination guidelines, for computer-implemented inventions, it must be established that the computer (or other technical) features, as defined in the claims, are integral to the invention in order for the actual contribution to comprise said computer (or technical features). Patents are protected for a period of 20 years from the date of application, once granted.

The Intellectual Property Office of Singapore ("**IPOS**") has also released Supplemental Guidance for Examination of AI-related Patent Applications, as a quick patentability reference for applicants seeking to protect their AI-related inventions.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protects expression of original works. Computer programs and software are literary works in which copyright can subsist. Copyright lasts for the life of the author plus 70 years (or 70 years after the year the work is first published if the author is not identified).

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected through the law of confidence in Singapore. The protection of trade secrets is enforced through actions for the breach of confidence for any unauthorised access, use, referencing or disclosure. Trade secrets must be demonstrated to be information that is of a sufficiently high degree of confidentiality (e.g., secret processes of manufacture such as chemical formulae or special methods of construction) and not every piece of confidential information will constitute a trade secret.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

There are no laws that apply specifically to academic technology transfers in Singapore. The National IP Protocol may apply to academic technology transfers if the technology transfer takes place in the context of publicly funded research and development ("**R&D**") activities. Please see the response to question 6.7.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Copyright would protect the SaMD as a literary work. Whether patent protection is available depends on the scope of the invention and whether it fulfils the requirements of being new and involving an inventive step (the third requirement of being capable of industrial application would be satisfied).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

This issue has not yet been tested before the Singapore courts. There is case law that interprets "inventor" under the Patents Act 1994 as being a natural person.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

There are no laws that apply specifically to government-funded inventions in Singapore. However, the National IP Protocol applies to all public agencies and R&D activities funded by public agencies. It sets out a general framework and principles for how intellectual property ("**IP**") arising out of public agencies/publicly funded R&D activities should be owned, protected, used and commercialised. It states that public agencies should generally reserve a royalty-free, irrevocable, worldwide, perpetual and non-exclusive right to use any licensed or assigned IP for their statutory functions, non-commercial and/or R&D purposes. Public agencies should consider the commercial interest of the third party before applying this principle and act in a manner that supports the effective commercialisation of the IP by the third party. Commercialisation of IP created using public funds should also benefit the researchers who are the inventors or creators of the IP.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

The Supplemental Guidance for Examination of AI-related Patent Applications was issued by IPOS in October 2024. While it is a guide and not in the nature of legislation or binding case law, it provides guidance to digital health innovators who may be looking at exploring patent protection for AI-related inventions.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Singapore law allows parties to determine *inter se* the ownership of IP in collaborative improvements. Whilst parties generally gravitate towards some type of co-ownership, and setting up a regime for this is possible as a matter of law, we would generally suggest that parties designate a single owner.

Parties may also contractually provide for ownership and rights of control of data generated from such collaborative improvements, e.g., controlling future uses of the data.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

No special considerations apply, beyond the need for the healthcare company to comply with its usual regulatory

obligations (and to check if any are specifically triggered by the agreement in question).

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Pursuant to the HIB, entities sharing relevant information (as defined in the HIB) for specific use cases will need to ensure that the data sharing agreement contains specified terms. Additionally, parties should consider contractually allocating the risk arising from additional obligations that may apply in the case of accidental or unauthorised re-identification of improperly anonymised healthcare data.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties who are users should contractually ensure that relevant data is not used for training or fine-tuning/customisation and improve coverage of certain associated risks that may arise from the use of generative AI (e.g., data protection and confidentiality issues, copyright infringement issues).

Strategically, for digital health solution providers, parties should consider how they intend to position the product in the local market and keep in mind the intended prescribed use(s) of the digital health solution in the healthcare context as this has an impact on the regulatory risk classification and extent of regulatory controls over the solution. Digital health solution providers should ensure that such product positioning is appropriately reflected in the terms of use and marketing materials (e.g., through disclaimers, indemnities) pertaining to the digital health solution.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is no specific or overarching AI/ML legislation in Singapore. Various regulatory authorities have sector-specific initiatives related to AI/ML. That being said, the IMDA has been closely involved in several initiatives relating to AI/ML in Singapore.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Presently, there is no specific legislation for the regulation of AI in Singapore, or AI-specific legislation applicable for the healthcare sector. Singapore has adopted a light-touch approach to AI governance and regulation where various regulatory authorities have issued guidelines/frameworks relating to AI, including:

- The PDPC's Model AI Framework.
- The IMDA and AI Verify Foundation's Model GenAI Framework, and its companion material like the Implementation and Self-Assessment Guide for Organizations.
- The IMDA's Model Agentic AI Framework.
- The PDPC's Advisory Guidelines: Use of Personal Data in AI Recommendation and Decision Systems (March 2024).
- The CSA's Guidelines on Securing AI systems (October 2024).
- The AIHGle.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

This issue has not yet been tested before the Singapore courts. Current case law requires that there must be a human author identified before a literary work will be an original work in which copyright subsists. Works created by humans with the assistance of AI may be protectable by copyright on the basis that the human is the author.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Common commercial considerations include the value of the data (e.g., whether other third parties have similar data), which may have an impact on whether the party providing the data can negotiate for any rights to any IP/value that is generated through the use of the data for ML. Since no IP subsists in data (except as a compilation, provided the compilation was created through the application of intellectual effort, creativity or exercise of skill or judgment), protecting the use of data by the receiving party through contractual restrictions and obligations (including confidentiality) is important.

The same commercial considerations apply when licensing healthcare data. Further, if there is any sharing of health and related information for specific use cases, the requirements of the HIB must be complied with. Where such data is obtained from a doctor or a healthcare services provider, disclosure will also be subject to the obligations of confidentiality owed to the patients.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

See the response to question 8.2 – different guidelines issued by different regulatory bodies have specific guidelines for AI/ML, and some are targeted specifically at generative AI to address the different risks arising from each technology.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

See the response to question 8.2 – at present, Singapore has adopted a light-touch approach to AI governance and regulation

where in place of legislation, a risk-based, accountability-based, light-touch and voluntary governance approach is adopted through providing guidance to the industry.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In Singapore, it is permitted (i.e., not an infringement) to use copyright-protected works for "computational data analysis", which would include training AI/ML. This exception is limited to training and does not extend to commercial applications of the AI/ML model. There are also certain purposes under the PDPA for which consent of users is not required, such as where personal data is used for business improvement or research.

There are currently no data disgorgement laws or initiatives in Singapore. Legal remedies generally available for infringement would be applicable such as injunctions, damages, account of profits and statutory damages. Regulatory authorities can also mete out financial penalties for unauthorised data uses and breach of the relevant regulations.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

In Singapore, civil liability for adverse outcomes in digital health solutions is typically based on tort or contract law. For example, actions for injuries caused by the use of faulty digital health products are typically founded on the tort of negligence, which requires that the elements of negligence (i.e., a duty of care, breach of the standard of care, causation and damage that is not too remote) be proven. Further, actions for breaches of patient confidentiality could be brought based on the tort of breach of confidence.

In addition, a contractual claim may lie if a contractual relationship exists between the claimant and defendant, and the adverse outcome arises due to breach of term of a contract and/or the contract prescribes remedies for the adverse outcome.

9.2 What cross-border considerations are there?

Increased popularity of digital health solutions gives rise to the increased potential for cross-jurisdictional delivery of healthcare (e.g., through telemedicine) or cross-jurisdictional manufacture or marketing of digital health equipment. This raises questions of, amongst others: (i) the proper forum for pursuing a claim; (ii) the applicable law for the purposes of determining liability if an adverse outcome occurs; and (iii) the enforcement of any award/judgment where a defendant's assets are situated in a foreign jurisdiction.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

In addition to complying with the regulatory requirements relating to ongoing clinical validation and post-market surveillance in place for AI-MDs set out in the responses to questions 2.6 and 2.7 above, the Model AI Framework, Model GenAI Framework and Model Agentic AI Framework also describe some best practices which may help organisations deploying AI technologies minimise the associated risks. These include: (i) ensuring that responsibility for and oversight of the various stages and activities involved in AI deployment are allocated to the appropriate personnel and/or departments, and ensuring that relevant personnel are aware of their responsibilities, properly trained, and provided with resources and guidance needed to discharge their duties; (ii) using reasonable efforts to ensure that data sets used for training the AI model are adequate for their intended purpose and to manage the risk of inaccuracy and bias, as well as reviewing exceptions identified during model training; (iii) establishing monitoring and reporting systems/processes to ensure that appropriate parties are kept informed should there be any issue relating to the deployed AI; and (iv) adopting third-party testing to enable independent verification of quality of the AI/ML. Similarly, the *Ethical Use of Big Data and Artificial Intelligence in Biomedical Research* report recommends best practices to assess the data used in an algorithm for bias, such as the implementation of auditing mechanisms to enable the tracking of AI behaviour and monitoring of its usage.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

In Singapore, liability for the misuse of such healthcare data includes criminal liability under the PDPA for acts such as the unauthorised disclosure of personal data and improper use of personal data without authorisation to cause harm/loss to another or gain to oneself. Where health information in the NEHR is concerned, criminal liability under the HIB may also lie where there is improper access or collection, or unauthorised disclosure, of accessible health information, or unauthorised disclosure or use of information derived from accessible health information. Where the data used for training contains copyrighted material or web scraped data, there is a possible risk of civil liability for copyright infringement or criminal liability under the Computer Misuse Act 1993 or the Penal Code 1871 for violation of the relevant statutory provisions. Additionally, if the misuse leads to a breach in patient confidentiality, there may be civil liability under the torts of breach of confidence and/or negligence. Finally, if a contract governs the use of the data, civil liability may lie for breach of contract.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cybersecurity and data protection (in particular where electronic health records of patients are involved) issues apply equally for Cloud-based services for digital health. Please see the response to question 3.1, and sections 4 and 5.

Further, there are upcoming amendments to the Cybersecurity Act 2018 under which providers of information technology systems relevant to the provision of cloud computing services could potentially be designated as a major foundational digital infrastructure service provider and be required to comply with the obligations thereto.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Depending on the manner of entry, there may be additional regulatory requirements, such as those highlighted in our responses above.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

The healthcare industry in Singapore is a highly regulated space, and specific regulations/requirements may apply depending on the precise operations/transactions in play. Venture capital and private equity firms should consider and seek advice on the relevant regulations (including the need for due diligence on potential regulatory exposure) before investing in digital healthcare ventures in Singapore. Depending on the technology involved and the area of application in digital health, it may also be necessary to consider freedom-to-operate searches to assess third-party IP infringement risks and whether sufficient steps have been taken to protect IP rights that may subsist in the digital health solution.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Digital health solutions are increasingly available in Singapore. However, key challenges for widespread clinical adoption of digital health solutions include:

- Costs of digital transformation: Costs may include initial set-up costs and costs of maintaining digital systems, as well as employee training, creation of compliance strategies and the implementation of security measures to protect data.
- Singapore's ageing population: Many elderly Singaporeans remain unfamiliar with technology and digital health solutions, and training programmes/outreach efforts may be costly.
- The inability of digital health solutions to replicate the compassion and empathy associated with the healthcare profession: Patients may prefer the face-to-face interactions of visiting their doctor or healthcare professional.

In the context of implementing AI solutions, challenges include resolving questions of whether use of patient data and other confidential health information in the use, development and training of AI programs may infringe upon healthcare services providers' obligations in respect to the use of such data/information, obtaining informed consent from patients for the use of AI-MD in the delivery of care (which raises novel issues of the extent of information that a clinician has to give a patient about the nature of the AI input and the risks involved in the use of AI as compared to conventional management), and adapting existing regulatory frameworks to ensure safe and scalable adoption of AI solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Clinician certification bodies (such as the Specialists Accreditation Board under the Medical Registration Act 1997) do not routinely have the clinical adoption of digital health solutions as a focus. Instead, the clinical adoption of digital health solutions is heavily influenced by the Singapore government. In this regard, the MOH has set up an Office for Healthcare Transformation, which aims to evolve the healthcare system into one that is data-driven and digitally enabled. Further, there are government efforts in place such as the Smart Nation initiative, which seeks to leverage digital technologies to enhance Singapore's economy and society. More recently, the Health Promotion Board (a statutory board under the MOH) has launched programmes such as DigiCoach, a programme involving the use of wearable glucose-monitoring devices to provide users with real-time information on how glucose levels change with diet and physical activity and promote the formation of better habits, and HealthTrack SG, in which persons with hypertension, diabetes, or high cholesterol monitor their health and lifestyle using a wearable device and a dedicated application, providing data for use in health counselling.

Beyond the government, sentiments of healthcare professionals and the public and practical issues such as the costs of implementation influence the adoption of digital health solutions. Parliament also has a part to play, as legislation can also mandate the adoption of digital health solutions (e.g., the HIB will make contribution to the NEHR mandatory for all licensed healthcare providers).

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Patients who use digital health solutions in Singapore can be reimbursed by government insurers or private insurers. Details of the extent to which reimbursement will be provided and the requirements for reimbursement, including whether there are any requirements on the digital health solution provider, would depend on the specific coverage agreed between the insured and insurer.

Business entities that wish to adopt digital health solutions may be eligible for funding under the Enterprise Development Grant, which provides funding support for businesses to improve resource efficiency through automation and technology. Additionally, the MOH also announced funding support for healthcare providers and professionals to support them in their compliance with the requirements of the HIB.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence gaps in the context of digital health solutions arise in relation to ensuring the AI/ML-based solution's reliability, which is likely to have an impact on patient safety (whether directly or indirectly). In this regard, the AIHGle has identified a non-exhaustive list of areas in which these gaps may occur in the context of digital health solutions in the healthcare ecosystem, particularly for digital health solutions that would be regulated as medical devices using AI/ML with continuous learning capabilities:

- inappropriate initialisation parameters (i.e., incorrect or unsuitable starting settings);

- biased or unrepresentative input data that ultimately affect the algorithms behind the AI/ML-based solution;
- difficulties in fully validating the accuracy of updates to the model algorithms to ensure clinical validity and accuracy due to continuous learning capabilities;
- abnormal behaviour (e.g., maliciously introduced data) and/or end-user manipulations (e.g., the introduction of rare yet valid and important data); and
- ensuring clinical viability of synthetic data sets used in training and development of algorithms.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

Given various trends, such as an ageing population, there is an increasing focus on primary care to prevent illness, including increasing the support for private general practitioners. Once it takes effect, the HIB will facilitate greater integration of the healthcare ecosystem, by requiring licensed healthcare providers (including private providers) to input patients' medical records into the NEHR. This enables important patient data to be made accessible to various care providers and facilitate good continuity of care, and also enhances overall efficiency of the healthcare system.

Issues such as risks of potential mismanagement of/improper access to patient data, and cybersecurity lapses, arising from expanded collection, storage and sharing of patient data, will become more acute. Whilst the HIB may legislatively provide for certain safeguards and also deals with issues such as patient preferences to restrict access to their data in the NEHR, it remains to be seen how effective such safeguards will be in practice. Further, while breaches of the requirements of the HIB will be taken seriously by the MOH, it has also been indicated that the MOH wishes to take a supportive role and approach, working together with healthcare providers and professionals to uplift data and cyber security, rather than taking a punitive approach; how this will play out in practice will also be a point to watch out for.

At the same time, there are legitimate concerns as to how advances in the realm of digital health will affect healthcare professionals and providers' ability to practice and meet the standards required of them in the implementation of digital health solutions. The passing of the HIB, in particular, raises issues such as the need for clarity as to how the availability of vast amounts of health information in the NEHR may impact a clinician's exercise of professional judgment in deciding when to access the NEHR, and how much health information and medical history must be reviewed in order to discharge the duty of care.

Acknowledgments

The authors would like to thank Sreshya Kamakshi Vishwanathan, Senior Associate and Charlene Tan, Associate from Allen & Gledhill LLP, for their valuable assistance in the preparation of this chapter.



Gloria Goh is a Counsel in the Technology & Corporate Intellectual Property Practice. Her areas of expertise are in IP, technology and pharmaceuticals, health products, cosmetics and food regulation.
She has acted in a broad range of contentious and non-contentious matters involving trade mark, copyright, patent, domain names, confidential information and data protection. Her experience includes conducting IP due diligence in corporate transactions, conducting intellectual property audits for clients and advising clients on their IP management policies, advising clients on the acquisition of IP and drafting and negotiating commercial agreements relating to the acquisition of IP.

Allen & Gledhill LLP
One Marina Boulevard, #28-00
Singapore 018989

Tel: +65 8318 0162
Email: gloria.goh@agasia.law
LinkedIn: www.linkedin.com/in/gloria-goh-283546186



Koh En Ying specialises in litigation and dispute resolution. Her work involves court disputes, arbitrations and mediations, with a focus on medical malpractice and construction disputes.
She has experience dealing with medical negligence claims, disciplinary proceedings and Coroner's inquiries, and has advised and represented a medico-legal defence organisation, insurers, healthcare professionals and healthcare institutions in matters across a range of general and specialist medical practices. Her practice also includes advising on healthcare regulatory issues, such as the regulation of healthcare professionals, healthcare service providers, and health products, including where relevant to operational matters and corporate transactions. She presently sits on the Advisory Board of the Singapore Psychological Society.

Allen & Gledhill LLP
One Marina Boulevard, #28-00
Singapore 018989

Tel: +65 9730 9974
Email: koh.enying@agasia.law
URL: www.allenandgledhill.com/sg/partners/5019/koh-en-ying



Tham Hsu Hsien is a specialist practitioner in healthcare disputes and healthcare regulatory matters in Singapore.
He advises and acts for medical professionals, hospitals, pharmaceutical companies, professional indemnifiers and insurers in contentious and non-contentious healthcare matters. In particular, he acts regularly for medical and dental professionals in contentious malpractice claims in the Courts, and in disciplinary proceedings before professional disciplinary bodies such as the Singapore Medical Council and the Singapore Dental Council.
He also regularly advises on healthcare regulatory matters, with special interest in digital health and AI.

Allen & Gledhill LLP
One Marina Boulevard, #28-00
Singapore 018989

Tel: +65 9798 0538
Email: tham.hsuhsien@agasia.law
URL: www.allenandgledhill.com/sg/partners/4971/tham-hsu-hsien



Alexander Yap is the Co-Head of the Firm's FinTech Practice and a Partner in the Technology & Corporate Intellectual Property Practice.
He advises on three key pillars:

- the acquisition, divestiture, provision, sharing, and receipt, of data, technology and IP-related services and assets, including cryptographic tokens and digital assets;
- data breach and cybersecurity strategy, communications, management and compliance; and
- emerging and frontier technologies, such as autonomous driving, metaverses, large language models, transformer neural networks, and generative AI.

Allen & Gledhill LLP
One Marina Boulevard, #28-00
Singapore 018989

Tel: +65 9010 3081
Email: alexander.yap@agasia.law
LinkedIn: www.linkedin.com/in/alexander-yap-a327471b

Allen & Gledhill is an award-winning full-service law firm which provides legal services to a wide range of premier clients, including local and multinational corporations and financial institutions in Asia. Established in 1902, the Firm is consistently ranked as one of the market leaders in the region, having been involved in a number of challenging, complex and significant deals, many of which are the first of its kind. The Firm's reputation for high-quality advice is regularly affirmed by the strong rankings in leading publications, and by the various awards and accolades it has received from independent commentators and clients. The Firm is consistently ranked band one in the highest number of practice areas, and has the highest number of lawyers recognised as leading individuals. Over the years, the Firm has also been named "Singapore Law Firm of the Year", "Regional Law Firm of the Year" and "SE Asia Law Firm of the Year" by many prominent legal publishers.

www.allenandgledhill.com

ALLEN & GLEDHILL

Switzerland


Tobias Meili


Carlo Conti


Martina Braun


André S. Berne

Wenger Plattner

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no common general definition of "digital health" in Switzerland. Medicinal products (i.e., pharmaceuticals) and medical devices are subject to general regulation by the Federal Therapeutic Products Act (TPA). Detailed provisions are regulated in several ordinances. However, neither the TPA nor its ordinances contain a legal definition of the term "digital health".

The Federal Office of Public Health (FOPH), which by default acts as the competent authority for all public health matters, defines "digital health" applications and devices as products that use digital technology to accomplish their medical objectives. This includes telemedicine, telemonitoring, mobile applications and other similar applications, but not digital applications that solely assist healthcare professionals in their duties (such as controlling a device or reading and analysing data).

Swiss scholars partially use the term "digital health" as a collective term for "eHealth" (i.e., the use of ICT in healthcare) and "mHealth" (i.e., the use of mobile devices for patient care, such as smartphones or tablets).

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Growing use of telemedicine: Telemedicine solutions, including hybrid care combining virtual and in-person consultations, enjoy an extensive presence, are widely recognised in Switzerland and continue to further emerge. For instance, one of the largest medical telemedicine centres in Europe is managed by the Swiss digital health company *Medgate* in Basel, providing health insurance providers with the opportunity to serve as their policyholders' family physicians and/or gatekeepers. *SWICA*, a health insurance provider, among others, also provides telemedicine solutions, telemedical consultations and remote monitoring of vital parameters. Based on this, further telemedicine models enter the sector. Hence, an important part of the Swiss population has already been exposed to telemedicine.

Electronic Patient Record (EPR): In April 2017, the Federal Electronic Patient Record Act (EPRA) came into force with the aim that all patient records are maintained exclusively digitally and that all vital health documents (e.g., nursing and hospital reports, examination results, X-rays) are centrally stored and securely shareable among healthcare professionals. However, its spread has been hindered due to the voluntary nature of its use and limited funding. To accelerate digitalisation, the Federal Council (i.e. the Swiss government) decided in November 2025 to replace the existing EPR model with a newly established electronic health dossier (E-HD), designed to consolidate individual health data and mandate its use by healthcare professionals, while granting patients complete control over access. The proposed Federal Electronic Health Dossier Act, already submitted to Parliament for deliberation, shall aim to delineate roles, competencies, and funds, designating central infrastructure administration to the federal government and implementation to the Cantons. Currently, the implementation of the E-HD is aimed for completion by 2030.

Wearables: Wearable technology monitoring personal health information in real time is fashionable and gaining users steadily. Since the COVID-19 pandemic, wearables have experienced additional expansion and are increasingly being integrated with EPRs, telemedicine platforms and AI/machine learning (ML)-driven analytics.

eMedication: "eMedication" refers to electronic systems that furnish data regarding the prescription, dispensation and processing of a patient's medication. This feature facilitates a multitude of operations, including the establishment of a medication schedule and a medication reminder system and is intended to increase process efficiency and patient safety. eMedication is a prevalent use case within the EPR framework. For instance, the EPR (and in future the E-HD) can be integrated with reminder functions that prompt patients to take their prescribed medications.

E-commerce of therapeutic products: In Switzerland, medicinal products do not necessarily have to be purchased in brick-and-mortar pharmacies or physicians' practices, but pharmacies may upon request be granted the permission to engage in mail-order sales under certain conditions (Art. 27(2-4) TPA). Patients can therefore order medicinal products and certain medical devices online from a Swiss mail-order pharmacy and have them delivered at home. Over 30 mail-order pharmacies are currently active in Switzerland. However, following a Federal Supreme Court (FSC) ruling in September 2015, such pharmacies must request a prescription for both prescription-only and over-the-counter (OTC) medicinal products (FSC 142 II 80). Thus, prior consultation with a physician remains mandatory and online offerings continue to be strictly regulated.

1.3 What is the digital health market size for your jurisdiction?

The Swiss market for digital health products and services is expanding rapidly. Several market size estimates exist,

contingent upon the pertinent key performance indicators and the definition of digital health (see question 1.1). Accordingly, recent studies estimate that in 2024, the market size of digital health in Switzerland ranged between USD 1.23 billion (Statista: https://www.statista.com/outlook/hmo/digital-health/switzerland?srsltid=AfmBOooLuQsfQNhYTRbrfv65e-eNpDuHNO-VwVe2hxkDOZeMNILOUln0) and USD 3.79 billion (Databridge: https://www.databridgemarketresearch.com/nucleus/switzerland-digital-health-market?utm), with projections suggesting strong growth to USD 14.11 billion by 2032 (Databridge).

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

A considerable number of digital health-specialising companies are also engaged in other technology or health-related industries. Thus, there are no reliable data regarding what the largest digital health companies in Switzerland are. Global technology companies, including Apple, Google, Huawei, IBM, Samsung and Xiaomi, are important players in the Swiss digital health market, as in other countries. Furthermore, several companies have established themselves in the field of telemedicine and e-commerce with therapeutic products (see question 1.2). In addition, more and more spin-offs, particularly from the two Swiss Federal Institutes of Technology in Zurich and Lausanne, are entering the market and often arise foreign investors' interest.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

In Switzerland, there are nearly 200 companies engaged in the digital health sector, demonstrating varying rates of growth. Since revenue information is typically not disclosed to the public, a subjective evaluation is necessary. Furthermore, the varying levels of maturity among the companies must be considered: start-ups and scale-ups typically experience rapid growth; however, their overall market significance often remains quite limited.

Some notable companies include: (i) Sleepiz, a manufacturer of medicinal products focused on sleep quality; (ii) Dacadoo, a provider of health scoring and lifestyle navigation solutions; (iii) Bluespace Ventures, which offers an integrated healthcare ecosystem platform in Switzerland under the Compassana trademark; (iv) OptiChroniX, whose solutions target modifiable risk factors for cognitive health in older adults; and (v) Holmusk, a European branch of a Singaporean company specialising in data analytics and digital therapies. RetinAI and Rhovica are also notable as recent market entrants reflecting strong financing rounds, team expansion, and market activity.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

In Switzerland, the FOPH is by default the competent authority for all public health aspects, unless the cantonal (health) authorities are in charge. In the area of therapeutic products, however, neither the FOPH nor the cantonal health authorities, but rather the Swiss Agency for Therapeutic Products (Swissmedic) acts as the competent Swiss regulatory and supervisory authority for medicinal products, including OTC products as well as medical devices (Arts 68, 69 and 82 TPA).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The core principles are outlined in the TPA, which refers to medicinal products and medical devices as "therapeutic products" (Art. 2(1)(a) TPA, *"Heilmittel"*). This also includes OTC medicinal products, as well as supplements to medical devices. Due to the high export rate of such products to the European Union (EU), the Swiss legislator aims at a far-reaching conformity between Swiss and EU law.

Detailed provisions that are crucial in practice are regulated in several Ordinances such as the Medical Devices Ordinance (MedDO). Since digital health technologies often qualify as medical devices, the requirements of the MedDO apply. In this context, Swissmedic has issued specific guidance referring to guidelines and publications of the EMA, FDA, WHO, CIOMS, IMDRF and ICH, aiming to clarify how such technologies are to be assessed and regulated under Swiss law. In addition, EU regulations pertaining to medical devices must be considered in conjunction with Swiss statutory provisions when it comes to digital health technologies that qualify as medical devices.

Finally, if cantonal health authorities are competent in a certain matter (e.g. in case of authorisations for medical activities), the relevant cantonal regulations apply.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

If digital health technologies or products do not comply with the provisions of the Swiss Data Protection Act (FADP), the cantonal criminal authorities may impose fines of up to CHF 250,000 on offenders in accordance with the penal provisions of chapter 8 FADP.

Digital health technologies or products that qualify as medical devices according to the TPA must comply with the regulations of the TPA and MedDO. Failure to comply with the regulations of the TPA or the MedDO may qualify as a criminal offence (Arts 86 and 87 TPA). For example, intentional introduction, export or use of non-compliant medical devices, or the use of medical devices without meeting the necessary technical and operational requirements may be sanctioned by imprisonment of up to three years or a fine (Art. 86(1)(d) TPA).

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Digital health solutions qualify as medical devices when they (i) are intended to be used for human beings, and (ii) serve to fulfil medical purposes, such as (a) diagnosis, prevention, monitoring, treatment or alleviation of diseases, injuries or disabilities, (b) investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, (c) providing information by means of *in*

vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and/or (d) control or support of conception (Art. 3(1)(c) MedDO).

According to Swissmedic, acting as the competent Swiss regulatory and supervisory authority for medical devices, software or apps are not considered medical devices if their sole purpose is related to fitness, well-being, nutrition (such as diets), hospital resource planning, reimbursement, management of doctors' visits, statistical analysis of clinical or epidemiological studies or registers, functioning as a diary, replacing paper-based health data, or serving as electronic reference works containing general non-personalised medical information.

In September 2018, the Swiss Federal Administrative Tribunal (FAT) ruled in a landmark decision that an app designed to assess a woman's fertility by analysing her vital signs meets the criteria to be classified as a medical device (FAT C-669/2016).

Thus, the term "medical device" is interpreted comprehensively. Hence, if software has a medical purpose, regardless of whether it has a proven medical effect, it may qualify as a medical device. In such a case, the software must adhere to the regulatory requirements that apply to medical devices, including the registration obligations in the Swiss medical devices database (see question 2.5 below).

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Current Swiss legislation does not encompass AI/ML-powered digital health devices or software solutions. Consequently, the overarching principles are applicable to these products; if classified as a medical device, the relevant regulations for clinical use must be adhered to (see question 2.4 above). It is important to note that medical devices, in contrast to medicinal products (for the differentiation, see question 1.1) are not governed by a state authorisation process; instead, they adhere to the principle of self-regulation, wherein conformity is demonstrated through a declaration from the manufacturer, typically validated by a conformity assessment body. Whoever manufactures or distributes medical devices is required to establish a reporting system and notify Swissmedic of adverse effects and incidents (Art. 59 TPA), whereupon Swissmedic can take the necessary action in a particular instance, including recalls (Art. 66(2) TPA).

As of 1 July 2026, registration of all medical devices, systems and treatment units placed on the Swiss market will be mandatory in the Swiss medical devices database (swissdamed), which is based on the EU database EUDAMED. Voluntary registration has been possible since August 2025.

Nevertheless, comprehensive regulation of AI/ML in Switzerland is not anticipated, as the Federal Council declared in February 2025 that sector-specific AI regulations will be implemented into existing legislation, rather than a general horizontal AI legislation.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

See question 2.2 above.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

See question 2.6 above.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Digital health products are typically classified as medical devices (see question 2.4 above) as regulated by the TPA and the MedDO. Due to their nature as federal laws, the Cantons lack legislative authority but play a role in the law's enforcement: on the one hand, Swissmedic operates with the Cantons' involvement (Art. 68(1) TPA), as the Cantons have the right to nominate members to the Swissmedic Agency Council (Art. 72(2) TPA); on the other hand, the Cantons are tasked with regulating points of sale, particularly medical practitioners, and issuing retail trade licences for the sale of therapeutic products, including digital health products, in establishments such as pharmacies and drugstores, as well as overseeing the related inspection system.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

See question 2.6 above.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Telemedicine and virtual healthcare are well-established practices in Switzerland (see question 1.2 above). Except for specific cantonal regulations, telemedicine is not governed by any legal provision. However, telemedicine is permitted to a certain extent by the regulations that govern the professional obligations of physicians so long as it satisfies the obligations of the duty of care.
- **Robotics**
  Depending on their intended use, robotics in healthcare may be classified as medical devices and, thus, subject to the relevant medical device regulations (especially TPA and MedDO).
- **Wearables**
  Wearables collect and process vital signs (heartrate, blood pressure, etc.), which from a legal perspective qualify as personal data. Accordingly, the collection and processing of such data must comply with the FADP. Additionally, if these devices qualify as medical devices due to their potential for medical applications (refer to question 2.6) they must comply with regulatory requirements applicable to medical devices.
- **Virtual Assistants (e.g. Alexa)**
  See question 3.1, Wearables.
- **Mobile Apps**
  See question 3.1, Wearables.
- **Software as a Medical Device**
  See questions 2.2 and 2.6.

- **Clinical Decision Support Software**
  See question 2.6.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  See questions 2.5, 8.1 and 8.2.
- **IoT (Internet of Things) and Connected Devices**
  Depending on their intended use, IoT and connected devices in healthcare may be classified as medical devices.
- **3D Printing/Bioprinting**
  A fact sheet pertaining to the 3D printing of medical devices was released by Swissmedic. Swissmedic distinguishes in this regard between adaptable medical devices, mass-produced/patient-matched medical devices and custom-made devices (Art. 10 MedDO). Bioprinting technology may give rise to several regulatory and legal concerns pertaining to transplantation, gene technology, intellectual property and liability law.
- **Digital Therapeutics**
  The term "digital therapeutics" encompasses a wide range of device-controlled therapy measures. Digital therapeutics, specifically, could potentially be impacted by both the regulatory requirements applicable to medical devices and the data protection provisions outlined in the FADP. See also question 2.5.
- **Digital Diagnostics**
  In Switzerland, like in the EU, the regulatory obligations pertaining to *in vitro* diagnostics are regulated in a specific legal statute, which is the *In Vitro* Diagnostic Medical Devices Ordinance (IvDO). The latter sets forth that it applies, *inter alia*, to software or systems, whether used alone or in combination, intended by the manufacturer to be used *in vitro* for the examination of specimens derived from the human body (Art. 3(1)(a) IvDO). Thus, digital diagnostics must meet the requirements of the IvDO. Depending on the manufacturer's intent, additional regulatory or legal requirements may apply (see also questions 2.1, 2.3 and 2.6).
- **Electronic Medical Record Management Solutions**
  See question 1.2, Electronic Patient Record (EPR).
- **Big Data Analytics**
  The regulatory approach on big data analytics is caught in a dilemma: whilst this technology raises significant data protection concerns, the purpose of a medical treatment using big data can only be achieved through transparency. Furthermore, there may be situations where legal requirements are in direct contradiction to each other.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain-based healthcare data sharing technology has the potential to streamline and increase the transparency of processes within the healthcare sector. However, Swiss healthcare regulatory authorities have not yet explicitly designated this technology as a target of regulation. Like other technologies, its legal or regulatory issues are thus contingent upon its specific objective. Accordingly, blockchain technologies that meet the criteria for medical devices might also be subject to their regulatory requirements.
- **Natural Language Processing**
  Natural language processing (NLP), i.e., the computer-based capability to comprehend spoken and written language in a manner analogous to that of humans, is not generally classified as a medical device. NLP may, notwithstanding, be susceptible to regulatory requirements applicable to medical devices, provided that the manufacturer explicitly designates it for medical use. Moreover, data protection requirements must be observed.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

In Cantons where digital platform providers are permitted to establish operations, the competent cantonal authority must issue an operating licence to such digital platform providers who wish to offer digital health services. This necessitates, *inter alia*, that the individual bearing the ultimate medical responsibility meets the prerequisites for ordinary physicians and that he/she directly and personally practises his/her profession. Nevertheless, delegation is permissible, specifically to practice assistants with sufficient training and oversight. The competent authority has the power to exercise discretion in determining the personnel that is necessary for the digital health activity.

Furthermore, it is mandatory to uphold medical confidentiality and ensure the safeguarding of patient records to prevent unauthorised access. Depending on the location of the digital platform provider, other and/or additional key issues may arise. Thus, a case-by-case assessment is always necessary.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The FADP governs the processing of personal data by private persons and federal bodies. Data processing activities of cantonal bodies are subject to the respective cantonal data protection legislation.

Personal data is defined as all information relating to an identified or identifiable natural person. Data of legal entities are not considered personal data. The FADP recognises so-called sensitive personal data for which stricter rules apply in certain aspects. Among others, health data is considered as sensitive personal data.

The FADP outlines several principles to be observed for the processing of personal data: processing must be lawful, conducted in good faith and proportionate. Personal data may only be used for the purposes for which it was collected, and those purposes must be made transparent to the data subjects. If personal data is no longer necessary for processing, it must be either destroyed or anonymised. Additionally, the processed personal data must be accurate and protected through appropriate technical and organisational measures. Finally, the law provides for several further obligations of data processors and for rights of the concerned data subjects.

It is important to note that in contrast to the EU GDPR, the FADP does not require a justification for every data processing activity by private persons. Therefore, data processing by private persons is in principle permitted unless explicitly prohibited by law.

In addition to the requirements stipulated by data protection legislation, healthcare professionals and their auxiliaries must adhere to professional confidentiality obligations, the breach of which is subject to criminal sanctions.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As outlined above, the FADP governs the processing of personal data by private persons and federal bodies, whilst data processing activities of cantonal bodies are subject to the respective cantonal data protection legislation (see question 4.1). This also applies to personal health data.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The FADP distinguishes between private data processors and federal bodies. Federal bodies are subject to more stringent requirements. Data processing by cantonal bodies is governed by the respective cantonal data protection legislation (see question 4.1). For example, healthcare professionals employed by cantonal hospitals are subject to the cantonal data protection legislation in question. Further, the FADP recognises so-called sensitive personal data (e.g., health data), for which stricter rules apply in certain aspects (see question 4.1).

4.4 How do the regulations define the scope of personal health data use?

Personal data may only be processed for the specific purpose for which it was collected, and which purpose is transparent to the individuals whose data is being processed, unless there exist grounds for justification (e.g., the data subject's consent, an overriding private or public interest, or an explicit legal basis). Moreover, federal bodies may only process personal data if there is a statutory basis for doing so.

The FADP contains a list of circumstances in which the controller may have an overriding interest. This may be the case, among others, if the data controller processes personal data for non-personal purposes, such as research, planning or statistics, provided that the following requirements are satisfied: in such cases, the data controller must (a) anonymise the personal data as soon as the processing purpose allows, or if anonymisation is not feasible or requires disproportionate effort, implement appropriate measures to prevent the identification of the data subject, (b) disclose personal data that includes sensitive personal data (such as health data) to third parties in a manner that renders the data subject unidentifiable, and if this is not possible, guarantee that the respective third parties process the personal data only for non-personal purposes, and (c) publish the results in a way that prevents the identification of the data subject.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The roles and responsibilities of the parties involved in data processing must be defined. In the case of the assignment of data processing to a third-party data processor, it is necessary to establish a written data processing agreement (DPA). A DPA should in particular set forth the rights and obligations of the parties, including the controlling rights of the data controller. Further, the data processor must undertake to implement and maintain adequate technical and organisational measures, which must be described in detail. For joint or independent data controllers, a contractual agreement is not mandatorily required, unlike under EU GDPR. However, it might nevertheless be advantageous in many instances to define at least the basic responsibilities of each party regarding the respective data processing activities in writing.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The principle applies that only accurate personal data may be processed. Every data subject has the right to have inaccurate personal data corrected. Furthermore, the constitutional prohibition of discrimination also applies to the processing of personal data by federal bodies.

If a decision, which produces legal effects for a data subject or significantly affects a data subject, is based on automated decision-making, the data controller shall, upon request, provide the data subject with the opportunity to make a statement. The data subject may also request that the automated decision-making be reviewed by a natural person.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The FADP and cantonal data protection laws set forth the principles governing the collection and use of personal health data. The Swiss Federal Health Insurance Act (HIA) imposes strict limits on how insurers can use health data, ensuring it is only processed for specific purposes, namely the provision of insurance services. In November 2025, a project for an E-HD with central data processing to be implemented by 2030 has been presented (see question 1.2, EPR). More generally, the eHealth Switzerland initiative aims at facilitating the secure exchange and management of health information, whilst giving patients control over who accesses their data. Finally, the Swiss Medical Association (FMH) has issued several guidelines directed at healthcare professionals, which outline the applicable data protection principles, and emphasise patient confidentiality and the necessity of informed consent.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the FADP, it is crucial to distinguish between sharing personal data with a data processor and sharing it with a third party. Subject to statutory or contractual confidentiality obligations (such as, for example, medical professional confidentiality obligations), the sharing of personal data with a data processor is generally permitted, requiring only a DPA, assurance of the data processor's data security and informing data subjects about the categories of recipients receiving their personal data. If the data controller is bound by professional

confidentiality obligations, generally the consent of the data subject is necessary.

If personal data is shared with third parties, stricter rules apply when it comes to the disclosure of special categories of personal data such as health data. The disclosure of such data by private processors requires either consent of the data subject, an overriding private or public interest or justification by law. Moreover, federal bodies may only disclose personal data (irrespective of whether sensitive or not) to third parties if there is a statutory basis for doing so, or if one of the statutory exceptions apply (see question 5.2).

Another critical consideration is the location where the shared data is processed. Personal data may only be transferred to countries that afford a level of protection which is deemed adequate from a Swiss law perspective. If personal data is disclosed to countries with data protection legislation of a comparatively lower standard, this is permissible only (a) with the data subject's consent, (b) under contractual agreements ensuring a level of data protection equivalent to Swiss standards, or (c) if any of the other statutory exceptions apply.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

See questions 5.1 and 5.3.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Here again, a distinction is made as to whether the data controller is a private person or a federal body.

For the processing of personal data (including disclosure) by a data controller who is a private person, see question 5.1.

Personal data may only be processed and disclosed to third parties by a federal body if there is a statutory basis or if one of the statutory exceptions apply (see questions 4.4 and 5.1). Additionally, personal data may be disclosed in the context of public information if it pertains to a public duty and there is an overriding public interest. The data subjects may object to the disclosure of certain personal data by federal bodies if they can demonstrate a protected interest. However, the federal body may disregard the objection if there is a legal duty to process the data or if fulfilment of the respective body's tasks would otherwise be jeopardised.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

As laid out, the FADP imposes requirements on the collection, processing and sharing of personal health data (see question 5.1). The HIA regulates the exchange of data between those responsible for implementing, monitoring or supervising the implementation of said act (see also question 4.7). The eHealth Strategy, overseen by the FOPH, aims at establishing an interoperable digital healthcare ecosystem that promotes secure and efficient data exchange. In particular, the EPRA shall be revised comprehensively and facilitate secure data sharing across healthcare providers, with patient consent as a central principle (see question 1.2, EPR). Further, see also question 5.5.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Federated models of healthcare data sharing must navigate complex regulatory considerations and technical challenges. Interoperability standards are the basic prerequisite to enable seamless data exchange across decentralised systems. Security measures, including encryption, access controls and audit trails, are essential to protect sensitive health information. Contractual frameworks, such as DPAs, clarify responsibilities and liabilities, particularly in the event of data breaches. To promote the digital transformation in the healthcare sector, the Federal Council has launched the so-called "*Digisanté* Project", being implemented since 2024 onwards. This project aims at creating a nationwide digital healthcare system for the secure and seamless exchange of data, including a medical register (see question 1.2, EPR above). All stakeholders shall obtain access to the relevant health information in accordance with data protection legislation. Data entry shall be performed in a uniform and standardised system, the "Swiss Health Data Space", which shall improve the quality and safety of the entire treatment chain, from prevention to diagnostics, treatment and care. Secure access to standardised data shall also help to promote academic and industrial medical research and the professional and political management of the healthcare system.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Digital health products regularly encompass both software and hardware elements. Patents for inventions are granted for new inventions applicable in industry. No specific requirements exist for innovations in the digital health sector. However, exclusions from patentability cover, among others, methods for treatment by surgery or therapy and diagnostic methods practised on the human or animal body. Also excluded are computer programs as such, which are protected by copyright law (see question 6.2). However, computer-implemented inventions, which solve a technical problem, are patentable.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The Swiss Federal Copyright Act (CopA) protects literary and artistic intellectual creations of individual character, irrespective of their value or purpose. Computer programs are explicitly recognised as copyright-protected works. Digital health software can therefore be protected by copyright if the requirements are met. It is worth mentioning that there are no specific formal requirements to obtain copyright protection in Switzerland. Copyrights are automatically established upon the creation of the respective work.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected by provisions of the Federal Unfair Competition Act and the Swiss Criminal Code. Furthermore,

the Swiss Code of Obligations stipulates that an employee may not utilise or disclose to others any facts to be kept secret, in particular manufacturing and business secrets, of which he or she becomes aware in the service of the employer. No specific provisions apply to digital health technologies.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Based on the laws described above, universities and colleges issue their own regulations concerning the utilisation of intellectual property in the context of university activities.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

See questions 6.1–6.4.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No, in principle only individuals can be named as inventors. Whilst a device or AI may contribute to the invention process, only a human being may be named as inventor. Nevertheless, there is an ongoing debate in Switzerland regarding whether it is necessary for an inventor to be a natural person. A notable case regards the AI system DABUS: on 26 June 2025, the Swiss Federal Administrative Court ruled that when applying for a patent, a natural person must be named as the inventor (FAT B-2532/2025).

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The Federal Act on the Promotion of Research and Innovation sets the legal basis for the promotion of research and of aspects of innovation in Switzerland. Together with the Federal Act on Funding and Coordination of the Swiss Higher Education Sector, it defines the legal framework for scientific activities in Switzerland.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Several key precedents in the realm of intellectual property rights concern digital health innovation. The Swiss Federal Patent Court has issued several rulings clarifying the scope of patentability for digital health technologies. Finally, an example relating to trademark law regards the rejection of the registration of the trademark "ID NOW" for medical devices by the Federal Administrative Court, based on the grounds that said sign was considered descriptive of the respective goods (FAT B-1776/2023). The ruling clarifies the high standards of distinctiveness required for trademarks and reiterates that trademarks must not give rise to misleading expectations as to the functionality or performance of the respective products, which also applies in the area of medical devices. See also question 6.6.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

In practice, collaborative agreements are frequently entered into with universities, non-university research institutions and/or other industrial partners, in addition to internal research and development activities. As a starting point, the involved parties need to determine whether they are interested in engaging in a research collaboration or in conducting contract research. Research cooperation agreements are frequently considerably more complex than mere research agreements due to various regulations governing the transfer of IP rights and their compensation.

Furthermore, to facilitate the commercial exploitation of the work results from such collaboration, it is essential that the respective party's intellectual property rights be protected. Additionally, publication rights, marketing rights, regulatory responsibility and product liability ought to be contractually agreed upon.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

In addition to the aforementioned aspects (see question 7.1) and the core healthcare regulatory schemes to be complied with (see question 2.1 *et seq.*), particular attention must be given to ensuring that healthcare companies and their employees do not obtain undue benefits (Art. 55(1) TPA). The existence of an undue benefit must be determined on a case-by-case basis; benefits of modest value (up to CHF 300 annually) or in support of research, further education or training, contingent upon fulfilling specific criteria are, for example, not considered as "undue" (Art. 55(2)(a)(b) TPA).

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Federated learning (FL) in healthcare is the process of developing ML models over datasets that are distributed across various data centres (e.g., hospitals, clinical research labs and mobile devices) without exchanging the data itself. Companies dealing with agreements establishing such collaboration and data sharing must determine whether they are members of a FL consortium in which all other parties are trustworthy prior to proceeding (i.e., whether attempts to corrupt the model or intentionally extract sensitive information can be excluded). Furthermore, by definition, FL systems prevent the exchange of health-related data among participating institutions. However, through reverse engineering, the shared information may still indirectly expose private (highly sensitive) health data (i.e., leakage risk). Mitigation of the results from all these risks is required.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

See questions 8.3, 8.4 and 9.3.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

See questions 2.5, 2.6 and 2.8.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

See questions 2.4 and 2.8.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Intellectual property may only be created by a natural person (i.e., a human being) in accordance with Swiss copyright and patent law (Art. 6 CopA; Art. 3(1) Patent Act). As a result, advancements achieved through ML without explicit human intervention do not qualify as inventions protected under Swiss intellectual property law. Nevertheless, dissenting views exist regarding the allocation of credit to the algorithm's owner (e.g., programmer) for works and inventions generated by algorithms. However, ownership cannot be acquired by or through an algorithm.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

When procuring data for ML, it is crucial to consider significant commercial factors. These include, but are not limited to: (i) establishing data ownership and intellectual property rights; (ii) defining financial terms including fees and royalties; (iii) addressing concerns related to data security and confidentiality; and (iv) ensuring adherence to applicable laws and regulations, with particular emphasis on privacy. The application of ML in digital health technologies may potentially involve sensitive personal data, which raises several obligations under the FADP (see question 1.3).

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

As far as can be seen, no established practice has yet emerged among regulatory bodies overseeing AI/ML technologies to differentiate between standard AI and generative AI technologies and products.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction?

Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

See question 8.5 above.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

If AI/ML models are trained on data for which the developer lacks the appropriate data rights, the developer may face legal consequences under the FADP (see question 4.1 *et seq.*). Any person may request from a data controller information about the processing of personal data concerning him or her, which he or she has provided to the data controller, in a commonly used electronic format, if (i) the controller processes the data by automated means, and (ii) the data are processed with the consent of the data subject or in direct connection with the conclusion or performance of a contract between the controller and the data subject (Art. 28(1) FADP).

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Digital health solutions are subject to the general rules on contractual and tort law liability. In addition, the regulations governing therapeutic products stipulate that whoever manufactures or distributes therapeutic products (including but not limited to digital health solutions) is required to establish a reporting system and notify Swissmedic of adverse effects and incidents that (i) are attributable to the therapeutic product itself, its use or improper instructions for use, or (ii) may endanger the health of consumers, patients, third parties or animals (Art. 59(1) TPA). Furthermore, quality issues must be reported to Swissmedic (Art. 59(2)(3) TPA).

Violations of the reporting obligations primarily trigger criminal law consequences (Art. 87(1)(c) TPA). However, civil liability may also apply based on (i) the Swiss Product Liability Act, which is based on the EU product liability directive, (ii) contract law, and/or (iii) tort law. In addition, a manufacturer may be held jointly and severally liable with any authorised representative in Switzerland of a person injured by a digital health solution that qualifies as a defective medical device (Art. 47d(2) TPA).

A certificate of conformity (CoC) for a digital health solution that qualifies as a medical device may be an indicator that the product is not defective. However, such CoC does not exempt a manufacturer of the respective product from potential product liability claims.

9.2 What cross-border considerations are there?

Anyone who manufactures a digital health solution that qualifies as a medical device in Switzerland, or who makes it available in Switzerland, must report any adverse reactions suspected of being associated with this medical device to

Swissmedic (Art. 66(1) MedDO). The response to such alerts is entirely up to Swissmedic's discretion. However, recalls in the US and/or the EU may encourage Swissmedic to consider similar administrative measures in Switzerland, as well.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

When deploying generative AI in Swiss digital health solutions, (i) compliance with the FADP, (ii) assurance of transparency and informed consent from users, as well as (iii) maintenance of accuracy and dependability via routine validation and documentation should take precedence. The incorporation of professional oversight and human intervention mechanisms are crucial in the healthcare decision-making processes. User agreements should incorporate unambiguous liability disclaimers and limitations, which underscore the technology's supportive nature. Furthermore, it is imperative to enforce strict cybersecurity protocols and to ensure ongoing training for healthcare professionals.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Swiss civil law may hold entities accountable under contractual and non-contractual theories for harm caused by negligent or improper use of AI/ML models, including medical malpractice claims if AI decisions lead to medical errors or harm. Furthermore, under the FADP, misuse can lead to violations of privacy rights and data protection, especially if sensitive health data is processed without consent or adequate safeguards. Additional liability provisions may apply.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based digital health services and their interfaces are usually hosted on external systems and sometimes even spread across several platforms. Therefore, when sharing data with other parties, key concerns are data security, namely the potential for unauthorised disclosure of personal data, the encryption and interoperability of data, the coordination of access and incident management, as well as data protection issues since cloud-based services for digital health store substantial quantities of very sensitive data (see question 4.1). In addition, it is necessary to ascertain whether the cloud-based services for digital health meet the criteria to be classified as a medical device (see question 2.3).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Digital health products and/or services are subject to rigorous regulation and oversight. Therefore, regulatory and data protection considerations necessitate a thorough assessment of the respective company's business model and its intended use of products and/or services. A comprehensive compliance organisation considering, among others, the aforementioned factors should be established prior to the entry of non-healthcare companies into the digital healthcare market. Ultimately, we recommend evaluating whether Swiss compulsory health insurance may potentially cover the cost of the digital health products and/or services in question (see questions 2.2 and 10.6).

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Key topics that should be considered before investing in digital healthcare ventures are the adherence to the constantly evolving data protection requirements, the necessity for comprehensive title-chain documentation, the ramifications of employee stock-option plans, and the identification and adherence to relevant healthcare regulatory schemes (see questions 2.1 *et seq.*).

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

High market-entry barriers, a complex procedure for registering new products or services for reimbursement by compulsory health insurance, and a complex regulatory framework in general are the key barriers for new digital health solutions in Switzerland. In addition, Switzerland is a federal state comprising 26 Cantons, each of which may have its own regulatory requirements on certain healthcare aspects. Moreover, the presence of four official languages in Switzerland may necessitate the employment of multilingual staff depending on the business model, products or services.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The FMH is the professional association of all Swiss physicians and issues the FMH Code of Ethics and its appendices, which must be observed by all physicians. Given that the implementation of digital health solutions is essentially governed solely by law, the FMH's influence is limited to political advocacy work for its members' interests and those of patients to influence the respective legislative process.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

The possibility of reimbursement by mandatory health insurance for the use, rental or sale of digital health solutions is governed by the HIA and its ordinances. The FOFP is the competent authority in all matters relating to this. Several digital health solutions already exist in Switzerland, which are reimbursed by mandatory and/or private insurances. Nevertheless, the approaches utilised for this are highly dependent on the structure of this digital health solution. For instance, in most Cantons, the reimbursement application for

a telemedicine solution can be submitted together with the request to carry out such an activity. Therefore, a case-by-case assessment is recommended.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

In Switzerland, certain due diligence gaps within the healthcare ecosystem for evaluating digital health solutions may create challenges for stakeholders in maintaining safety, compliance and ethical standards. Identified gaps encompass: (i) data governance, characterised by insufficient clarity regarding data ownership, consent management and compliance with data protection requirements, especially for sensitive health data; (ii) algorithm transparency, marked by limited understanding of AI/ML models' decision-making processes, which may give rise to liability and unfair competition risks; (iii) regulatory oversight, with the absence of specific regulations for AI/ML in healthcare (see question 2.5), resulting in uncertainties related to compliance with medical device regulations and standards for safety and efficacy; (iv) interoperability, emphasising challenges in ensuring secure and effective integration of digital health solutions with existing healthcare systems and standards; and (v) clinical validation, indicated by the lack of robust frameworks for the ethical evaluation and clinical validation of AI/ML models in medical contexts, potentially undermining trust and effectiveness.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

In addition to the issues mentioned above, the evolution of Swiss regulatory (digital) health policy is to be seen in conjunction with similar EU policy. Given that Switzerland's largest trading partner is the EU, and that Switzerland exports a significant quantity of therapeutic products to EU Member States, the Swiss legislator strives for a comprehensive harmonisation of Swiss and EU legislation. Consequently, developments in Swiss digital health are also profoundly influenced by EU regulatory developments.

A recent development further reinforcing this alignment is Switzerland's association with key EU programmes, such as Horizon Europe and the Digital Europe Programme, retroactively applied from early 2025. This participation strengthens opportunities for Swiss researchers and innovators in digital health to collaborate with EU partners, secure funding, and engage in EU-wide initiatives, thus fostering innovation and regulatory alignment.



Tobias Meili is a Partner in the practice groups Governance & Compliance, Life Sciences & Health Law, and M&A/Corporate. He advises clients, particularly in the life sciences sector, on commercial and corporate law, especially on corporate governance (including corporate responsibility issues), restructuring, M&A, and contract and technology law. His area of activity also includes internal investigations as an examiner or investigator appointed by FINMA or companies.
Due to his many years of experience in a leading position in the legal department of a formerly SMI-listed multinational corporation and an international consulting and technology company, Tobias Meili is familiar with the structures, processes, and challenges of large companies. In his legal practice, he combines an authentic, pragmatic, and solution-oriented advisory approach with solid legal expertise and negotiation skills.

Wenger Plattner
Aeschenvorstadt 55, 4010 Basel
Switzerland

Tel: +41 61 279 70 00
Email: tobias.meili@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/tobiasmeili



Carlo Conti is Of Counsel in the field of Life Sciences and Health Law. He advises institutions and organisations on issues related to life sciences and health law, as well as on constitutional and administrative law matters. He is president or member of various boards of directors.
He has many years of professional experience and profound knowledge in all areas of life sciences and health law, as well as in constitutional and administrative law. For more than 15 years, he held executive positions in the pharmaceutical industry. Subsequently, Carlo Conti became a member of the state government in Basel-Stadt and head of the public health department. He was also president of the Swiss Conference of Public Health Ministers and chairman of the board of Swiss DRG AG, as well as vice president of the board of Swissmedic (the Swiss Agency for Therapeutic Products).

Wenger Plattner
Aeschenvorstadt 55, 4010 Basel
Switzerland

Tel: +41 61 279 70 00
Email: carlo.conti@wenger-plattner.ch
URL: www.wenger-plattner.ch/en/team/conti-carlo



Martina Braun is a Partner and a member of the practice groups IP, IT & Data Protection as well as Sports Law. She advises national and international companies and start-ups as well as associations, foundations and private individuals comprehensively on contractual matters and represents them in complex negotiations.
Her focus lies in copyright, trademark, personality and data protection law. She has extensive experience in the commercialisation of intangible assets and specialises particularly in licensing and sponsorship agreements in the sports and entertainment industries.
Martina Braun has written a dissertation on copyright law and completed a CAS in international sports law. She also publishes regularly on IP law and is active in professional organisations.

Wenger Plattner
Seestrasse 39, 8700 Küsnacht-Zurich
Switzerland

Tel: +41 43 222 38 00
Email: martina.braun@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/martina-braun-81930b20



André S. Berne is a Senior Associate and primarily handles commercial law and various regulatory issues. His main areas of focus include life sciences law, health law, competition law, data protection law, and general contract law.
He also advises companies and organisations on Swiss commercial and corporate law, administrative law, and EU law, and represents them before courts and authorities in German and French.
In addition to his advisory and litigation activities, André S. Berne prepares expert opinions in his areas of specialisation. He regularly publishes and lectures in these fields.

Wenger Plattner
Aeschenvorstadt 55, 4010 Basel
Switzerland

Tel: +41 61 279 70 00
Email: andre.berne@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/andr%C3%A9-s-berne-866b0199

Wenger Plattner has been advising and representing clients in all aspects of business law for over 40 years, and has offices in Basel, Zurich and Bern. The lawyers identify practical, workable solutions and help clients implement these to achieve the best possible commercial outcomes. Wenger Plattner has a team of experts, many of whom are involved in decision-making as members of public authorities and other bodies, giving them an in-depth understanding of client needs. As a fully integrated partnership, the firm places a strong emphasis on teamwork and co-operation. Wenger Plattner's clients have access to dedicated, highly experienced specialists who offer top-level advice to help them meet their specific objectives efficiently and effectively.

www.wenger-plattner.ch

Wenger Plattner

Taiwan


Tsung-Yuan Shen


Rachel Chen


Nita Ye

Lee and Li, Attorneys-at-Law

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no clear definition of "digital health" under Taiwanese law.

The definition of "digital medicine" provided in Article 4, Paragraph 1, Item 7 of the Act for the Development of Biotech and Pharmaceutical Industry may serve as a reference. Under such Act, "digital medicine" refers to an innovative product or technology that is applied in the field of healthcare with big data, cloud computing, Internet of Things (IoT), artificial intelligence (AI) and/or machine learning (ML) technologies, and is used to enhance the prevention, diagnosis and treatment of diseases, as approved by the competent authority in conjunction with the central governmental authority in charge of the subject industry. Notably, the medical device software using AI or ML technology shall be subject to the approval of the central governmental authority in charge of the subject industry.

Generally, "digital health" encompasses various domains, including mobile health, health information technology, wearable technology, telehealth and telemedicine, personalised medicine, and other uses of information and communication technology within the healthcare fields.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

In recent years, there have been significant investment in and development of medical technologies and digital health solutions. These include healthcare big data, IoT, AI, 5G technology, biomedical chip technology, sensors, wearable devices, biobanks, telehealth and telemedicine. Much of this investment and development has been encouraged by government organisations.

1.3 What is the digital health market size for your jurisdiction?

According to National Science and Technology Council (NSTC), digital healthcare revenue in Taiwan has been growing in recent years, reaching NT$ 50.2 billion (around US$ 1.67 billion) in 2022, NT$ 55 billion (around US$ 1.75 billion) in 2023, and NT$ 60.5 billion (around US$ 1.93 billion) in 2024, with an annual growth rate of approximately 10%.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

In Taiwan, the digital health market is primarily funded by leading electronic technology companies. Since these companies report their revenue based on overall enterprise performance, it is challenging to isolate their earnings or establish a ranking specifically within the digital health sector.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

As noted above, it is currently not easy to quantify or rank companies' performance in digital health. Many Taiwanese companies are investing considerable resources and efforts in this emerging industry. Benefitting from the advanced technologies, these companies are developing rapidly and each company has its own strengths.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Ministry of Health and Welfare (MOHW) is the competent authority responsible for supervising healthcare-related matters, products and industries. The MOHW has a wide-ranging mandate aimed at enhancing the quality of healthcare service.

Under the MOHW, the Food and Drug Administration (TFDA) oversees the regulation of food, drugs, medical devices and cosmetics to ensure their safety and quality. The TFDA is responsible for granting product registrations and approving clinical trials, as well as monitoring manufacturing processes and imports. The TFDA also conducts safety surveillance activities for health-related products.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The Medical Devices Act provides core regulations governing medical devices. Regarding digital health in the context of

a medical device, such aspect falls under the purview of the Medical Devices Act. According to the Medical Devices Act, the term "medical device" refers to instruments, machines, apparatuses, materials, software, reagents for *in vitro* use and related articles thereof, whose design and use achieve one of the following primary intended actions in or on the human body by means other than pharmacological, immunological, metabolic or chemical means: (a) diagnosis, treatment, alleviation or direct prevention of human diseases; (b) modification or improvement of the structure and function of the human body; and (c) control of conception.

From a legal perspective in Taiwan, the manufacture or import of medical devices can only be conducted once a medical device permit licence, which provides registration and market approval, has been issued by the MOHW. Furthermore, the production of medical devices must adhere to the guidelines established in the Good Manufacturing Practice (GMP) under the Pharmaceutical GMP Regulations.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The Medical Devices Act establishes a three-tiered classification system for medical devices based on risk levels: Class I for low-risk products; Class II for medium-risk products; and Class III for high-risk products.

Separately, any person who manufactures or imports medical devices without obtaining the prior approval could face imprisonment for up to three years, along with the possibility of an administrative fine not exceeding NT$ 10 million.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

In addition to the regulations discussed in our response to question 2.2, the Guidance for Medical Software Classification issued by the TFDA is also relevant to software as a medical device. On December 24, 2020, the TFDA published a revision to this Guidance, clarifying that medical software designed to monitor heart rate and blood oxygen levels (including wearable devices) for everyday health management of the general public is not classified as a medical device, provided it is not intended for disease diagnosis or treatment. On September 15, 2022, the TFDA published another revision to the Guidance, which adds multiple examples not classified as a medical device and the evaluation criteria for classifying medical software. However, the actual classification for a particular device is determined at the discretion of the competent authority.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

There are currently no specific regulations established particularly for AI/ML-powered digital health devices or software solutions. All medical devices fall under the purview of the Medical Devices Act, with Chapter IV outlining regulations related to the management of clinical trials for such devices. In addition to the Medical Devices Act, the relevant rules such as the Regulations on Good Clinical Practice for Medical Devices, the Human Subjects Research Act and the Regulations on Human Trials should be taken into consideration.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

On September 11, 2020, and August 16, 2021, the TFDA published the Guidance for the Inspection and Registration of Medical Software of AI/ML-based Technologies. The Guidance describes the inspection and registration checkpoints for medical software using AI/ML-based technologies. Additionally, such Guidance is also applicable to the medical devices using AI/ML-based technologies.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Currently, all medical devices fall under the purview of the Medical Devices Act. In accordance with Article 37, Paragraph 1 of the Medical Devices Act, before initiating any clinical trial, the clinical trial institutions or trial sponsors shall file an application with the TFDA for prior approval.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

All digital health products and solutions classified as medical devices are regulated by the Medical Devices Act. The applicability and regulatory density do not vary between regional and country levels.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

The TFDA has published several guidelines that take into account the progress and advancement of technologies such as AI and ML for applicants' reference.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Under the Physicians Act, physicians are generally prohibited from treating or prescribing medication for patients they have not personally diagnosed, except in urgent situations or for those in remote areas. The Rules of Medical Diagnosis and Treatment by Telecommunications specify which locations qualify as mountainous, outlying islands or remote areas.
- **Robotics**
  The legal and regulatory issues for robotics as medical devices are similar to those for telemedicine, particularly regarding medical device regulations, personal data protection and product liability.
- **Wearables**
  The legal and regulatory issues for wearables as medical devices are similar to those for telemedicine, particularly regarding medical device regulations, personal data protection and product liability.

- **Virtual Assistants (e.g. Alexa)**
  The legal and regulatory issues for virtual assistants are similar to those for robotics.
- **Mobile Apps**
  The legal and regulatory issues for mobile apps are similar to those for wearables.
- **Software as a Medical Device**
  The legal and regulatory issues for software as a medical device are similar to those for wearables.
- **Clinical Decision Support Software**
  These technologies face regulatory scrutiny similar to that applied to robotics, especially concerning the Physicians Act, if AI assumes roles traditionally held by physicians.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  The legal and regulatory issues for AI/ML-powered digital health solutions are similar to those for robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **IoT (Internet of Things) and Connected Devices**
  These areas are governed by regulations similar to those applied to wearables and robotics, with specific concerns regarding the Physicians Act for AI applications.
- **3D Printing/Bioprinting**
  The legal and regulatory issues for 3D printing/bioprinting are similar to those for wearables.
- **Digital Therapeutics**
  The legal and regulatory issues for digital therapeutics are similar to those for robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **Digital Diagnostics**
  The legal and regulatory issues for digital diagnostics are similar to those for robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **Electronic Medical Record Management Solutions**
  The legal and regulatory issues for electronic medical record management solutions are similar to those for wearables.
- **Big Data Analytics**
  The legal and regulatory issues for big data analytics are similar to those for robotics, if the results of data analysis will be used as the basis for diagnosis or treatment.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The legal and regulatory issues for blockchain-based healthcare data sharing solutions are similar to those for wearables.
- **Natural Language Processing**
  There are no special regulations related to Natural Language Processing.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The Personal Data Protection Act (PDPA) serves as the primary legislation regulating the use, collection and processing of personal data to protect individual rights and ensure the responsible use of such information. Digital platform providers must adhere to the requirements outlined in the PDPA whenever personal data is involved in their products or services.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The PDPA serves as the primary legislation for personal data protection. Key considerations for the use of personal data under the PDPA include, but are not limited to, the following points:

- Determining whether the data qualifies as "personal data" under the PDPA.
- Assessing whether the "personal data" is considered "sensitive personal data" as defined in our response to question 4.4.
- Ensuring that the use of personal data adheres to the relevant regulations of the PDPA, including the necessity of obtaining informed consent from the data subject, or whether there is any exemption from the applicable requirements.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal data, including personal health data, is regulated by the PDPA. The applicability and regulatory density do not vary between regional and country levels.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The considerations listed in our response to question 4.1 remain consistent, irrespective of the nature of entities involved. However, the types of exemptions from the requirement to obtain informed consent from the data subject vary between non-governmental and governmental entities.

4.4 How do the regulations define the scope of personal health data use?

Under the PDPA, "personal data" is defined in a broad manner to encompass various types of information, including: name; date of birth; identification card number; passport number; physical characteristics; fingerprints; marital status; family details; educational background; occupation; medical records; information regarding medical treatment; genetic data; details about sexual life; health examinations; criminal history; contact information; financial status; social activities; and any other information that could directly or indirectly identify an individual.

Furthermore, personal data related to an individual's medical records, healthcare, genetic information, sexual life, physical examinations and criminal record is categorised as "sensitive personal data", which is subject to more stringent regulations under the PDPA.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

If any collection, use or processing of personal data is contemplated under a contract, it is suggested that the "informed consent" requirement be fully complied with, unless any applicable exemptions are met.

Adhering to the PDPA, especially in securing the necessary "informed consent" for the use, collection and processing of personal data, as well as ensuring that the use and processing of such data remain within the defined scope of specific purposes, is a critical legal concern. Any breach of the PDPA, such as the unlawful use, collection or processing of personal data, could result in civil, criminal and/or administrative penalties.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Regarding personal health data inaccuracies, the PDPA grants data subjects the right to correct or supplement their personal information, as well as the right to request the deletion of the data.

In respect of data bias and discrimination, there are currently no specific laws or regulations in place to tackle such issues. However, we anticipate that discussions will increasingly arise in various legal fields, including labour and employment law (concerning factors such as gender, race, religion or beliefs, and political views), privacy law, antitrust law and other areas where concepts of "equality" and "fairness" are significant to social and economic activities. This is particularly relevant in light of challenges that may arise from the use of AI algorithms and big data analytics.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Since its launch in 1995, Taiwan's National Health Insurance (NHI) system has been managed by the National Health Insurance Administration (NHIA), which oversees a vast amount of personal data. The NHIA delegated data management to the National Health Research Institute, which created the National Health Insurance Research Database for external research from 2000 to 2016. In response to concerns about data privacy, seven individuals objected in 2012 to the NHIA's release of their personal data to third parties, leading to petitions and lawsuits that were ultimately unsuccessful. In 2017, they sought a constitutional interpretation regarding the legality of the data release.

In August 2022, Taiwan's Constitutional Court ruled that laws must be revised within three years to enhance personal data protection under the PDPA. Key requirements included establishing an independent oversight mechanism, clarifying regulations for NHI data usage, and allowing individuals to opt out of data usage.

To comply, the PDPA was amended in May 2023, designating the Personal Data Protection Commission (PDPC) as the authority overseeing these regulations. A Preparatory Office for the PDPC has been established, with the official commission expected to launch soon. In November 2025, the PDPA was further amended to realign the authority and responsibilities following the official establishment of the PDPC. This latter amendment not only clarified and enhanced the PDPC's regulatory oversight but also expanded the surveillance responsibilities of government entities. Additionally, the revised PDPA promotes greater collaboration between central and local government bodies in regard to personal data protection. The effective date of the amended PDPA is pending determination by the Executive Yuan.

In May 2025, the Executive Yuan released the draft National Health Insurance Data Management Act aimed at enhancing the governance of health insurance data. The proposed legislation seeks to establish an advisory council to oversee data management practices, implement standardised protocols for data handling and transmission, and introduce provisions allowing data subjects to opt out of data sharing. Following its submission, the draft legislation underwent review by the Legislative Yuan and is currently pending further negotiation and revision.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Please refer to our response to question 4.1 above, as sharing personal data would be classified as "processing" and/or "use" of personal data under the PDPA.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Please refer to our response to question 4.2 above, as sharing personal data would be classified as "processing" and/or "use" of personal data under the PDPA.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Please refer to our response to question 4.3 above.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please refer to our response to question 4.7 above.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Regarding federated models for sharing healthcare data, the concerns outlined in our answers to questions 4.1 through 5.4 are relevant and should be noted. For instance, the requirement for "informed consent" should be adhered to unless any of the applicable exemptions are met.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

The Patent Act defines patentable subjects as inventions, utility models and designs. An invention refers to technical ideas that leverage natural laws, while a utility model pertains to the shape or structure of an article, also based on natural laws. Designs focus on the aesthetic aspects, such as shape, pattern or colour, and can include applications for computer-generated icons and graphic user interfaces. For any of these categories to be patentable, they must meet requirements of novelty, inventive step and enablement. However, diagnostic, therapeutic and surgical methods for human treatment are excluded from patentability, which may affect digital health technologies that incorporate such methods.

Additionally, digital health inventions may involve software or algorithms, which are assessed under the Examination Guidelines for Computer-related Inventions. These guidelines classify software patents into three categories: process (specific operational steps using a computer); product (programmable devices directed by software); and computer-readable storage medium (articles that instruct a computer to perform functions). Software patents are deemed patentable if they effectively interact with computer systems to deliver technological advancements.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Under the Copyright Act, a "work" refers to a creation in the literary, scientific, artistic or other intellectual domains. This encompasses oral and literary works, musical compositions, dramatic and choreographic pieces, artistic creations, photographic images, pictorial and graphical works, audiovisual materials, sound recordings, architectural designs and computer programs. While there are no registration or filing requirements for copyright, certain criteria must be met for a work to qualify for protection, including "originality" and "expression". Additionally, software developed for "digital health" is eligible for copyright protection.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected when they meet the following criteria: the information must be applicable in production, sales or operations; the information must possess a degree of secrecy; the information must have economic value; and the owner must have taken reasonable steps to maintain its confidentiality. There are no registration or filing requirements for legal protection of a trade secret. To maintain confidentiality during court proceedings, trials may be conducted privately if deemed appropriate by the court or agreed upon by the parties involved. In intellectual property (IP) lawsuits, parties can request the court to issue a "protective order". Individuals bound by such an order are prohibited from using the trade secrets for any purpose unrelated to the trial and must not disclose the secrets to anyone not covered by the order.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Academic institutions typically establish internal guidelines regarding academic technology transfers. In general, these internal policies outline the ownership and management of technologies developed by scholars, researchers, graduate students and staff. Furthermore, institutions have the authority to license or assign their IP to third parties for commercial purposes, ensuring that the innovations generated within academia can be effectively utilised in the marketplace while adhering to established legal frameworks.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Software can be protected through various rights, including patents, copyrights and trade secrets. Specifically, for software-implemented inventions that combine software and hardware to process information and achieve a technical effect, patent protection is often available. This legal framework ensures that developers can safeguard their innovations, fostering an environment conducive to technological advancement in the medical field.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

The Taiwan Intellectual Property and Commercial Court has specifically determined that AI cannot be designated as an inventor of a patent. Judicial practice, particularly rulings from the Taiwan Intellectual Property and Commercial Court, holds that patent inventions stem from the creative capacities of the human spirit, which AI lacks. According to Taiwanese law, only natural or legal persons are entitled to hold such rights.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Government-funded inventions are governed by specific IP rights as outlined in the Fundamental Science and Technology Act and the Government Scientific and Technological Research and Development Results Ownership and Utilization Regulations. When projects in scientific and technological research and development (R&D) receive government support, the management and utilisation of the resulting R&D outcomes must adhere to such regulations.

Notably, the R&D results and any income generated may be partially or wholly assigned to the executing R&D units for ownership or licensing, and are exempt from the National Property Act. Furthermore, the determination of ownership and utilisation rights is guided by principles of fairness and effectiveness. This assessment considers various factors, including the contributions of capital and labour, the nature of the R&D results, their potential applications, societal benefits, national security implications and market impact.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

In Taiwan, there are currently no notable judicial precedents specifically addressing IP rights concerning digital health innovations. The Taiwan Intellectual Property and Commercial Court has determined that AI cannot be recognised as an inventor for patent purposes, and that patent inventions must originate from human creativity, as only natural or legal persons can hold such rights under Taiwanese law.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Effective collaboration relies on well-defined agreements concerning IP ownership, obligations and responsibilities. It is crucial to evaluate applicable laws and agreements among involved parties, especially between funding providers and inventors or developers. Typically, IP laws state that ownership of collaborative improvements is governed by existing agreements; in their absence, rights generally belong to the inventor or developer, while the funding provider may utilise the invention.

In copyright scenarios, the creator is recognised as the author and retains economic rights unless a mutual agreement specifies otherwise. Although the funding provider can use the work, ownership rights remain with the author. Co-ownership of improvements requires adherence to specific provisions in the Patent Act. Joint patent applications must be filed collectively, and any independent filing by a co-owner risks patent cancellation by others. Furthermore, joint patent rights cannot be assigned or abandoned without unanimous consent from all co-owners; if a co-owner abandons their share, such share reverts to the remaining owners. Ultimately, clear agreements are essential for clarification of IP rights in collaborative endeavours.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

As stated in our response to question 2.2 above, the manufacturing or importation of medical devices is permitted only after a medical device permit licence has been issued, granting registration and market approval. Therefore, determining whether the company possesses or is required to obtain such permit licence is a crucial matter.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Please see our response to question 5.5 above.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

In general, when two or more parties are involved in the use of generative AI, they should consider several factors, including the internal allocation of risks related to contractual liabilities, tort liabilities and criminal liabilities, as well as agreements on the ownership of IP rights (if applicable) and data sharing or transfer.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

In Taiwan, the principal regulatory authorities overseeing AI and ML enforcement include the Executive Yuan and the NSTC. In February 2023, the Executive Yuan launched the Taiwan AI Action Plan 2.0 (2023–2026) to guide government policy. Until early 2025, the NSTC held responsibility for drafting legislation related to AI. Such responsibility was subsequently transferred to the Ministry of Digital Affairs.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

As indicated in our response to question 8.1 above, there are currently no comprehensive regulations governing AI/ML; however, a draft of the Fundamental Law on Artificial Intelligence was provided in August 2025. The Executive Yuan remains committed to actively engaging in constructive dialogue with the Legislative Yuan and relevant societal stakeholders to garner broad-based support and facilitate the timely completion of the legislation. The government has initiated several policies, including the Taiwan AI Action Plan (2018–2021) and its subsequent version (2023–2026), focusing on ethical principles, national policy, privacy protection and regulatory sandboxes.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

A letter from Taiwan's Intellectual Property Office (2018) states that AI is not recognised as a legal "person", meaning AI-generated works lack copyright protection.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

If any "personal data" is collected, used or processed in relation to training data or data licensing, the PDPA regulatory framework (including our responses to questions in sections 4 and 5 above) will apply. Specifically, for any "sensitive personal

data", additional restrictions will be in place, such as the requirement for "informed consent" to be obtained in writing (as discussed in our response to question 4.3). We believe that PDPA compliance, as outlined, should be carefully considered in the context of data licensing.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Regulatory bodies overseeing AI and ML technologies are starting to distinguish between standard AI and generative AI using a risk-based framework, as detailed in the draft of the Fundamental Law on Artificial Intelligence. This framework emphasises the necessity for the Ministry of Digital Affairs to refer to international standards, such as the US Artificial Intelligence Risk Management Framework, to create a risk classification system. Although specific regulations are still being developed, the legislative rationale reflects a commitment to ensuring the safety and stability of AI by categorising risks, including prohibiting certain AI practices.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

As noted in our response to question 8.2 above, the legal and regulatory landscape for generative AI technologies is evolving, primarily through the Fundamental Law on Artificial Intelligence, which is still in draft form and has not yet been legislated. This framework emphasises ethical principles, national policy, privacy protection, and the establishment of regulatory sandboxes and guidance mechanisms. While it outlines general principles, specific regulations are being developed by various departments for different sectors. Key issues include: copyright disputes, as current laws do not recognise AI as a copyright holder; privacy concerns, as detailed in our prior answers regarding privacy regulations; and discrimination and fairness, which are addressed by the Ministry of Science and Technology's guidelines established in September 2019.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

The protection of personal data in AI applications is primarily regulated by the PDPA. The PDPA requires non-public entities to establish specific purposes and legal grounds for collecting or processing personal data. The draft of the Fundamental Law on Artificial Intelligence highlights the importance of minimising unnecessary data collection and incorporating data protection measures into AI development. Additionally, the Ministry of Digital Development has released guidelines on privacy-enhancing technologies to effectively address these issues.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

The theories of liability related to adverse outcomes are primarily categorised as follows:

- Civil Liability: This includes breaches of contract, torts and product liability, and is governed by the Civil Code and the Consumer Protection Act.
- Criminal Liability: This pertains to injuries resulting from intentional acts or negligence, as well as the manufacturing or importation of goods without the necessary permits or approvals. Relevant legislation includes the Criminal Code, the Physicians Act, the Pharmaceutical Affairs Act and the Medical Devices Act.
- Administrative Liability: This involves the manufacturing or importation of goods without the required permits or approvals, specifically under the Medical Devices Act.

9.2 What cross-border considerations are there?

If any digital health-related services are provided to individuals in Taiwan from offshore entities, there may be questions regarding the necessity for those offshore entities to comply with Taiwan's regulatory requirements, particularly concerning licensing (e.g., prior approval, permits, or licences needed to operate a medical device company or engage in healthcare-related activities), as healthcare is a regulated industry in Taiwan. For further details on these regulatory requirements, please refer to our response to question 10.2.

From a contractual perspective, even if the governing law of the contract for the digital health-related service is a foreign law (i.e., non-Taiwanese law) and a foreign court is designated for dispute resolution, we cannot entirely dismiss the possibility that, in the event of a dispute where Taiwanese individuals file a suit in a Taiwanese court, such court may still review the case and determine that Taiwanese laws (such as the Taiwan Consumer Protection Act) apply to protect those individuals.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

To mitigate liability risks associated with the use of generative AI, product and solution providers should ensure that their offerings meet applicable technical and professional standards, as well as reasonably expected safety requirements, before bringing them to market, in accordance with Taiwan's Consumer Protection Act.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

The misuse of healthcare data in AI/ML models raises legal concerns under various regulations. According to the Hospital Personal Data Security Maintenance Implementation Guidelines, hospitals must promptly address incidents of data

theft, leakage or alteration to protect individuals' rights. This includes taking measures to mitigate harm, investigating the cause, and notifying affected parties within 72 hours. Additionally, the PDPA stipulates that non-public entities violating data protection laws may face penalties, including bans on data collection, mandatory deletion of data and public disclosure of violations.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Regarding cloud-based services for digital health, the PDPA is applicable, as organisations utilising these services may collect data from individuals, which is then forwarded to a service provider for processing and use. Consequently, from a legal perspective in Taiwan, the primary concern with cloud-based services for digital health is compliance with the PDPA. Please refer to our responses to the questions in sections 4 and 5 above, particularly where personal data is classified as "sensitive personal data". In such cases, written informed consent is required. Additionally, there are exemptions from the informed consent requirement for use by non-government entities or academic institutions under specific circumstances.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Healthcare is a regulated industry in Taiwan. For instance, operating a medical device company, as well as manufacturing and selling medical devices, necessitates obtaining prior approvals and permits in accordance with current regulations. Furthermore, under the Physicians Act, individuals cannot practice medicine as physicians without the required licence. In the context of telemedicine, physicians are prohibited from treating patients, issuing prescriptions or certifying diagnoses for patients they have not personally examined, except in specific circumstances such as remote areas or urgent situations (refer to our response to question 3.1 above for more details). Given such considerations, it is advisable for non-healthcare companies to thoroughly evaluate the licensing and regulatory requirements before entering the digital healthcare market in Taiwan.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

From a legal standpoint, it is advisable for venture capital and private equity firms to thoroughly assess whether the business model of the target digital healthcare venture aligns with Taiwan's regulatory framework during the due diligence phase. This includes a critical evaluation of compliance with licensing and regulatory requirements, as outlined in our response to question 10.2, as well as adherence to the PDPA, particularly if the personal data collected by the target company meets the definition of "sensitive personal data".

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Based on our observations, the current legal obstacles in Taiwan that may impede the development of digital health solutions include the following: (i) as noted in our response to question 3.1, physicians are generally prohibited from treating, prescribing medicine for, or certifying diagnoses for patients they have not personally examined, except in specific situations such as remote areas or urgent circumstances – consequently, the provision of telemedicine services by physicians is largely restricted under current Taiwanese law; and (ii) there are typically more stringent regulations governing the collection, use and processing of "sensitive personal data", which is often integral to the development of digital health solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Taiwan, physician certification bodies, such as the Taiwan Surgical Association, do not significantly influence the clinical adoption of digital health solutions. Adherence to existing regulatory requirements is paramount. For details on the licensing and regulatory requirements from a Taiwanese perspective, please refer to our response to question 10.2 above.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

To our knowledge, no private insurers specifically exclude patients who use digital health solutions from filing insurance claims for covered incidents, provided that no additional documentation is required unless stated in the insurance policy. Regarding government reimbursement, the NHIA announced a pilot plan in 2020 aimed at including virtual care for remote areas under NHI coverage. Under this pilot plan, patients receiving care from approved medical institutions offering virtual services may only need to pay registration fees, subject to certain exceptions outlined in relevant regulations.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

There is a lack of transparency concerning data privacy and protection, as many digital health solutions fail to adequately disclose their practices related to data collection, usage, storage and sharing, especially during AI model training, which may involve insufficiently anonymised data. The opacity of AI/ML algorithms complicates the understanding of their decision-making processes, potentially leading to accountability issues when errors arise. The legal framework governing liability and risk allocation remains ambiguous, particularly regarding the responsibilities of developers,

healthcare providers and users. Regulatory compliance and market-entry standards for digital health products are still evolving, with existing guidelines lacking comprehensive adjustments to effectively address these challenges.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

As indicated in our response to question 4.7, Taiwan's Constitutional Court ruled in August 2022 on the PDPA, mandating the amendment of relevant laws within three years. Consequently, the PDPA was revised in May 2023 and further revised in November 2025, and the preparatory office for the independent PDPC was established in December 2023. Looking ahead, it is essential to monitor the PDPC's development and any further amendments to related legislation.



Tsung-Yuan Shen specialises in the fields of biomedical and food technology law, IP protection, unfair competition, construction/BOT and dispute resolution. His professional background spans biotechnology, law and economics.
Mr. Shen has represented many biotech-related companies in the fields of pharmaceuticals, medical instruments, chemicals, health food and GMO, and governmental research organisations in IPR matters and legal matters. He has also advised high-tech companies in the fields of electronics, optoelectronics, communications, precision industry and multinational construction companies on matters of IPR, high-tech laws and public construction disputes.
Clients served by Mr. Shen include Pfizer, Merck Sharp & Dohme, DuPont, TSMC, AU Optronics, Qualcomm, Molex, Lockheed Martin, and other leading companies or organisations.
Mr. Shen has also utilised his background in economics in cases involving the management or licensing of IP portfolios. In addition, he has acted on behalf of companies during governmental investigations of unfair competition and in administrative lawsuits with outstanding results.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 110055
Taiwan

Tel: +886 2 2763 8000 ext. 2539
Email: tsungyuanshen@leeandli.com
LinkedIn: www.linkedin.com/in/tsung-yuan-shen-沈宗原-02401019



Rachel Chen is a senior attorney in Lee and Li's Hsinchu Office. With backgrounds in both finance and law, her practice areas include corporate investment, corporate governance and compliance, securities law and labour law, with a special focus on M&A as well as commercial contract review and drafting.

Lee and Li, Attorneys-at-Law
No. 1, Gongye E. 2nd Rd.
East Dist., Hsinchu 300091
Taiwan

Tel: +886 3 579 9911 ext. 3206
Email: rachelchen@leeandli.com
LinkedIn: www.linkedin.com/in/rachel-chen-93018726a



Nita Ye is an attorney at Lee and Li, Attorneys-at-Law. Ms. Ye's practice focuses on arbitration, labour disputes, investment and personal data protection, regarding which she provides clients with consultation and professional advice.

Lee and Li, Attorneys-at-Law
No. 1, Gongye E. 2nd Rd.
East Dist., Hsinchu 300091
Taiwan

Tel: +886 3 579 9911 ext. 3269
Email: nitaye@leeandli.com
URL: www.leeandli.com/EN/Professions/901/529.htm

Lee and Li is now the oldest and largest law firm in Taiwan and is highly sought after by clients worldwide for its comprehensive and premium legal services. Our services are performed by a total of around 870 employees, including around 210 attorneys, as well as many patent attorneys, patent agents and trademark attorneys and over 100 professionals with backgrounds in technology and other fields. Many members of our team hold advanced degrees in law and IP rights from internationally renowned institutions. A number of our colleagues are also certified lawyers or patent agents in the United States and mainland China.
Lee and Li has established various practice groups based on our specialisations in banking and finance, capital markets, corporate matters and investment, trademarks and copyrights, patents and technology, and litigation and dispute resolution, as well as our Japan Practice Department. Practice groups put the formidable resources of a large firm and the highly customisable services of a boutique firm at our clients' disposal. We also have special task forces that corral experts from different departments and practice groups to tackle unusual challenges.
Our close rapport with prominent international law firms and business consultancies, accounting firms and financial institutions allows us to swiftly mobilise resources and expertise across disparate fields, and to devise optimal legal solutions for transnational matters. We collaborate with L&L-Leaven, Attorneys-at-Law in Shanghai and Lee and Li-Leaven IPR Agency Ltd. in Beijing to assist clients in the Greater China region with cross-strait legal matters and IP rights. This cross-strait platform saves our clients the effort of finding lawyers and agents in mainland China and prevents misunderstandings due to differences in Taiwanese and mainland Chinese legal systems and practices.
Lee and Li's services and expertise have earned high praise from clients both at home and abroad. In international surveys of law firms and IP firms, we are consistently rated as the best legal services provider in Taiwan.

www.leeandli.com

理律法律事務所
SINCE 1965 LEE AND LI ATTORNEYS-AT-LAW

United Kingdom


Pieter Erasmus


Emma Drake


Tristan Sherliker


Mario Subramaniam

Bird & Bird

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no specific definition of "digital health" in the United Kingdom (**UK**). The term generally refers to the use of technology (such as apps, programmes, software, etc.) in healthcare – either standalone or combined with other products such as therapeutics, diagnostics or medical devices.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging digital health technologies in the UK include the following:

- Digitised health systems – in particular, the wholesale digitisation of patient data and prescription delivery in the UK National Health Service (**NHS**).
- mHealth – apps on mobile and connected wearable devices to monitor and improve health and wellbeing.
- Telemedicine – delivery of health data from mHealth apps to the patient's clinician, and the provision of remote support and care to patients, either through healthcare practitioners, allied service providers or AI. There is a trend towards the integration of telemedicine services with digitised health systems.
- Health data analytics – the digital collation, analysis and distribution (including on a commercial basis) of patient health data.
- Personalised medicine – using genomics to get a faster diagnosis of a condition and being given personalised treatments based on that diagnosis.
- Artificial intelligence (**AI**) and machine learning (**ML**) – these technologies are being used to enhance digital health more broadly and improve operational efficiencies.

1.3 What is the digital health market size for your jurisdiction?

Given the breadth of the market and underlying technology, there is no specific estimate of the digital health market in the UK; however, certain sources suggest that the UK digital health market will reach approximately £15 billion in 2025/2026, although this is likely to be an underestimation.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Based on certain sources, examples of the more prominent digital health companies operating in the UK include:

- Huma.
- Limbic.
- Ally.
- Cera.
- Hexarad.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Based on certain sources, examples of growing digital health companies attracting investment and operating in the UK include:

- Exscientia.
- Benevolent AI.
- Healx.
- Zoe.
- E-therapeutics.
- Numan.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Medicines and Healthcare products Regulatory Agency (**MHRA**) regulates medical devices, including digital health technologies, ensuring they meet safety, quality and performance standards. NHS Digital is responsible for the national digital infrastructure and services, ensuring the secure and efficient use of data and technology in the NHS.

The National Institute for Health and Care Excellence (**NICE**) provides guidance and sets standards for health and social care practices, including the evaluation of digital health technologies.

With respect to the use of such digital health technologies in healthcare settings, the four nations of the UK are regulated by the following regulatory authorities:

- England – Care Quality Commission.
- Scotland – Healthcare Improvement Scotland.
- Wales – Care Inspectorate Wales.

- Northern Ireland – The Regulation and Quality Improvement Authority.

The Information Commissioner's Office (**ICO**) regulates the use of personal data in accordance with the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA**).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

In an increasingly multi-disciplinary area, the core healthcare regulatory schemes related to digital health in the UK are numerous. In addition to software as a medical device (**SaMD**) and AI as a medical device (**AIaMD**) regulation, these include data protection and privacy; the use of personal data in digital health is regulated primarily by the UK GDPR, the DPA, and laws on confidentiality that vary between the four devolved nations of the UK. Further examples include cybersecurity, data compliance and governance.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Key areas of enforcement include:

- **Data protection and privacy**: Ensuring compliance with the UK GDPR and the DPA. This includes safeguarding patient data and ensuring proper data handling practices.
- **Medical device regulation**: The MHRA oversees the safety, quality and performance of digital health technologies (including software) classified as medical devices.
- **Telemedicine and remote care**: Ensuring that telehealth services meet the required standards for safety and quality, including proper registration and compliance with healthcare regulations.
- **Clinical safety and effectiveness**: Ensuring that digital health solutions provide clinically safe and effective care, adhering to standards set by bodies such as NICE.

Emerging areas of enforcement include:

- **AI and ML**: As AI becomes more integrated into healthcare, there is increasing focus on ensuring these technologies are safe, effective and ethically used.
- **Cybersecurity**: With the rise of digital health technologies, protecting against cyber threats and ensuring the security of health data is becoming a critical area of enforcement.
- **Interoperability standards**: Ensuring that digital health systems can effectively communicate and share data across different platforms and healthcare providers (**HCPs**).
- **Digital therapeutics**: As digital therapeutics become more prevalent, there is a growing need to regulate these solutions to ensure they meet clinical standards and provide real therapeutic benefits.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

SaMD, including AIaMD, is primarily governed by the UK Medical Devices Regulations 2002, as amended (**MDR 2002**). The MHRA has issued guidance specifically dealing with SaMD, including AIaMD, which assists with determining whether software is regulated under the MDR 2002. The MHRA has been working towards the reform of the general medical device regulatory framework in Great Britain (being England, Wales and Scotland). Post-market surveillance draft regulations were laid before Parliament on 21 October 2024 and came into force 16 June 2025. A consultation was further launched on 14 November 2024 regarding "Pre-market" regulations. The consultation outcomes regarding the UK Government's approach to assimilated EU law were published on 26 February 2025 and the resulting legislation came into force on 24 May 2025. Consultation outcomes regarding matters such as international reliance and UKCA-marking were published on 22 July 2025. The MHRA has further published guidance (in October 2025) regarding the clinical investigations of medical devices, including SaMD.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

See response to question 2.4 above.

In addition, the UK regulations governing medical devices placed on the Great Britain market, including AIaMD, are under review as part of the wider programme of reform to medical device regulation. While there has been extensive discussion regarding AIaMD, no binding updates have yet been made to existing regulations to address the complexities of AI in medical devices. AI-specific guidance and commentary have, however, been published on several related topics. According to the MHRA's policy paper of 30 April 2024, where AI is used for a "medical purpose", it is very likely to fall within the definition of a general medical device. This means that it must meet the requirements of the UK MDR before being placed on the Great Britain market. In short, the MHRA proposes to deliver regulatory reform in this area through light-touch regulatory amendment and updated guidance, more streamlined processes for SaMD/AIaMD, and the potential up-classification of such devices (from the current Class I). This area remains in flux and should be monitored closely.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

See the responses to questions 2.4 and 2.5 above.

The MHRA launched the *AI Airlock* in May 2024 (in collaboration with the Department of Health and Social Care, the NHS AI Lab and "Team AB" (being a group established in February 2024, bringing together expertise from approved bodies)), which was the first regulatory sandbox for AIaMD; this pilot project ran until April 2025. The objective of this project is to identify regulatory challenges associated with AIaMD, to help manufacturers explore how to best collect evidence as support for the approval of their product, and to understand and mitigate any risks that are uncovered through the project. The second phase of the *AI Airlock*, which includes seven additional technologies spanning AI-powered clinical note-taking, advanced cancer diagnostics, eye disease detection tools, and obesity treatment support systems, was launched earlier in 2025 and will continue until March 2026.

Additionally, and by way of further example, in January 2025 the MHRA launched a pilot real-world evidence Scientific Dialogue Programme, which is designed to help innovators refine their evidence-generation strategies while providing clear guidance on regulatory expectations. This programme aims to facilitate robust decision-making across the entire life-cycle of products, benefitting both regulatory and health technology assessment evaluations relevant to the UK.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data plays a key role in the regulatory considerations for AI/ML-based digital health solutions. The MHRA requires robust clinical validation data to approve AI/ML-based medical devices. This data helps regulators assess the accuracy, reliability and clinical relevance of the AI/ML algorithms. Clinical validation data also supports ethical and transparent use of AI/ML in healthcare. It helps in understanding the decision-making process of AI algorithms, and ensuring they are fair and unbiased.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Regulation in this area remains broadly aligned at the UK national level, subject to the nuance brought about by the Northern Ireland Protocol whereby the regulatory regimes differ between Great Britain and Northern Ireland. Therefore, while the primary regulatory framework is set at the national level, regional health authorities and NHS Trusts may have additional requirements or guidelines for the implementation and use of digital health technologies. These can include specific data-sharing agreements, local clinical governance standards and region-specific pilot programmes.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

As mentioned in the response to question 2.6, examples include the MHRA introducing the *AI Airlock* initiative to test and refine the regulatory framework for AI-powered medical devices. This initiative allows for real-time performance monitoring and continuous validation of AI technologies. In addition, regulatory bodies such as the MHRA and NICE are developing dynamic guidance that can be updated as new evidence and technologies emerge. This ensures that regulations remain relevant and effective.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  - Determining whether any of the devices used qualify as medical devices.
  - Determining whether such activity requires registration as a regulated activity.
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring that algorithms are robust and unbiased.
  - Contractual issues between the various suppliers of services and devices.
  - If telemedicine is included, compliance with the local pharmacy and prescribing rules and regulations will be necessary.
  - Cybersecurity.
- **Robotics**
  - Liability allocation for poor outcomes – designer, manufacturer, HCP or even power supplier.
  - Compliance with regulations: e.g. for waste electrical and electronic equipment.
  - Compliance with MDR 2002.
- **Wearables**
  - Determining whether any of the devices used qualify as medical devices.
  - Data protection compliance – assessing whether health data is collected by publishers or whether this is strictly limited to the local device, ensuring a lawful basis for processing (likely to be consent), ensuring privacy by design, explaining data processing to individuals, implementation of necessary security measures and retention of necessary information.
  - Contractual issues between the various suppliers of services and devices.
- **Virtual Assistants (e.g. Alexa)**
  - Similar issues as for Telehealth.
- **Mobile Apps**
  - Similar issues as for Telehealth.
- **Software as a Medical Device**
  - Compliance with MDR 2002.
  - Data Protection compliance. Similar issues as for Telehealth.
- **Clinical Decision Support Software**
  - Similar issues as for Telehealth.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  - Similar issues as for Telehealth.
- **IoT (Internet of Things) and Connected Devices**
  - Similar issues as for Telehealth.
- **3D Printing/Bioprinting**
  - Liability allocation for poor outcomes – designer, manufacturer and/or HCP.
  - Contractual issues between the various suppliers and customers of services/products.
  - IP ownership issues.
- **Digital Therapeutics**
  - Similar issues as for Telehealth.
- **Digital Diagnostics**
  - Similar issues as for Telehealth.
- **Electronic Medical Record Management Solutions**
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring compliance with data retention rules.

- Cybersecurity.
- Contractual issues between the various suppliers of services.

- **Big Data Analytics**
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring that algorithms are robust and unbiased.
  - Liability allocation for poor outcomes – algorithm designer and/or HCP.
  - Contractual issues between the various suppliers of services.
- **Blockchain-based Healthcare Data Sharing Solutions**
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, difficulties with amending records, issues with "right to be forgotten" and erasure of data, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; and implementation of necessary security measures.
- **Natural Language Processing**
  - To the extent applicable, similar issues as for Telehealth and Big Data Analytics.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Data protection, patient confidentiality and especially the lawful transmission, storing, processing and use of data – and ensuring an adequate lawful basis is available for all relevant uses. Rights of access to and rights to reuse data for additional purposes are also key issues.

The digital platform provider must ensure, to the extent it is responsible: (i) that advice and services provided on the platform are fit for purpose as failure to process information resulting in personal injury may result in liability; and (ii) where the activity requires registration as a regulated activity, such activity is registered and complies with relevant regulations.

In the UK, to the extent a digital platform provider can allow interactions between third-party users, such as self-employed clinicians and patients, it is often likely to be in scope of the UK's Online Safety Act. This has substantial risk assessment and detailed measures that must be adopted to protect all children.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

- The UK GDPR and DPA are the primary laws to consider in relation to data use in the UK. Patient confidentiality is separately regulated as a matter of common law, and is also relevant to the legality of processing personal data.
- Key issues include determining whether relevant data is personal data or has been sufficiently anonymised. Anonymisation is recognised as difficult to achieve in practice, and may reduce the utility of the relevant dataset. Simply removing identifiers may result in pseudonymous data, which is still caught by the UK GDPR.
- Also important is confirming the roles of the parties involved in the processing – which parties are controllers or processors – and putting appropriate contracts in place.
- Identifying whether data is *concerning health* (and therefore subject to more stringent rules, as are other categories of "special-category" data such as personal data on sex life or religion), *versus* less sensitive data that might, for instance, be collected for wellness purposes is usually a key consideration for technologies (e.g. step counts, sporting performance, etc.).
- An important requirement is identifying the appropriate legal basis for processing data and obtaining any necessary consent – consent may not be the appropriate lawful basis, especially where processing is not mandatory.
- Health data uses almost always require the carrying out of a Data Protection Impact Assessment (**DPIA**), and ensuring that appropriate risk mitigations are put in place, including measures to ensure data minimisation, privacy by design, data retention limits and appropriate information security measures.
- As mentioned above, ensuring that any overlapping requirements related to rules on patient confidentiality are met is also vital.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

This is not applicable, except as relates to the NHS – see question 4.3 below.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

There is a significant distinction between the use of data within *versus* outside the NHS; the impact of "soft law", such as restrictions deriving from NHS policy and "Directions" issued by the UK Secretary of State, will be more acutely felt when working with NHS-originating data, compared to data in (or sourced from) private or consumer settings.

Even in public sector contexts, the rules differ between different parts of the UK. An important example is the "National Data Opt-out", a scheme allowing NHS patients to easily opt out from certain secondary uses of their personal data in England. This does not apply to patient data from Northern Ireland, Scotland or Wales.

4.4 How do the regulations define the scope of personal health data use?

The GDPR/DPA generally prohibit the use of health-related personal data without prior, explicit consent, but list exemptions from that restriction – e.g. use of personal data to provide healthcare (by or under the responsibility of a person bound by a duty of confidentiality) is permitted. Similarly, they allow non-consensual scientific research in the public interest (provided that such research does not entail the taking of

decisions affecting the relevant individual(s), unless the project has ethical committee approval).

However, as noted in the response to question 4.7 below, there are overlapping restrictions under contract, soft law and confidentiality/misuse of private information (**MoPI**) rules, which may affect the need to obtain consent.

Although this consent does not have to meet the same standard as explicit consent under the UK GDPR, care should be taken (and specialist advice obtained) to ensure that, where relying on UK GDPR/DPA grounds for processing personal data, these restrictions do not apply to the use of personal data.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Digital health companies will often find themselves subject to heavy requirements imposed by NHS customers. Organisations not dealing with the NHS will often have greater freedom to operate.

More generally, a key consideration for the design and negotiation of contracts is whether, for UK GDPR purposes, the different parties are "processors" or "controllers" of the data – and in the latter case, whether two or more parties are "joint" or "independent" controllers. That classification will dictate the UK GDPR-imposed terms that must be included in the contract, and also inform each party's compliance strategy and required risk protections (indemnities, warranties, due diligence and insurance).

If personal data is travelling internationally, then the UK GDPR will often require that additional contractual terms (typically based on a pre-approved set of "standard"/"model" contractual clauses) must be put in place between the data's exporter(s) and importer(s), and onward transferees.

By contrast, UK data protection laws generally have little impact on contracts with individuals; data protection-related matters should be dealt with outside of those contracts (e.g. through dedicated privacy notices, and stand-alone consent requests).

The legality of planned and future uses of personal data will be conditional on ensuring that notices, consents, contracts and/or lawful exemptions cover all anticipated uses – or expose an organisation to significant investigations and civil and/or criminal liability. In parallel, failure to secure appropriate IP rights from rights holders can expose the organisation to a risk of being sued by that organisation, and/or additional criminal liability under the DPA (if the data is personal data).

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The UK GDPR requires controllers to ensure that data is accurate, up to date and processed fairly. It also requires controllers to notify individuals about how their data may be processed, including the logic used in automated decisions made about them. Further, controllers are required to ensure that any individuals are not subject to substantial and entirely automated decision-making without explicit consent, contractual necessity or legal obligation.

The ICO has released detailed guidance on the use of AI, including guidance on addressing risks associated with automation such as bias, automated decision-making and risks of discrimination. The ICO is also carrying out active investigations into the use of AI tools in certain sectors, such as recruitment, and the potential for bias in the use of these tools.

The NHS in England has an active AI Ethics Initiative, run by the NHS AI Lab, which has various projects considering bias and risk in AI datasets.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The use of personal data in digital health is regulated primarily by the UK GDPR, the DPA and laws on confidentiality that vary between the different parts of the UK.

In addition, a substantial body of "soft law" tends to be imposed by other stakeholders' policies and contracts.

Additional legislation can apply for specific data uses, e.g. the Privacy and Electronic Communication Regulations restrict non-consensual access to and storage of data on Internet-connected devices. Medical device or clinical trial laws further limit the use of personal data.

- The UK GDPR imposes significant restrictions on the use of health data without providing notice of that use and demonstrating an appropriate legal basis for processing the special-category data. Often, explicit consents from individuals will be necessary. This must be specific, informed and freely given.
- Operators in England and Wales (in particular) must also deal with more restrictive requirements of "common law", particularly surrounding patient confidentiality and MoPI. Without consent (which for confidentiality/MoPI purposes could be implied or explicit), or a clear statutory permission, only uses of patient personal data that are necessary for patient care or in the public interest, are permitted under English and Welsh law on confidentiality and MoPI.
- The UK GDPR also imposes additional requirements, including to keep data secure, maintain its availability and accuracy, report data incidents, appoint a Data Protection Officer and/or a "Representative", conduct DPIAs, and generally ensure that usage of personal data is fair, lawful and does not involve excessive amounts of data.
- The UK GDPR grants individuals substantial personal data rights, e.g. to access or delete their data. The DPA adds certain additional rules, including criminal offences for re-identifying personal data, or selling it after it has been improperly obtained.
- Data protection law also includes laws that regulate the use of automated means to take significant decisions that have legal or "substantially similar" effects on an individual. This will need to be borne in mind as software (e.g. AI) becomes increasingly capable of replacing (rather than merely supporting) human decision-making in healthcare settings.
- There have been recent changes to UK data protection law under the Data Use and Access Act 2025. At the time of writing, these have not yet been commenced. These change some rules on, for example, relevant rights (including a new right to complain to the controller) and new lawful bases for processing. Some changes are made to assist research organisations, including an exemption to providing notice where impossible or disproportionate and where processing is for scientific research purposes. Additional restrictions, however, are placed around the ability to reuse data. A close eye should be kept on these

developments throughout 2026 – as should attention on EU-equivalent relaxations in the UK.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

As with general use of such data, the key laws are the UK GDPR, the DPA and patient confidentiality derived from common law. Changes are still awaited under the final commencement of the Data Use and Access Act 2025. The sharing of personal data means that confidentiality and privacy concerns will often be more acute than simply using data within a single organisation. For example, in England and Wales, even greater attention needs to be paid to the existence of a care need, consent, statutory permission and/or a public interest justification for the proposed data sharing if it involves patient data processed for the purposes of providing care. To complicate matters, that legal basis might be different for the different parties, and thus subject to differing restrictions and conditions.

Sharing personal data also introduces potentially significant counterparty risk: both parties to a data-sharing arrangement might face legal risk even if just one of the parties misuses the data. Due diligence, contracting and clear compliance arrangements are therefore important.

Key aspects of the data sharing may need to be explained to individuals, in accordance with the GDPR's transparency obligations. Finally, sharing personal data across borders – even just by providing remote access to it – raises GDPR data transfer compliance issues.

See also the potential for certain services to be caught by the UK's Online Safety Act, as discussed above.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

This is not applicable.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

As with data use, key legal variations tend to be driven by differences in the purpose of data sharing, not the nature of the entities involved. That said, certain public sector entities (particularly, those within the NHS) might have specific legal powers – or restrictions – regarding data sharing and the performance of their public duties. This could also vary depending on their location within the UK.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

There are numerous NHS initiatives for the sharing of healthcare data. For example:

- NHS England has a role as statutory custodian for health and social care data for England, taking a role in creating data collections, data sets and allowing specific authorised access to third parties.
- The Health Research Authority's (**HRA**) Confidentiality Advisory Group provides independent expert advice to the MHRA and the Secretary of State for Health on whether applications to access confidential patient or service user information without consent should or should not be approved.
- The Clinical Practice Research Datalink, a real-world research service supporting retrospective and prospective public health and clinical studies collecting data from a network of services.
- The NHS Federated Data Platform.
- The NHS Data Security and Protection Toolkit, for those who have access to NHS data.
- NHS pilot programmes, including Improving Elective Care Coordination for Patients and Dynamic Discharges.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Where a choice has been taken to consider federated learning data sharing for the purposes of protecting patient confidentiality and personal data, it is key to ensure that appropriate protections are offered by the tools, software and contracts establishing this framework to ensure these purposes are fulfilled – there must be appropriate security, use of sufficient anonymisation tools and restrictions on sharing to ensure the intended benefits are achieved.

The preceding responses, in particular to questions 4.1, 4.5, 5.1 and 5.3, have covered the key regulatory requirements applicable to the sharing of personal data in a digital health context.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patent protection is still available for digital health technologies that satisfy the requirements for the grant of a patent in accordance with the UK Patents Act 1977 (**PA**).

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protection is still available for digital health technologies that satisfy the requirements of the UK Copyright, Designs and Patents Act 1988 (**CDPA**); see also response to question 6.5 with respect to protection of software.

In respect of AI training with respect to copyright-protected data, the UK does not have the same concept of fair use as is often relied upon in other jurisdictions such as the USA. The relationship between copyright and AI is subject to an ongoing consultation as of December 2024, which notes that the position is disputed, that the *status quo* cannot continue, and emphasises the government intention to remove legal uncertainty and promote innovation and investment in both creative and AI industries.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Digital health technologies that satisfy the requirements of a trade secret and/or confidential information will continue to be protected as a trade secret (protection under statute) and by the common law of confidence, which protects information that:

- has a quality of confidence;
- is disclosed under an express or implied obligation of confidence; and
- is used or further disclosed in an unauthorised manner.

The UK Trade Secrets (Enforcement, etc.) Regulations 2018 also prevent acquisition, use or disclosure of trade secrets where this would constitute a breach of confidence in confidential information.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

IP rights in technology developed in academic institutions usually vest in the academic institution, as a result of employment or other contractual arrangements. Absent contractual arrangements, the ownership of IP rights can be more complicated. Academic institutions typically seek to commercialise technologies by way of licensing arrangements (for example, to existing businesses, commercial research partners, or via the creation of a spin-out company dedicated to commercialising the technology).

There are no specific laws governing academic technology transfer. In very rare cases, under the PA, the publication of a patent or disclosure of related information may be restricted if it might be prejudicial to national security or public safety, with resulting effects on technology transfer.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

A software-implemented invention is only patentable in the UK to the extent that it meets the requirements in the PA. While inventions implemented in software are patentable, software *per se* is not. The requirements are stringent and difficult to meet. Generally, software *per se* will be protected as a literary work under the CDPA (although the protection applies to the particular expression of ideas and principles that underlie an algorithm and not to the ideas and principles themselves) (see response to question 6.2).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No. Following the decision of the UK Supreme Court in *Stephen L Thaler v. The Comptroller-General of Patents, Designs And Trade Marks* [2023] UKSC 49, an AI device cannot be named as an inventor of a patent in the UK under current legislation. In October 2021, the UK Intellectual Property Office (**UKIPO**) (the executive Government Department) issued a public consultation on whether the PA should be amended to permit an AI system to be named as an inventor or whether the definition of inventor should be expanded to include humans responsible for an AI system that devises inventions. The outcome of the consultation was that AI was not considered advanced enough to invent without human intervention and that there was therefore no planned change to UK patent law for AI-devised inventions.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Government funding for innovation is available in the UK. This funding is classed as a subsidy and therefore must be consistent with the UK subsidy control regime, WTO rules, the EU–UK Trade and Cooperation agreement and other bilateral UK Free Trade agreements.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

The following guidelines and IP decisions are particularly relevant with regard to the AI and software aspects of digital health innovations. The UKIPO and the European Patent Office (**EPO**) have established guidelines on the patentability of AI-related innovations. The various responses to the UK Government's 2024 consultation into the general regulatory landscape regarding AI and ML also provide useful guidance on the rationales that may inform future decisions from regulators.

With respect to copyright in outputs of AI systems, the UK has considered the interaction between AI and copyright in one leading case between Getty Images and Stability AI (*Getty Images v. Stability AI* [2025] EWHC 2863 (Ch)). Bird & Bird acted for Stability AI. During that trial, arguments were abandoned that had alleged that Stability AI trained its models in the UK. Allegations were also abandoned as to the question of whether outputs of the AI infringed copyright. The position therefore remains unresolved. See above at question 6.2 with respect to the ongoing government consultation in this area.

Patent case law emphasises the importance of demonstrating that the software component of the digital health product has a technical effect, beyond the mere implementation of a mathematical method on a computer. For instance, the EPO's decision in G 1/19 (Simulations) and the UK court's decision in *Aerotel v. Telco and Macrossan's Application* [2006] EWCA Civ 1371 clarified the approach to computer-implemented inventions, which can be relevant to AI in digital health.

Copyright case law in relation to software programming highlights that ideas and principles (such as operational methods, mathematical concepts and procedures) in software are not protected by copyright (*SAS Institute v. World Programming*, Case C-406/10; *Nova Productions Ltd v. Mazooma Games Ltd* [2007] EWCA Civ 219). Therefore, a competitor can develop a competing software product that does effectively the same thing or operates according to the same principles, as long as the competitor did not copy the code or other pivotal structural design aspects of the original product.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

It is often suggested that joint ownership of IP/improvements is the fairest way of approaching collaborations. The downside

of this blanket approach is that treatment of jointly owned IP varies from jurisdiction to jurisdiction and also by IP right. The consequence is that the joint owner might be unclear as to their rights to exploit such IP if not expressly set out in the collaboration agreements.

Alternative ways of approaching collaborative improvements would be for ownership to follow the ownership of background on which the improvement is made or to assign such collaborative improvements in accordance with predetermined fields of use. In all instances, it would be prudent to include relevant licences to background and royalty provisions, as applicable.

More broadly, parties should consider including robust provisions relating to confidentiality to protect sensitive information shared during the collaboration, as well as clearly defining performance obligations and milestones to track progress and ensure accountability. The parties should be prepared to adapt to changing circumstances and new information and rightsholders, as flexibility is crucial for navigating the dynamic nature of collaborative projects in digital health technologies.

On 18 November 2025, NHS England published its updated IP Guidance, being the first time it has been updated in over two decades. The guidance applies to any collaboration with NHS Trusts and adopts a balanced perspective on IP ownership and exploitation. Rather than focusing exclusively on NHS Trust ownership of IP rights – traditionally viewed as the optimal position for the NHS – it explores alternative arrangements through which the NHS can derive value from collaborations, including licensing structures and commercial models.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

When entering into agreements between healthcare and non-healthcare companies, particularly in areas like digital health, parties must consider stringent regulatory compliance, data protection, liability allocation, and cultural alignment. As with any agreement, the allocation of rights and obligations should be set out clearly, especially in relation to liability. It is likely that the parties will have responsibilities related to their respective expertise, and these should be specified, as well as responsibility for data protection compliance.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Agreements should carefully outline the terms of the data sharing, specifying who has control over the data and how decisions regarding data usage will be made. Issues related to data access, modification and deletion should also be addressed. Rules around ownership of the model itself should also be established.

As the raw data is not shared, parties should agree on common data formats and standards to ensure interoperability. Ideally, the data sharing agreement should facilitate seamless integration of data from different sources, potentially by using established healthcare interoperability standards such as Fast Healthcare Interoperability Resources.

Agreements should also comply with data protection laws, for example, setting out rules around data minimisation and purpose limitation.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties should ensure clear data ownership agreements that respect the interests and expectations of both parties, as well as data subjects and stakeholders involved.

The quality and availability of data is another consideration. It may be difficult to obtain large amounts of high-quality data to train the AI model due to the sensitive and confidential nature of most healthcare data. Biased, inaccurate or unrepresentative data in datasets could lead to bias or inaccuracies in the results.

As to the use of AI outputs in practice, licensees and licensors of AI systems may wish to consider the specific uses to which such models are to be put and to seek agreement as to the fitness for use of such systems and set down terms as to the degree to which liability for allegations of intellectual property infringement will be shared, disclaimed, warranted or indemnified as between the parties.

Navigating rules around patient privacy and data protection will also be an issue, along with rules and regulations governing generative AI itself, which are rapidly evolving from country to country.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is currently no AI-dedicated regulator in the UK. Regulators have been encouraged by the Government to develop approaches specific to their own domains, and the wider approach to legislation and development is under development. See response to question 8.2 below for information about important programmes of relevance to AI/ML in healthcare.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

For now, unlike the EU, there is currently no specific regulatory regime in relation to AI/ML in the UK, although the Government is developing an AI Opportunities Action Plan over the course of 2025. At the moment, there are cross-sector guiding principles published by the UK Government that are implemented by various regulatory authorities using their existing powers and under existing regimes. However, the landscape is developing. In particular:

- The Government Department for Science, Innovation and Technology has a special division, the AI Safety Institute – a state-backed organisation to conduct research and safety assessments for AI in the UK.
- In early 2024, a Government consultation concluded into the general regulatory landscape under AI and ML topics was conducted. The consultation involved communication with, and consultation responses from, many interested regulators including the MHRA, ICO and Office for Statistics Regulation (the body governing official

statistics in the UK). The regulator responses to the Government consultation, and the consultation itself, are useful resources for understanding the direction of movement, albeit that the incumbent Government has changed in the UK since that consultation took place and, to the extent that regulation is enacted pursuant to Government policy, the policy objectives may differ (as to which, see below).

- The MHRA in particular has been active in developing its regulatory posture and has conducted consultation and development activities since at least 2021.
- In December 2024, a Government consultation and call for views began in the field of copyright and AI. The consultation ran until February 2025 with the outcome being expected in the near future.
- The Government has stated its policy goals in relation to AI generally, and the overlap between AI and IP specifically, to be broadly in favour of promoting the development and adoption of AI technologies in the UK.
- It is therefore likely that the regulatory response to AI will develop significantly throughout the course of 2025 and 2026.

Some regulatory programmes with specific relevance to digital health include:

- **Personal Data**: The ICO lists AI as a "priority area" due to the potential effects on individuals. The ICO operates a regulatory "Sandbox" programme, which is a free service designed to give access to regulators themselves, for businesses in need of specific guidance. The ICO lists digital healthcare companies as examples of beneficiaries of this programme.
- **SaMD**: The MHRA operates a dedicated Software Group for the regulation of SaMD *per se*. In October 2022, the agency published a Roadmap for the regulation of AIaMD. The Roadmap indicated a blend of recommended legislative, regulatory and best-practice guidelines in that context. The recommendations ranged from passing new laws, to changing the use of nomenclature and increased monitoring and surveillance of SaMD in use.
- **Health Data Governance**: NHS Digital and the HRA oversee the use of health data in AI/ML applications. They regulate the use of data in healthcare AI in respect of compliance with data protection laws and ethical standards, particularly in research contexts.
- **AI in Clinical Trials and Research**: For AI/ML technologies used in clinical trials, the HRA and MHRA provide guidance on ethical considerations, data management and regulatory compliance. This includes ensuring that AI systems used in research are transparent, explainable and subject to rigorous evaluation.
- **Ethical Standards and Best Practices**: NICE has, in 2024, published an AI Code of Ethics, covering seven topics (plus sub-topics) for the adoption of AI in clinical and research settings. The principles touch on broad matters including integrity, transparency and accountability, as well as addressing specific concerns such as bias mitigation, and the use of quality checks and regular assessments.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under English law, algorithms are potentially protectable by copyright as original literary works, although the protection applies to the particular expression of ideas and principles that underlie an algorithm and not to the ideas and principles themselves.

Where an algorithm is written by a human, the author of that work is the person who creates it (Section 9(1) CDPA). This is taken to be the person responsible for the protectable elements of the work, being those elements which make the work "original" (i.e. those parts that are the "author's own intellectual creation").

First ownership of a work and the duration of the protection available are defined with reference to the author. However, where an algorithm is written using ML without active human involvement, it may not be possible to identify a human who can be said to have created the work, i.e. there is no human author such that the work qualifies as "computer generated" under Section 178 CDPA. In these circumstances, Section 9(3) CDPA deems that the author of the work is the "person by whom the arrangements necessary for the creation of the work are undertaken". This can potentially be one or more natural or legal persons. Under Section 12(7), the duration of protection of a computer-generated work is 50 years from the end of the calendar year in which it is created.

While the test set out in Section 9(3) CDPA determines the identity of the author of a computer-generated work, it is not currently clear as a matter of English law whether such work will qualify as copyright work. Under Section 1(1) CDPA, copyright only subsists in original literary works, which requires an intellectual creation by the author which reflects an expression of their personality. It is questionable whether an algorithm developed by ML without human involvement could be said to be an intellectual creation reflecting the personality of the person making the arrangements necessary for its creation.

As a result, such an algorithm may not qualify for copyright protection under English law. An alternative view is that Section 9(3) CDPA in fact creates its own *sui generis* right for computer-generated works which is not subject to the usual requirement for originality. These issues have not thus far been addressed by the English courts and claims to copyright (or an absence of rights) in algorithms developed by ML without human intervention must therefore be treated with caution.

In October 2021, the UKIPO issued a public consultation seeking views on possible reforms to the protection of computer-generated works in the UK. The options under consideration included retaining the existing position under Section 9(3) CDPA, removing protection for computer-generated works or replacing Section 9(3) with a new and narrower form of protection with a limited duration, e.g. five years from creation. The UKIPO published its response to the consultation on 28 June 2022. It concluded that AI was still in its early stages, and it was not possible to undertake a proper evaluation of any changes to the law, which may have unintended consequences. The Government therefore proposed to make no changes to the current law, while keeping a decision of whether to amend, replace or remove protection under Section 9(3) under review.

Looking ahead, the UK Government is expected to continue to develop and set out its approach on AI regulation and will act to ensure the UK has a competitive copyright regime that supports the UK's AI sector. The Government has cited AI technology as a major part of its policy focus.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Many ML projects often involve collaboration between a party

with expertise in deploying ML and another party with access to the data required to train a ML system to solve a particular problem. Common commercial issues that arise in this context include the rights each party obtains in the resulting system, e.g. can the resulting system be resold to others or adapted for purposes that go beyond those originally envisaged?

Similar considerations apply to the future use and disclosure of the training data itself, e.g. is the recipient allowed to retain the data after the project is complete and can it be re-used for other purposes (either in its original form or in some aggregated/derived form) and/or shared with third parties (and if so, under what terms)? Where the data is provided on a long-term basis with a defined scope of use, the licensor may wish to include audit rights to ensure the data continues to be used and disclosed in compliance with the terms of the licence.

Data licences will need to address potential liabilities arising from use of the licensed data. These will include any harm arising from defects in the licensed data, e.g. systematic inaccuracies in training could give rise to models that do not perform as required. A licensor will generally try to disclaim liability for errors or inaccuracies in a dataset. Liabilities could also arise through infringement of third-party rights in the data. These could include infringement of IP rights and other related rights, e.g. infringement of copyright in scientific publications or breach of an obligation of confidence owed by the licensor to a third party with respect to a particular dataset. In addition to conducting pre-contract due diligence on the legal rights affecting datasets, licensees will also often seek warranties and indemnities in the licence agreement to reduce their exposure to these risks.

Issues regarding use of training data commonly arise in the context of AI service agreements. An AI service provider will commonly wish to re-use data received from a customer during the course of providing the service to further improve the AI system that is used to provide the service, or potentially to develop new AI models for use in a different context.

Customers may resist contractual terms that permit this re-use of their data for these purposes, considering it to be a net value transfer from them to the service provider. Provisions relating to the use of derived data and meta-data, anonymisation and data retention post-termination may all be affected by this issue.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

At present, UK regulatory bodies have not established distinct regulatory frameworks specifically differentiating between standard AI and generative AI technologies. However, they are aware of the unique challenges and considerations that generative AI presents. For instance, the MHRA is working with a developer of a generative AI tool that helps users write documents or analyse data. Additionally, the Digital Regulation Cooperation Forum – formed of the ICO, Ofcom, Competition and Markets Authority (**CMA**) and Financial Conduct Authority – undertook joint consumer research on generative AI; the joint report found that consumers tend to assume regulation is in place if using generative AI in certain settings (financial services in particular) and expect organisations deploying generative AI tools to be accountable if things go wrong; as such, warnings and messaging can increase consumers' sense of personal responsibility.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

IP: In the field of IP, the dominant conversation concerns the use of copyright-protected works for the training of ML models, and the effect of the use of ML models on IP rights ownership in their outputs. The UK Government's *AI Opportunities Action Plan* (2025) highlights that it will act to ensure there is a competitive copyright regime that supports the UK's AI sector, and states that it may take forward the recommendation of establishing a copyright cleared training data set that can be licensed internationally at scale.

Misinformation, Deepfakes and Defamation: The UK Government's ongoing open consultation on copyright and AI includes assessing whether the current legal framework is sufficient to provide individuals with control over use of their likeness and whether further intervention is required. The ICO is also currently reviewing the application of UK data protection rules in this area and will issue guidance in due course.

Bias and Discrimination: Fairness is one of the UK Government's guiding AI principles and is therefore a key aspect implemented by regulatory authorities such as the ICO and CMA and NICE (as referred to above). Additionally, in 2023–2024, a UK Government scheme offered £400,000 in investment to fund innovative solutions to tackle bias and discrimination in AI systems. One of the winners of the scheme was King's College London, who will design a solution to address bias and discrimination in healthcare, in particular in early warning systems used to predict cardiac arrest in hospital wards.

Data Privacy and Confidentiality: This continues to raise issues with respect to: the use of personal data and training materials; the potential applications of synthetic data; and security issues arising from the risk of AI-powered malware.

Accountability and Liability: This will be a significantly developing issue. Questions of responsibility for actions attributable to AI are not clear under the current law. The regulatory response is being developed, and accountability is one of the UK Government's guiding AI principles and is therefore a key consideration for regulatory authorities.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

These are difficult issues under the UK law and are currently before the courts in at least one major dispute. It is likely that 2026 will begin to bring clarity to the assessment of these questions, at least from a jurisdictional standpoint. It is also highly likely that some legislative or policy developments will emerge from the open consultation on copyright and AI that is currently underway.

In the case of *Getty Images v. Stability AI,* the High Court rejected allegations that importation into the UK of an AI model could infringe copyright in training data on the basis of a secondary infringement.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Liability for adverse outcomes in digital health is governed both by the law of contract (where services are delivered in accordance with a contract) and by the common law of tort/negligence where, whether or not a contract is in place, a duty of care exists between parties, and a breach of that duty (by falling below the reasonable standard expected in carrying out that duty) causes loss (including personal injury).

Additionally, the UK Consumer Protection Act 1987 sets out a strict liability regime for consumer products, including medical devices. In summary, under such claims a claimant does not need to show any fault on the part of the defendant. Instead, a claimant needs to demonstrate: (i) the presence of a defect in a product according to an objective standard of safety as reasonably expected by the public; and (ii) a causal link between that defect and the loss suffered.

Finally, the UK GDPR might create joint and several liability between partnering organisations if non-compliance led to an adverse outcome – for example, basing clinical decisions on inaccurately recorded patient data or a biased algorithm.

9.2 What cross-border considerations are there?

Previously, under EU law (the Rome Regulations), generally, UK national (English and Welsh, Scots or Northern Irish) laws have applied to non-contractual (e.g. personal injury) and contractual claims based on digital health delivery to consumers/patients in the UK, whatever the country of origin of the provider. In accordance with retained EU law, the situation is not expected to change significantly in the short term.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Developers of generative AI products bear a duty towards the end-users, especially when the AI's decision-making mechanisms are unclear or complex. However, software developers may counter this by stating that generative AI-based healthcare solutions are designed to work in conjunction with HCPs who can overrule them if they propose a potentially harmful path, thereby shifting responsibility to the HCPs.

The British Medical Association's principles for the application of AI in healthcare (2024) provides some best practices to follow, such as ensuring HCPs and patient involvement throughout the development and implementation process, ensuring HCPs are initially and continuously trained on new technologies, and allowing HCPs to challenge decisions made by AI.

In the absence of legislation clearly governing liability of parties, it is essential that commercial contracts spell out which party is liable for errors when using generative AI in digital health solutions. Indemnification clauses could limit the liability of HCPs and AI algorithm creators. Alternatively, a special adjudication system could be considered. This would establish a separate legal pathway for addressing claims related to generative AI usage in healthcare, particularly for those claims that are challenging to resolve under current liability structures.

Insurance could serve as a safeguard against the financial risk linked with the application of generative AI by compensating for any potential damages and promoting responsible AI use among HCPs.

When building new generative AI tools, HCPs should insist that developers' models follow the MHRA's 10 guiding principles in relation to good ML practice for medical device development.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

The general principles briefly set out in the response to question 9.1 above apply. There may also be breach of patient confidentiality if patient data is used without appropriate anonymisation and without consent or other lawful exemption to consent.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Key issues include: (i) data security; (ii) commercial re-use of the data by the Cloud-based service provider; and (iii) whether data will leave the UK.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

It is a complicated and heavily regulated area, with regulations varying, in some instances, within the UK. There is no single, broad-brush approach and given the rapid development of digital health technologies, monitoring regulatory changes will be essential.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

When considering a target:

- Ensure that procedures are in place for compliance with relevant areas, especially data protection, patient confidentiality, and the variety of medical device regulations and guidance.
- Consider IP ownership and protection – do they own all necessary IP and have steps been taken to secure protection for all material IP, for instance including trade secrets?
- Competitive landscape – what other competing digital health technologies are in the market and what are their competitive advantages, e.g. advanced relationship with NHS, etc.?
- Do they have good supply and service contracts in place, and secure sources of hardware, software and labour?

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Generally, the use of digital health solutions in the UK is well established. The COVID-19 pandemic has increased the prevalence of digital health solutions.

However, regarding the delivery of telemedicine services specifically, there remains some legal uncertainty because the UK healthcare regulatory environment is not yet fully updated to deal with the issues arising from the delivery of telemedicine services. However, programmes like the Government's *Life Sciences Vision* and the MHRA's plans for reform to medical device regulation indicate that the regulatory environment is undergoing significant change to address these challenges.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

While not a clinician certification body *per se*, in the UK, the Association of British HealthTech Industries plays a key role in representing the industry to stakeholders, such as the Government, NHS and regulators.

There is continued need for leadership by the UK Government and its relevant ministries, for instance by ensuring that standardised and easily accessible criteria, such as the NICE Evidence standards framework for digital health technologies, are adopted in a risk-based manner.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

This would depend on the digital health solution and in which country in the UK it was deployed. In England, while there may not yet be specific publicly funded provision of general health apps *per se* direct to patients, the provision of, for example, telemedicine may, under certain circumstances, be funded via the NHS. The recent launch of the NICE Office for Digital Health, which will work with strategic partners to improve digital health approval pathways and reimbursement policy, may see future development of funding arrangements for digital health solutions.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

There may be various gaps depending on the complexity of the digital health solution in question, but potential due diligence gaps may include matters relating to data provenance, quality and integrity, regulatory compliance (from a data protection and medical device perspective, among others), interoperability issues, relationships with the NHS and HCPs, ethical considerations, etc.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The UK Government has demonstrated strong commitment to digitising the health system through multiple strategic plans, including the Industrial Strategy, Life Sciences Sector Plan, and the NHS 10-Year Health Plan, with up to £10 billion allocated towards technology and digital transformation in the NHS. Digital will become the default mode of access for most patients, with AI assisting clinicians in documentation, triage, and diagnosis, whilst back-office tools such as ambient voice technology and intelligent task automation will reduce administrative burdens. Key initiatives include new legislation for a Single Patient Record enabling patients to add data from validated wearables, transformation of the NHS App into a "full front door to the entire NHS" by 2028, and a new *Health Store* for centrally procured and funded health apps. Investment of up to £600 million will support the Health Data Research Service to create a secure, AI-ready platform uniting genomic, diagnostic, and clinical data at scale. NICE's technology appraisal process will be expanded to cover digital tools, wearables, and diagnostics with mandated NHS funding for approved tools. Regulatory reform remains critical, with a new framework for AI regulation/guidance scheduled for 2026 alongside wider proposals from the MHRA due in Autumn 2026, particularly to provide clarity on the regulation of SaMD, including AIaMD.

More generally, from 2026 we can expect the expansion of virtual healthcare and remote diagnostics with the greater use of remote diagnostic tools and wearable monitors, AI-supported symptom checking to speed up referrals, and integrated digital care pathways that connect GPs, specialists, and treatment providers.

Acknowledgments

The authors would like to thank David Pemberton and Serena Gordon for their invaluable contributions in the preparation of this chapter.



Pieter Erasmus is a senior associate in the IP Group in London, with a focus on regulatory and commercial IP matters primarily in the life sciences and healthcare sectors. Having a keen interest in all things life sciences and healthcare, he specialises primarily in providing regulatory and commercial advice in relation to a broad range of matters in these sectors. His experience includes advising on the regulation of pharmaceuticals, medical devices, general healthcare services, clinical trials, marketing and advertising of health products, borderline products, food and beverages (including food supplements and novel foods), cosmetic products and legislative drafting in the healthcare context. A key focus area is advising on all aspects relating to digital health, including software as medical device, the impact of AI and telemedicine. His practice further includes specialist transactional work, such as licensing deals, collaborations and the procurement/supply of high-value therapies.

Bird & Bird
12 New Fetter Ln, City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 905 6217
Email: pieter.erasmus@twobirds.com
LinkedIn: www.linkedin.com/in/pieter-miguel-erasmus



Emma Drake is a partner working on data and online safety compliance from the London office. She works with a wide variety of organisations, particularly in the media, sports and life sciences sectors. She also advises extensively on children's and employee privacy matters. Her work covers all aspects of data protection, e-privacy and online safety law, including advice on compliance documentation, policy and procedure, risk and impact assessment and individual rights. She has a particular focus on digital regulation that impacts on the handling of special category data or vulnerable groups, including employees and children. She regularly helps clients with assessment of new products or processes, including across multiple jurisdictions and defence in front of regulators. She has also assisted numerous clients on personal data breaches and knows the importance of prompt pragmatic advice when handling security incidents.

Bird & Bird
12 New Fetter Ln, City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6728
Email: emma.drake@twobirds.com
LinkedIn: www.linkedin.com/in/emma-drake-43a3573b



Tristan Sherliker specialises in resolving IP disputes before the Courts in London, where he is of counsel in the IP practice. He is a solicitor advocate working in leading IP cases and high-technology disputes. His focus is on litigation in the High Court and Court of Appeal, and advisory work to prevent disputes that could otherwise go there. He builds close working relationships with clients with a deep knowledge of their business, their needs and their technology. In disputes, he acts in the dual role of solicitor and counsel. Before law, his background was in biomedical engineering, combining more traditional engineering disciplines (such as electronics, mechanics, materials science and computing) with medical concepts (including anatomy, drug delivery and biochemistry). Technology is still at the centre of his practice, both to handle complicated technical matters, as well as making use of technical innovations to bring cases on efficiently and effectively.

Bird & Bird
12 New Fetter Ln, City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6641
Email: tristan.sherliker@twobirds.com
LinkedIn: www.linkedin.com/in/sherliker



Mario Subramaniam is a partner in our highly rated (*The Legal 500* and *Chambers*) Life Sciences and IP Team, advising life science clients on strategic licensing, collaboration and partnering transactions. He has over 15 years of experience in advising life science clients on the development and exploitation of pharmaceutical, biotech, medtech and digital health technologies, with a particular emphasis on strategic IP licensing, collaboration and partnering transactions, as well as joint ventures, high-value manufacturing, supply and outsourcing arrangements. He also provides strategic support on M&A and asset acquisitions and disposals for life science clients. His background includes substantial periods as a research scientist in immunology and molecular biology and as in-house counsel at several prominent life science companies. This gives him a unique perspective and a deep understanding of the technology and issues involved in complex and innovative transactions.

Bird & Bird
12 New Fetter Ln, City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6000
Email: mario.subramaniam@twobirds.com
LinkedIn: www.linkedin.com/in/mariosubramaniam

Recognised across the major global directories as a top-tier firm for life sciences and healthcare expertise, Bird & Bird is the go-to international law firm for over 50% of the world's largest pharmaceutical and biotechnology companies. We guide our clients through every aspect of the life cycle of innovative healthcare products and services, including incorporation, development and financing, exploitation of IP and portfolio management, regulatory and contractual issues, clinical trials and securing marketing authorisation.

www.twobirds.com

Bird & Bird

USA


Roger Kuan


Jason Novak


Apurv Gaurav

Norton Rose Fulbright

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Digital health is a technology sector that is a convergence of high technology with healthcare. The result is a highly personalised healthcare system that is focused on data-driven healthcare solutions, individualised delivery of therapeutics and treatments to patients powered by information technologies that enable seamless integration and communication between patients, providers, payors, researchers and health information depositories.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging digital health subsectors are:

- Personalised/Precision Medicine (treatments tailored to an individual's uniqueness).
- Clinical Decision Support Tools (analytics tools used to assist physician decision-making).
- Remote Patient Monitoring and Delivery of Care (e.g., Internet of Medical Things, telemedicine, virtual healthcare, mobile applications, wearables, etc.).
- Big Data Analytics (clinically relevant inferences from large volumes of medical data).
- Artificial intelligence/machine learning (AI/ML)-powered Healthcare Solutions (e.g., diagnostics, digital therapeutics, intelligent drug design, clinical trials, etc.).
- Robot-Assisted Surgery (precision, reduced risk of infection).
- Digital Hospital (digital medical information management, optimised hospital workflows).
- Digital Therapeutics (use of digitally enabled devices or software to provide therapeutic treatment to patients).
- Generative AI – generative AI models, such as generative adversarial networks, can be used to generate training data that are used to train traditional AI/ML models that are used for intelligent drug design and AI-powered diagnostics.

1.3 What is the digital health market size for your jurisdiction?

Depending on the source and how they define the digital health market, estimates of the digital health market size in the USA for 2026 can vary, but forecasts are generally around USD100 billion.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Depending on the definition of "digital health company", ones operating in digital health *vs.* solely digital health companies, this answer can differ. For those operating in digital health, the answers can vary, but commonly cited companies are Apple, Pfizer, Medtronic, Phillips, and Epic. For solely digital health companies, the answers can differ, but commonly cited companies are Amwell, Dexcom, Teladoc, IRhythm, and GoodRx.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Depending on the definition of "digital health company", ones operating in digital health *vs.* solely digital health companies, this answer can differ. For solely digital health companies, the answers can differ, but commonly cited companies are:

- Teledoc Health.
- Dexcom.
- GoodRx.
- Hims & Hers Health.
- iRhythm.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

In the United States, the U.S. Department of Health and Human Services (HHS) regulates the general health and safety of Americans through various programmes and divisions, including the U.S. Food and Drug Administration (FDA), Centers for Medicare and Medicaid Services (CMS), Office of Inspector General, Office for Civil Rights (OCR), Department of Defense and Department of Homeland Security, among many others.

The Federal Trade Commission (FTC) regulates digital health through the Health Breach Notification Rule (HBNR). The HBNR requires companies that manage digital health records to notify consumers and the FTC if there is a breach of personal health information. The rule applies to most health

apps that are not covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The FDA is the principle regulatory body charged with administering and enforcing the provisions of the Federal Food, Drug & Cosmetic Act, including those that relate to medical devices and Software as a Medical Device (SaMD). The FDA's jurisdiction covers all products classified as food, dietary supplements, drugs, devices or cosmetics, which have been introduced into interstate commerce in the United States.

In respect of the FDA's regulatory review of digital health technology, the Digital Health Center of Excellence (a part of the FDA based in the Center for Devices and Radiological Health) aligns and coordinates digital health work across the FDA by providing regulatory advice and support to assist in its regulatory review of digital health technology.

The Digital Health Center of Excellence provides services in the following functional areas of digital health:

- Digital health policy and technology support and training.
- Medical device cybersecurity.
- AI/ML.
- Regulatory science advancement.
- Regulatory review support and coordination.
- Advanced manufacturing.
- Real-world evidence and advanced clinical studies.
- Regulatory innovation.
- Strategic partnerships.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

HIPAA, as amended by the Health Information Technology for Economic and Clinic Health Act (HITECH Act), is a core healthcare regulation related to digital health. HIPAA sets forth the federal privacy and security requirements for how certain entities must safeguard protected health information (PHI) (inclusive of electronic PHI (ePHI)) and how to handle security breaches of PHI or ePHI. In the U.S., individual states may also have state-specific healthcare privacy laws that pertain to their state residents that may apply to digital health offerings in a particular state and that may also be more strict than HIPAA.

In addition, a provider of digital healthcare will also be subject to various healthcare laws and regulations designed to promote transparency and prevent fraud, abuse and waste. Such laws and regulations to the extent applicable may include, but are not limited to, the federal Anti-Kickback Statute, the Ethics in Patient Referrals Act (or "Stark Law"), the federal False Claims Act, laws pertaining to improper patient inducements, the federal Civil Monetary Penalties Law, and state-law equivalents of each of the foregoing.

The newly minted "BIOSECURE Act", signed into federal law in December of 2025, restricts federal agencies from contracting with any entity that uses biotechnology equipment or services from "biotechnology companies of concern", primarily those linked to foreign adversaries. By tying federal funding (NIH, BARDA, DARPA, etc.) to foreign involvement, the law has a cascading effect across the public, private and research sectors, making any exposure to certain foreign-controlled biotech platforms (directly or indirectly) a key consideration across the supply chain.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The FDA has expressed its intention to apply its regulatory oversight to only those digital health software functions that are medical devices and whose functionality could pose a risk to a patient's safety if the device were to not function as intended. From a digital health perspective, this is a key area of enforcement, particularly in regard to digital health medical devices that are being marketed without the necessary FDA clearances or approvals in violation of applicable FDCA regulations.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

SaMD is regulated by the FDA and is defined by the International Medical Device Regulators Forum (IMDRF) as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device". SaMD can be used across a number of technology platforms, including medical device platforms, commercial platforms and virtual networks. For example, SaMD includes software with a medical purpose that operates on a general-purpose computing platform.

If the software is part of a hardware medical device, however, it does not meet the definition of SaMD and is not regulated by the FDA. Examples include: software that relies on data from a medical device, but does not have a medical purpose (e.g., encryption software); or software that enables clinical communication such as patient registration or scheduling.

Consistent with the FDA's existing oversight approach that considers functionality of the software rather than platform, the FDA has expressed its intention to apply its regulatory oversight to only those software functions that are medical devices and whose functionality could pose a risk to a patient's safety if the device were to not function as intended. For software functions that meet the regulatory definition of a "device" but pose minimal risk to patients and consumers, the FDA exercises its enforcement discretion and will not expect manufacturers to submit premarket review applications or to register and list their software with the FDA. Examples of such minimal-risk software includes functionalities that help patients self-manage their medical condition without providing specific treatment suggestions or that automate simple tasks for healthcare providers. The FDA publishes a more detailed list of examples of device software functions that are not the focus of FDA oversight.

In regard to the clinical evaluation of SaMD, the FDA issued the *Software as a Medical Device: Clinical Evaluation* final guidance to describe an internally agreed upon understanding of clinical evaluation and principles for demonstrating the safety, effectiveness and performance of SaMD among regulators in the IMDRF. The guidance sets forth certain activities SaMD manufacturers can take to clinically evaluate their SaMD.

It should be noted that the FDA considers mobile medical apps (mHealth apps) to be medical devices if they meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated device. The FDA has published guidance that explains the FDA's oversight of mobile medical apps entitled the *Policy for Device Software Functions and Mobile Medical Applications Guidance*.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Digital health devices and software solutions that are powered by AI and ML technologies are subject to FDA regulations and related review. In April 2019, the FDA published the *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) – Discussion Paper and Request for Feedback*. The FDA remarked in its proposal that "[t]he traditional paradigm of medical device regulation was not designed for adaptive AI/ML technologies, which have the potential to adapt and optimise device performance in real-time to continuously improve healthcare for patients". The FDA also described in the proposal its foundation for a potential approach to premarket review for AI- and ML-driven software modifications.

In January of 2021, the FDA published the *Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan* that included the FDA's plan to update its proposed regulatory framework through a five-part action plan that addresses specific stakeholder feedback. The five-part plan includes the following actions:

- Develop an update to the proposed regulatory framework presented in the AI/ML-based SaMD discussion paper, including through the issuance of a Draft Guidance on the Predetermined Change Control Plan (PCCP).
- Strengthen the FDA's encouragement of the harmonised development of Good Machine Learning Practice through additional FDA participation in collaborative communities and consensus standards development efforts.
- Support a patient-centred approach by continuing to host discussions on the role of transparency to users of AI/ML-based devices. Building upon the October 2020 Patient Engagement Advisory Committee meeting focused on patient trust in AI/ML technologies, hold a public workshop on medical device labelling to support transparency to users of AI/ML-based devices.
- Support regulatory science efforts on the development of methodology for the evaluation and improvement of ML algorithms, including for the identification and elimination of bias, and on the robustness and resilience of these algorithms to withstand changing clinical inputs and conditions.
- Advance real-world performance pilots in coordination with stakeholders and other FDA programmes, to provide additional clarity on what a real-world evidence generation programme could look like for AI/ML-based SaMD.

The FDA highlighted that its work in this area will be coordinated through the Center for Devices and Radiological Health's new Digital Health Center of Excellence.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Agencies, such as the FDA, have historically struggled with the dynamic nature of AI/ML-based digital health solutions. Even in the recent FDA guidance regarding PCCPs for ML-enabled medical devices, the guidance seems to still lean towards versioning. This is understandable given that versioning gives all involved a snapshot of a moment, and all the details that surround that moment, which is consistent with the FDA's traditional approach for static approvals. It also requires that manufacturers have clear foresight as to how they are going to modify their software, or else be subject to a new FDA submission. This call for intense pre-planning around post-launch updates puts a lot of pressure on these product companies to predict change, perhaps sooner than is reasonable.

It is clear the FDA realises the importance of automatic modifications to the software through consistent model retraining, especially with new data inputs. In a 2023 paper discussing FDA market submission recommendations for PCCPs, the FDA effectively noted that while automatic modifications are key in AI/ML, these modifications are more complex and that applying this new FDA policy would be difficult and the FDA's experience will play a part. Further, the Modification Protocol Section of the 2023 paper, particularly the host of questions posed in Appendix A, is seemingly thorough but also seems to lean towards versioning.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data is essential in regulatory review, as it ensures that AI/ML-based digital health solutions perform accurately, safely, and effectively. Companies seeking FDA approval must prioritise well-designed clinical studies and adhere to Good Machine Learning Practices (GMLP) to navigate regulatory pathways successfully.

Clinical validation data factors into the regulatory process as follows:

1. Demonstrating Safety and Effectiveness: The FDA may require AI/ML-based digital health solutions to provide clinical validation data proving that the technology is safe and effective for its intended use. This typically involves:
   - Clinical trials or studies to assess performance.
   - Real-world evidence demonstrating accuracy and reliability.
   - Comparisons to standard care or existing approved devices.
2. Regulatory Pathway Considerations: AI/ML-based digital health solutions may fall under different FDA pathways depending on risk classification:
   - 510(k) Clearance (for moderate-risk devices with a predicate device).
   - *De Novo* Classification (for novel moderate-risk devices without a predicate device).
   - Premarket Approval (PMA) (for high-risk devices, requiring rigorous clinical evidence).

   In all cases, clinical validation data strengthens the submission by proving that the AI/ML model generalises well across patient populations.
3. GMLP: The FDA emphasises GMLP, which includes:
   - Ensuring that AI/ML models are transparent and reproducible.
   - Validating the AI/ML models with diverse datasets to avoid bias.
   - Continuous monitoring and post-market surveillance.

   Aligning clinical validation studies with these principles helps ensure unbiased, reliable AI performance.
4. Adaptivity and Real-World Performance: For continuously learning AI/ML models, clinical validation extends beyond initial approval:

- The FDA has proposed a PCCP, where manufacturers outline how they will validate future model updates.
- Post-market clinical validation may be required to ensure the model remains safe and effective as it evolves.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In the United States, digital health products and solutions are regulated at both the federal and state/regional levels, with differences in oversight based on the type of product, intended use, and risk to patients.

They are differentially regulated as outlined below.

Federal regulation

At the federal level, multiple agencies oversee digital health, with the FDA playing the most significant role.

1. FDA Regulation:
   - The FDA primarily regulates digital health products that qualify as medical devices (i.e., software or hardware used for diagnosis, treatment, or prevention of disease).
   - The level of oversight depends on the product's risk classification:
     - Class I (low risk): Minimal oversight (e.g., wellness apps).
     - Class II (moderate risk): Requires premarket review (e.g., some diagnostic tools).
     - Class III (high risk): Requires rigorous PMA (e.g., AI-powered decision-support tools for critical care).
   - The Digital Health Center of Excellence (part of the FDA) focuses on regulation and guidance for SaMD, AI in healthcare, and cybersecurity.
2. The Office of the National Coordinator for Health Information Technology (ONC):
   - Oversees health IT standards and interoperability, ensuring that electronic health records (EHRs) and digital tools meet federal standards.
   - Implements certification programmes for EHRs and interoperability rules under the 21st Century Cures Act.
3. The FTC:
   - Regulates consumer protection aspects of digital health tools, including data privacy, false advertising, and deceptive marketing claims.
   - Enforces compliance with the HBNR for apps and devices handling sensitive health data.
4. The HHS OCR:
   - Enforce HIPAA for digital health solutions handling PHI.
   - Ensure privacy and security standards are met by telehealth providers, health apps, and cloud-based healthcare services.

State/regional regulation

States have additional authority over digital health solutions, particularly in areas such as telehealth, professional licensing, and data privacy.

1. Telehealth regulation:
   - States determine licensing requirements for healthcare providers delivering telehealth services.
   - Some states participate in interstate compacts (e.g., the Interstate Medical Licensure Compact) that allow providers to practise across state lines with a streamlined licensing process.
   - Reimbursement policies for telehealth services vary by state Medicaid programmes and private insurers.
2. Data privacy and security:
   - Some states have stricter privacy laws than HIPAA, such as:
     - The California Consumer Privacy Act (CCPA), which provides additional protections for consumer health data beyond federal requirements.
     - The California Genetic Information Privacy Act, which focused on maintaining the privacy of genetic information.
     - Washington's My Health My Data Act, which regulates health data not covered by HIPAA.
     - Several states are adopting AI and cybersecurity regulations affecting digital health applications.
3. Consumer protection and digital health companies:
   - State Attorneys-General can investigate misleading health claims or unfair business practices related to digital health products.
   - Some states have specific regulations for digital pharmacies, remote prescribing, and direct-to-consumer health apps.

The federal government provides overarching regulations for digital health, especially for medical devices, health IT standards, and data privacy under HIPAA. However, states retain authority over telehealth practice, professional licensing, and consumer protection, leading to variability in how digital health products and solutions are regulated across the U.S. Companies operating in this space must navigate both FDA and state-specific laws to ensure compliance.

Key differences in regulation by federal and state/regions

Aspect	Federal Regulation (FDA, FTC, HHS)	State/Regional Regulation
Medical device oversight	FDA regulates SaMD and digital health tools based on risk.	States do not regulate medical devices but can regulate their use.
Telehealth licensing	No federal licence; CMS sets reimbursement rules.	States regulate provider licensing and practice requirements.
Privacy and security	HIPAA applies to covered entities.	Some states (e.g., CA, WA) have stricter laws.
Consumer protection	FTC regulates false advertising and data breaches.	State Attorney-Generals enforce local consumer protection laws.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Regulatory enforcement actions for digital health products and solutions in the United States are being tailored through a combination of existing laws, new guidance, and risk-based approaches by agencies like the FDA, FTC, and HHS, among others.

Enforcement is evolving as follows:

1. Risk-based FDA oversight: The FDA has adopted a risk-based approach to digital health regulation, focusing on SaMD, while exercising enforcement discretion for lower-risk products. Key actions include:
   - Guidance on AI/ML in medical devices: The FDA is developing frameworks for ML-based software that adapts over time.
   - Pre-Certification Pilot Program: Aimed at streamlining approvals for trustworthy developers rather than individual products.
   - Digital health software exemptions: Certain mobile health apps and wellness products are not actively regulated if they pose low risk to patients (e.g., fitness tracking apps).
2. The FTC's focus on consumer protection and privacy: The FTC enforces privacy, data security, and deceptive advertising regulations for digital health companies. Notable actions include:
   - HBNR enforcement: Targeting health apps and digital platforms that fail to safeguard sensitive health data.
   - False advertising claims: Taking action against companies that make unproven health benefit claims about digital therapeutics or wearables.
3. HHS and HIPAA enforcement for health data: OCR enforces HIPAA compliance, focusing on how digital health apps and telehealth services handle patient data. New rules under HHS expand protections around health data sharing, particularly as part of interoperability and information blocking regulations.
4. State-level regulations and Attorneys-General actions: State Attorneys-General are also stepping in to enforce consumer protection laws on digital health tools, particularly around:
   - Data privacy (CCPA in California, for example).
   - Telehealth licensing and reimbursement policies.
   - AI-driven healthcare decision-making.
5. Emerging regulatory trends: FDA's new Digital Health Center of Excellence to refine oversight strategies, such as:
   - AI-specific regulations are being debated in Congress, particularly for bias and explainability in healthcare algorithms.
   - Cybersecurity enforcement is increasing for connected medical devices.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  - State-specific practice of medicine licensing laws and requirements.
  - Data privacy laws including HIPAA, CCPA and HITECH Act with respect to health data that is collected from patients during consultation.
  - Data rights to health data collected from patients during consultation.
  - FDA regulatory issues such as SaMD, 510k certification and PMA.
  - Stark Law and Anti-Kickback statutes.
- **Robotics**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with respect to health data that is collected and used to train software used to operate the robotic device.
  - Tort liability (products liability or negligence theories) for injuries sustained by patients during surgery.
  - FDA regulatory issues such as 510k certification and PMA.
- **Wearables**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is collected by devices.
  - Data rights to health data that is collected from device wearers.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer seeks to make diagnostic or therapeutic claims for their devices.
- **Virtual Assistants (e.g. Alexa)**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to voice and Wi-Fi signal data that is collected by the virtual assistant.
  - Data rights to the voice and Wi-Fi signal data that is collected by the virtual assistant.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer seeks to make diagnostic or therapeutic claims for the virtual assistant.
- **Mobile Apps**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is collected by the mobile app.
  - Data rights to the health data that is collected by the mobile app.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer seeks to make diagnostic or therapeutic claims for the mobile app.
  - Tort liability (products liability or negligence) for injuries sustained by patients using mobile apps for diagnostic or therapeutic purposes.
  - Issues related to the patentability of software or diagnostics inventions.
- **Software as a Medical Device**
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer makes diagnostic or therapeutics claims for the software. Unique issues with evaluating safety and efficacy of software used to diagnose or treat patients.
  - Issues related to patentability of software of diagnostics inventions.
- **Clinical Decision Support Software**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is used in the software.
  - FDA regulatory issues such as SaMD, 510k and PMA if the developer seeks to make diagnostic or therapeutic claims for the software.
  - Tort liability (products liability or negligence) for injuries sustained by patients using the software for diagnostic or therapeutic purposes.
  - Issues related to the patentability of software or diagnostics inventions.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  - Inventorship issues with inventions arising out of AI/ML algorithms.
  - Clinical adoption of AI/ML software that is used in a clinical setting.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer makes diagnostic or therapeutics claims for the AI/ML-powered software. Unique issues with evaluating safety and efficacy of AI/

ML-powered software used to diagnose or treat patients.
    - Data rights issues related to the data sets that are used to train AI/ML software. This is even more complicated if the training data set includes data sets from multiple parties with differing levels of data rights.
- **IoT (Internet of Things) and Connected Devices**
    - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is collected by the IoT and connected devices.
    - Data rights to the health data that is collected by the IoT and connected devices.
- **3D Printing/Bioprinting**
    - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to handling patient imaging data used as 3D printing templates.
    - FDA regulatory issues such as SaMD, 510k, PMA and Biologics Licence Application depending on whether the manufacturer is making and selling rendering software, printing equipment and bioink with cells or other biological compositions.
- **Digital Therapeutics**
    - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is used in or collected by the software and/or devices.
    - FDA regulatory issues such as SaMD, 510k and PMA if the developer seeks to make therapeutic claims for the software and/or devices.
    - Tort liability (products liability or negligence) for injuries sustained by patients using the software or devices for therapeutic purposes.
    - Issues related to the patentability of software or diagnostics inventions.
- **Digital Diagnostics**
    - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to patient health data (e.g., biomarkers) that is used in or collected by the software and/or devices for the purpose of diagnosing medical conditions.
    - FDA regulatory provisions, such as SaMD, 510k and PMA, if the developer seeks to commercialise the digital diagnostics product (e.g., SaMD).
    - Tort liability (products liability or negligence) for injuries sustained by patients relying on a digital diagnostics product to undertake decisions that lead to the injury.
    - Issues related to the patentability of software or diagnostics inventions.
- **Electronic Medical Record Management Solutions**
    - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to patient health data that is used in or collected by the software and/or devices, and then processed and/or stored by electronic medical record (EMR) systems and/or other hospital information systems.
    - Data rights to the patient health data that is collected by software and/or devices and then processed and/or stored by EMR and other hospital information systems.
    - Issues related to the patentability of software, data processing or EMR management inventions.
- **Big Data Analytics**
    - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to any PHI or other sensitive data that is used in or collected by the software and/or devices.
    - Data rights to the PHI or other sensitive data that is collected by software and/or devices.
    - Issues related to the patentability of big data analytics inventions.
- **Blockchain-based Healthcare Data Sharing Solutions**
    - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to any protected health data that is used in or collected by the software and/or devices, rendered accessible to others in the blockchain network, or shared to other software and/or devices.
    - Data rights to the patient health data that is used in or collected by software and/or devices the software and/or devices, rendered accessible to others in the blockchain network, or shared to other software and/or devices.
    - Issues related to the patentability of software or blockchain-based healthcare data sharing inventions.
- **Natural Language Processing**
    - FDA regulatory issues if the natural language processing (NLP) software is used as part of a medical device or SaMD used as a diagnostic or therapeutic purposes.
    - Tort liability (products liability or negligence) for injuries sustained by patients using these apps or devices, that incorporates the NLP software, for diagnostic or therapeutic purposes.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The key issues for digital platform providers are:
- Compliance with data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is collected by the providers.
- Obtaining data rights to the health data collected from customers/patients by complying with informed consent requirements.
- Data sharing and intellectual property (IP) provisions in agreements.
- Tort liability (products liability of negligence) for injuries sustained by patients using these platforms for diagnostic or therapeutic purposes.
- Issues related to the patentability of software or diagnostics inventions.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

HIPAA is the primary and fundamental U.S. federal law related to protecting patient health information. In relation to HIPAA, the HITECH Act, signed into law in 2009, further increased patient rights by financially incentivising the adoption of EHRs and increased privacy and security protection, and also increasing penalties to Covered Entities and their Business Associates for HIPAA violations. The CCPA, enacted in 2018, is an example of a state statute primarily focused on addressing

the enhancement of privacy rights and consumer protection for that state's residents. Similar applicable laws exist in many U.S. states. Especially for data transactions with the EU, the General Data Protection Regulation (GDPR), in force since May 2018, protects natural persons in relation to the processing and movement of personal data.

There are a myriad of considerations that may arise from these laws and regulations. For example, what type of personal data is being used? If it is PHI, it would thereby be subject to HIPAA. Contrast this with wellness data, for example, which would appear to be health-related but in reality, is separate and distinct and, therefore, not regulated by HIPAA. Of course, personal data in general is subject to various state, federal and international data privacy laws.

Furthermore, what is the intended purpose of this data? Defining this purpose early and often is essential as it will become core to the metes and bounds of the data transaction and will help with the initial undertaking of seeking appropriate (patient) consents, which is far easier to do at the outset.

Even further, what are potential secondary uses of the data? Defining secondary uses up front is also important as a data user must maximise the value of the data transaction. Failing to set the expectation early may result in a data transaction of limited scope, forcing a data user to either seek amendment to the existing transaction or the need for a second agreement. In either case, leverage in negotiation will quickly pivot to the data holder, who will now have a clear idea of the importance to the data user of these secondary users.

Even further, where is the data coming from and where is it going? To answer this, detailed data maps need to be developed, tracing the path of data across various states and nations, thereby identifying the jurisdictions that will define the scope of data compliance requirements for a data user. As stated above, each impacted territory, whether state or country, may have unique data compliance (data privacy) laws that must be accounted for in executing the data strategy. Of note, data mapping is a requirement under several of the potentially applicable healthcare laws and as such, it factors into several parts of the data strategy.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In the United States, personal health data is regulated at both the federal and state levels, with some variations in scope and strictness. The federal government sets baseline protections, while states can impose additional or stricter regulations. Below is a breakdown of how these regulations differ:

1. Federal-level regulation: At the national level, the key laws governing personal health data include:
   - HIPAA:
     - Regulates how covered entities (healthcare providers, insurers, and clearinghouses) handle PHI.
     - Requires patient consent for data sharing, with exceptions for treatment, payment, and healthcare operations.
     - Enforced by the HHS OCR.
   - 21st Century Cures Act and Information Blocking Rules:
     - Promotes patient access to EHRs and prohibits providers from blocking information sharing.
     - Enforced by HHS and ONC.
   - FTC Act and Consumer Data Privacy Laws:
     - The FTC regulates consumer health apps, wearables, and other non-HIPAA-covered health data under unfair/deceptive practices rules.
     - The FTC HBNR applies to health apps and non-traditional health data handlers.
   - Substance Use and Mental Health Privacy (42 CFR Part 2):
     - Stricter than HIPAA, requiring explicit patient consent before sharing substance use disorder treatment records.
     - Enforced by the Substance Abuse and Mental Health Services Administration (SAMHSA).
2. State-level regulation: States can expand protections beyond federal laws, and many have done so, particularly regarding:
   - Comprehensive consumer privacy laws: Some states, like California (CCPA/CPRA), Virginia (VCDPA), and Colorado (CPA), have privacy laws that cover personal health data outside HIPAA (e.g., fitness trackers, genetic data, wellness apps). These laws often require opt-in consent, data minimisation, and stricter consumer rights.
   - Genetic data privacy: States like California, Arizona, and Illinois have enacted laws regulating genetic testing companies (e.g., 23andMe), requiring explicit consent for sharing genetic data.
   - Biometric data privacy: Illinois' Biometric Information Privacy Act (BIPA) is one of the strictest laws in the country, requiring informed consent before collecting biometric data, including health-related biometrics.
   - Health Information Exchange (HIE) and data sharing rules: Some states, like New York and Texas, impose additional rules on how healthcare providers and HIEs handle and share patient data.
   - Reproductive and mental health data protections: Post *Dobbs v. Jackson Women's Health Organization*, some states (e.g., California, Washington, and New York) have enacted laws protecting reproductive health data from subpoenas and law enforcement in states where abortion is restricted.

Key differences between federal and state regulation

Aspect	Federal (Nationwide)	State-Level (Varies by State)
Scope	HIPAA applies to healthcare entities; FTC oversees non-HIPAA health data.	States may regulate broader categories, including consumer health apps and genetic data.
Consent rules	HIPAA allows some data sharing without consent.	Some states require opt-in consent for data sharing.
Genetic data	Governed by the Genetic Information Non-discrimination Act, but limited.	Some states require explicit consent for genetic data use.
Enforcement	HHS (OCR), FTC, SAMHSA.	State Attorneys-General, privacy commissions.

Aspect	Federal (Nationwide)	State-Level (Varies by State)
Reproductive health	No specific federal protection post-*Dobbs*.	Some states protect abortion-related data from out-of-state requests.
Penalties for violations	Civil and criminal penalties under HIPAA, FTC fines.	State-specific fines and private lawsuits (e.g., BIPA in Illinois).

In summary, the federal government provides a baseline level of health data protection through HIPAA and other laws, while states fill in the gaps and sometimes impose stricter protections. The biggest regulatory gaps occur with non-HIPAA health data (like fitness trackers, apps, and direct-to-consumer genetic tests), where state laws are stepping in to add stronger privacy safeguards.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

Assuming the data under consideration is PHI, in dealing with HIPAA, a threshold determination is whether one is an entity subject to HIPAA (referred to as a "Covered Entity"), or a "Business Associate" of said Covered Entity by way of providing certain services for the Covered Entity. Covered Entities, aside from providers of healthcare that bill through claims, include, for example, government healthcare programmes (e.g., Medicare, Medicaid, military health programmes, veteran health programmes), health maintenance organisations, employee sponsored health plans and health insurance companies. Business Associates are parties (person or entity) that are not part of a Covered Entity workforce but, by virtue of acting on behalf of, or providing certain services to, a Covered Entity, receive access to PHI that is in the possession of the Covered Entity and which the Covered Entity has responsibility for.

4.4 How do the regulations define the scope of personal health data use?

Regulations concerning PHI, HIPAA and HITECH define the allowable scope of data use. According to HIPAA, the permitted data use for PHI includes the provisioning of healthcare (e.g., the treatment of patients), processing of healthcare payments and insurance claims, and facilitating the provisioning of healthcare (e.g., internal operations in hospitals and other facilities for the treatment of patients). HIPAA additionally requires limiting the use of PHI to the minimum possible extent that is necessary to fulfil the permitted use. Any data uses not explicitly permitted by HIPAA requires patient consent. However, even in situations where data use is permitted under HIPAA, it is important to check state privacy laws as they may restrict the scope of data use or require consent.

The HITECH Act further limits the scope of data use for PHI by strengthening privacy and security protections required under HIPAA. For example, the HITECH Act expands the enforcements of HIPAA data use requirements to Business Associates of HIPAA Covered Entities (e.g., cloud storage providers and billing companies of HIPAA Covered Entities). Furthermore, the HITECH Act enables patients of the PHI to request copies of EHRs and restrict disclosures of their PHI. Additionally, the HITECH Act mandates that any Covered Entities and Business Associates need to report breaches in data security of PHI.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The key contractual terms to consider depend on what is being contracted. For example, for a data transaction involving entities as part of collaborative research, it is essential to clearly define IP rights arising out of the research, as well as primary and secondary uses of the data. Field restriction language can also become important, as it can minimise the impact of a data transaction agreement to a company's overall business strategy. With PHI involved, if an involved entity has been identified as a Business Associate, then a Business Associate Agreement may be needed between the Business Associate and Covered Entity. With non-PHI involved, data processing agreements may still be needed for handling data, even though it is not subject to HIPAA. Other potentially important terms include terms addressing data breaches, data handling during and after the agreement period, and associated representation/warranty language associated with any breach.

Securing comprehensive rights is extremely important. Healthcare data is exceptionally valuable – valuable to both the patient and the company that is able to procure such data. Given its criticality, one must have permission to use healthcare data for a desired purpose. Regardless of whether the healthcare data is generated or acquired by the data user, the data user must have the consent of the data's ultimate owner, i.e., the patient, to use that healthcare data. In the cases where healthcare data is acquired from a third party, the data user must also have the consent of the third party to use the healthcare data for a desired purpose. Often, consent from a third party (e.g., a healthcare data warehouse or aggregator) comes in the form of a data transaction, whereby said data user will usually remunerate the third party to acquire the healthcare data for the desired purpose. Of course, the consent between data owner and data user will come via the data owner providing consent to this third party to transact the data to parties such as the data user. It is worth noting that a healthcare data warehouse or aggregator does not solely mean data mines such as personal genomics companies 23andMe and Ancestry. It also includes traditional entities such as hospitals and hospital systems, universities, research institutes and pharmaceutical companies. Consent can come in a variety of ways, but it is critical to be able to demonstrate such consent for any downstream data use.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Although case law for issues involving data inaccuracy, bias and/or discrimination are still developing, such issues may violate civil rights laws when it causes disparate impact (e.g., in healthcare) and perpetuates inequality. For example, if the use of an AI model trained on biased data results in the prescribing of different treatment options for different protected groups, this conduct could potentially violate anti-discrimination laws present, for example in Title VI and Section 1557 of the Affordable Care Act.

Furthermore, the use of problematic AI models having the aforementioned issues for medical treatment can lead to other liabilities. For example, if a patient is harmed as a result of the use of a biased AI model by a medical doctor, the patient may be able to issue a medical malpractice claim. The developers of the problematic AI model can also be held liable if they knew of the issues but failed to correct them.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

HIPAA is very relevant here, as it serves as the primary U.S. standard governing the use and collection of healthcare data, outlining privacy and security regulations for PHI managed by healthcare providers, plans and clearinghouses, ensuring patient data is handled responsibly and with appropriate safeguards. Key portions of HIPAA include the Privacy Rule (related to how PHI can be used, disclosed and accessed, including patient rights to access their medical records and request amendments), as well as the Security Rule (which discusses specific technical and administrative safeguards to protect ePHI, including access controls, encryption and data integrity measures). Also relevant here is the Health Level Seven (HL7) standard, which is widely used to facilitate electronic exchange of medical information between different healthcare systems. HL7 is discussed in more detail in section 5 below.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key issues include data privacy and security generally, regardless of whether the information is PHI. For personal data in general, as discussed herein, entities dealing in data must consider the regulatory requirements across different jurisdictions. For U.S. data sharing, federal and state laws must be considered. For international data sharing, ex-U.S. regulatory schemes must fold into a data sharing strategy.

When the personal data is PHI, the regulatory requirements only increase, with federal laws such as HIPAA and the HITECH Act to consider.

From a personal standpoint, each individual must recognise their own personal right to their data, and must consider agreeing to consent agreements that may provide entities with the right to transact one's personal data beyond the scope said individual might desire.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

This is not applicable.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

When data is PHI and subject to federal regulations such as HIPAA and the HITECH Act, entities that qualify as Covered Entities and Business Associates may have to execute Business Associate Agreements to be in proper standing, and may have to ensure that all associated parties involved meet the obligations imposed by federal laws for the handling of PHI.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

As discussed herein, HIPAA provides standards for creating, maintaining and sharing healthcare data. For example, the HIPAA Permitted Uses and Disclosures defines the circumstances in which a Covered Entity may use or disclose an individual's PHI without having to first obtain a written authorisation from the patient. State laws are known to be even more stringent in their standards for creating, maintaining and sharing healthcare data. Furthermore, both federal and state laws prohibit the use of PHI and/or other protected healthcare data beyond what is necessary, and specify deletion and/or disposal requirements. For example, the Privacy Rule in HIPAA states that "a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request". Furthermore, HIPAA mandates that unused media containing PHI should be adequately destroyed.

There are also initiatives to create standards for creating, maintaining and sharing healthcare data that facilitate interoperability. For example, the Consolidated Health Informatics initiative announced its requirement that all federal healthcare services agencies adopt the primary clinical messaging format standards (i.e., the HL7 Version 2.x (V2.x) series for clinical data messaging, Digital Imaging and Communications in Medicine (DICOM) for medical images, National Council for Prescription Drug Programs (NCPDP) Script for retail pharmacy messaging, Institute of Electrical and Electronics Engineers (IEEE) standards for medical devices, and Logical Observation Identifiers, Names and Codes (LOINC) for reporting of laboratory results) (Office of Management and Budget, 2003).

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

In a federated model of healthcare data sharing, multiple entities may function as nodes of an interconnected but decentralised network, and each node may locally store healthcare data. Furthermore, healthcare data can be queried or otherwise analysed by other nodes in the network without the healthcare data necessarily leaving the node at which it is located.

One of the major issues to consider for federated models of healthcare data sharing is interoperability. Specifically, one should consider whether the format (e.g., structures, concepts, syntax, ontologies) of healthcare data stored by each node is harmonised or can be readily converted to a format amenable to other nodes. For example, if a given (first) node of the federated model requests healthcare data stored by another (second) node, the healthcare data stored by the second node may need to be converted into a format that is understandable by the first node. As discussed herein, various initiatives have required or encouraged data sharing formats to facilitate interoperability for healthcare data (e.g., the HL7 V2.x series for clinical data messaging, DICOM for medical images, NCPDP Script for retail pharmacy messaging, IEEE standards for medical devices, and LOINC for reporting of laboratory results).

Another issue to consider is whether the federated model ensures privacy, data security and the appropriate level of access control for healthcare data being stored at each node. For example, depending on the node (e.g., a pharmacy information system, a radiology system, a clinical research institution, etc.), different stakeholders may be granted different levels of access to healthcare data stored in the node.

Yet another issue is the need to actively manage the healthcare data stored across the different nodes of the federated model. For example, there may exist potentially incomplete, unsynchronised and heterogenous healthcare data among various nodes of the federated model. Since this could impair healthcare for patients, the various nodes of the federated model should have a system by which to ensure that the healthcare data stored across the various nodes are updated and/or complete.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

As relevant to digital health, current U.S. patent law is generally unfavourable towards the subject matter patentability of software and diagnostics inventions. As such, successfully navigating the subject matter patentability hurdle is the first step to protecting digital health solutions. Recent U.S. Supreme Court and Federal Circuit cases have begun to chip away at this hurdle for diagnostics innovation (See *Hikma Pharmaceuticals USA Inc. v. Vanda Pharmaceuticals Inc.* (https://www.scotusblog.com/case-files/cases/hikma-pharmaceuticals-usa-inc-v-vanda-pharmaceuticals-inc) and *CardioNet, LLC v. InfoBionic, Inc.* (https://law.justia.com/cases/federal/appellate-courts/cafc/19-1149/19-1149-2020-04-17.html)) and the current expectation is that future cases will continue to swing towards affirming protection for this important class of innovation. In addition to satisfying the subject matter hurdle, novelty and non-obviousness are also required for patentability.

Regarding software innovation, U.S. patent case law has established that patenting an "abstract idea" is not permitted. An abstract idea covers concepts that are considered too fundamental or theoretical, and therefore lacking practical application. This can include, for example, mathematical formulas, basic mental processes, fundamental economic principles, and methods of organising human activity. Digital health-related concepts and principles may be considered under the umbrella of abstract ideas, and thus subject to particular tests that either label or establish an inventive concept beyond that abstract idea. In the past few years, however, the U.S. Patent and Trademark Office (USPTO) has provided more guidance to overcome such rejections and more software cases are seeing positive results at the federal courts.

The term of utility patent protection (with certain exceptions) is 20 years (15 years for design patents) from the date of filing the application. A patent gives the patent owner an affirmative right to exclude others from making, using or selling the patented invention.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

For digital health solutions, copyright protects the software source code and object code as works of authorship, and databases as compilations (provided there is sufficient originality in the structure, sequence and organisation of the database to meet the originality requirement). While copyrights arise automatically, the U.S. has a formal process to register copyrights, which is a prerequisite for commencing a copyright infringement action. Registered copyrights are eligible for "statutory damages" under the Copyright Act, which can help mitigate the difficulties in establishing the monetary value damages due to the copyright infringement. Copyrights that are registered within five years of publication establish *prima facie* evidence of the validity of the copyright and facts stated in the copyright registration certificate. Also, the burden of proof of non-infringement shifts to the alleged infringer.

To register software source code (or object code) or a database with the U.S. Copyright Office (a part of the Library of Congress) a "registration deposit" copy of the software code or database must be deposited that meets the requirements under the Act. The term of copyright protection is the life of the author plus 70 years, unless the work had been created as a work made for hire, in which case the term is the shorter of 120 years after creation or 95 years after publication.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secret protection can be used to protect formulas, practices, processes, designs, instruments, patterns or compilations of information that is not generally known to the public and have inherent economic value. Trade secrets have no fixed term but require the owner to appropriately mark the information and to put in appropriate safeguard measures to guard the information from being released to the public. However, unlike patents, trade secrets cannot prevent independent development of the trade secret information.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Most academic institutions require their professors, researchers and students to assign any IP they develop with the institution's resources or funding to back them. In some instances, the institutions, applicable departments and the professor/researcher enter into separate royalty sharing agreements.

The IP is typically out-licensed to third parties for commercialisation on terms that may include: royalties; upfront payments; milestone payments; and equity in the licensee company.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

SaMD, which the FDA defines as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device" can be protected by patents, copyrights and/or trade secrets. SaMD source code and objects can be copyrightable and protected as trade secret subject matter (providing that they are appropriately marked and appropriate protections are put into place to ensure that they are not released to the public). A SaMD can also be protectable by patents if it meets U.S. subject matter

patentability requirements and is novel and non-obvious over the prior art.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

In the United States, both the courts (in *Stephen Thaler v. Andrew Hirshfeld*, E.D.Va., 2021) and the USPTO have ruled that an AI machine cannot be an "inventor" for purposes of the U.S. Patent Act (35 U.S. Code). According to the courts, the issue of whether an AI device can be considered an inventor depends on the simple question of whether an inventor needs to be a human being. The Patent Act explicitly states, in its definitions, that inventors are "individuals". Since there is sufficient precedent supporting the conclusion that "individuals" are human beings, the courts concluded that non-humans, such as AI programs, cannot be considered individuals, and therefore cannot be considered inventors.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

In the U.S., the Bayh-Dole Act of 1980 (35 U.S.C. § 200–212) deals with inventions arising from federal government-funded research. Before the enactment of the Bayh-Dole Act, the government's consistent position was that the results of any research and development funded with taxpayer's money should be in the public domain and freely available to the public.

The Bayh-Dole Act permits qualified small businesses and non-profits to retain title to "subject inventions" arising out of federal-funded research providing that they comply with the following conditions: (1) the federal government receives a licence in subject inventions; (2) the private party has properly notified the government of the subject inventions; (3) the preference for U.S. industry that is found in all technology transfer programmes is included; and (4) the federal government retains "march-in rights". Within this framework, a "subject invention" is any invention of a qualified private party (i.e., small business or non-profit) conceived or first actually reduced to practice in the performance of work under a funding agreement. Whereas, "march-in rights" permit the federal government to order a private party to grant a compulsory licence to a third party (including competitors) when they make a determination that the private party has not: (1) taken effective steps to achieve practical application of the invention within a reasonable time; (2) reasonably satisfied national health and safety needs; (3) reasonably satisfied regulatory requirements for public use; or (4) received the required permission from the government under the U.S. industry preference provision before licensing.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Several key legal cases and decisions have shaped IP rights protection for digital health innovations in the United States. These cases span patent law, copyright, and trade secrets, affecting how digital health technologies are protected. Below are some of the most important precedents:

1. Patent law and software-related digital health innovations

Alice Corp. v. CLS Bank International (2014) – 573 U.S. 208:

- This Supreme Court decision established the two-part test for patent eligibility of software and abstract ideas.
- Many digital health innovations rely on software-based processes, and this case has led to numerous invalidations of patents related to health IT and medical algorithms that are deemed abstract.
- It has made it harder to patent AI-driven health diagnostics and decision-support tools unless they involve a concrete technological improvement.

Mayo Collaborative Services v. Prometheus Laboratories (2012) – 566 U.S. 66:

- The Court ruled that laws of nature and natural correlations (such as biomarker-based diagnostic methods) are not patentable unless they contain an inventive step beyond merely applying a natural law.
- This case significantly affected precision medicine and digital health patents involving AI-driven diagnostics and personalised treatment algorithms.

Association for Molecular Pathology v. Myriad Genetics (2013) – 569 U.S. 576:

- The Supreme Court held that naturally occurring DNA sequences cannot be patented but synthetic DNA (cDNA) could be.
- This decision impacted digital health companies using genetic data and sequencing technologies.

2. Copyright protection in digital health

Google LLC v. Oracle America, Inc. (2021) – 593 U.S.:

- The Supreme Court ruled that Google's use of Java APIs in Android was fair use.
- This case has implications for interoperability in digital health software, especially regarding whether the reuse of APIs in health IT systems and EHRs can be protected by copyright or subject to fair use.

3. Trade secret protection in digital health

Epic Systems Corp. v. Tata Consultancy Services Ltd. (2020):

- A jury awarded Epic Systems nearly USD1 billion in damages after Tata misappropriated trade secrets related to Epic's EHR software.
- This case underscores the importance of trade secret protection for digital health technologies, especially for proprietary algorithms and data analytics.

Waymo LLC v. Uber Technologies, Inc. (2018):

- Google's self-driving car subsidiary sued Uber over alleged trade secret theft involving AI and sensor technology.
- Although not strictly a digital health case, it demonstrated how AI-driven innovations can be protected under trade secret law, which applies to AI-powered health diagnostics and medical robotics.

4. FDA and regulatory considerations affecting digital health IP

Apple Inc. v. Masimo Corp. (Ongoing, 2023–2024):

- Masimo sued Apple, alleging that Apple stole its pulse oximetry technology for use in the Apple Watch.
- This case is significant for digital health wearables and raises questions about trade secrets *vs.* patent protection.

These cases illustrate how digital health innovations face complex IP challenges. Patent law limits software and diagnostic method protections, copyright law affects software interoperability, and trade secrets provide alternative protections.

Given the evolving legal landscape, companies developing digital health technologies must carefully navigate IP strategies, including patents, trade secrets, and regulatory compliance.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Collaborations are commonplace in digital health and can generally be grouped into two categories: collaborations that are data driven; and those that are technology driven.

In data-driven digital health collaborations, the parties are interested in granting, acquiring or sharing access to data that is used to power digital health solution(s).

Typical data-driven collaboration scenarios are:

- A healthcare institution (e.g., hospital system, hospitals, clinics, community health organisations, etc.) sharing their patient data (typically patient medical records, biological samples used to generate data, questionnaires, etc.) with a company that utilises the data to discover or power their digital health solution(s).
- A university or non-profit research organisation sharing their research data with a company that utilises the data (typically genomic, proteomic, microbiome, study results, etc.) with a company that utilises the data to discover or power their digital health solution(s).
- Companies sharing patient or research data where the data flows from one company to the other or between the companies to discover or power their digital health solution(s).

In technology-driven digital health collaborations, the parties are interested in either obtaining technology from one another or sharing their collective technologies to develop the digital health solution(s).

Typical technology-driven collaboration scenarios are:

- A university or non-profit research organisation sharing their technology or know-how with a company that utilises that technology for their digital health solution(s).
- Companies sharing technology or know-how to develop combined digital health solution(s).

Ownership of IP rights (e.g., patents, copyrights, technical know-how, research results/data, etc.) to the collaborative improvements that result from the shared data and technologies can be governed by U.S. IP laws and/or in the terms of the agreement between the parties. Although the default stance is typically joint ownership, data owners have unique negotiation leverage to insist that they own the IP rights (with the data recipient being granted a licence or option to those rights) since their data is the core asset in the collaboration.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

The most important legal considerations to pay attention to in agreements between healthcare and non-healthcare companies are data privacy compliance and data rights.

With respect to data privacy compliance, the parties need to pay attention to their respective roles and responsibilities in the agreement as it relates to compliance with HIPAA and patient informed-consent requirements. Failure to properly develop and/or execute processes that are compliant with HIPAA or informed-consent requirements can result in patient data that is tainted, which will encumber its use by the parties.

Data rights is another important consideration in this type of agreement where data (e.g., patient medical records, questionnaires, etc.) is typically owned by the healthcare company which then shares it with the non-healthcare company. It is important for the non-healthcare company to secure the data rights it needs from the healthcare company so that they can use the data for what they need it for and to have the healthcare company warrant or represent that they have properly secured the rights to the data from their patients.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Although AI can revolutionise healthcare based on the large volume of medical data that is now available, AI is restricted in its ability to do so because medical data is often siloed among different entities (e.g., companies, institutions, systems) with barriers preventing access to such medical data. These barriers often arise from data privacy concerns. Federated learning may provide a solution to this problem by training AI models collaboratively without exchanging the patient-specific healthcare data itself. While the training for these AI models may occur locally (e.g., at a participating company), the results of the trained AI model (e.g., weights, parameters, etc.) can be transferred elsewhere in the federated network (e.g., to a different company in the federated network). Although federated learning, in theory, obviates the privacy concerns associated with sharing patient-specific healthcare data among different companies in a federated network, the sharing of federated learning data (e.g., the weights or parameters of a locally trained AI model) is not bullet-proof in eliminating all privacy and data security concerns, and may additionally lead to other issues to consider.

For example, since locally trained AI models are based on locally available healthcare data, locally trained AI models based on non-heterogeneous, non-diverse or small-sized healthcare data may potentially reveal private information about a set of patients that may not have provided consent. Thus, even in a federated learning environment, additional privacy-preserving measures may be implemented when exchanging the results of locally trained ML models across companies.

Secondly, since locally available healthcare datasets used to train the ML models in federated learning are characteristically smaller in comparison to healthcare data available to companies and entities across the healthcare landscape, the ML models thus trained may not necessarily have the best performance. Simply put, there may be a trade-off between the advantages of preserving data privacy conferred through federated learning, and the reduced performance of the ML models developed through federated learning.

Therefore, when entering federated learning healthcare data sharing agreements, a party should consider the trustworthiness of other members of the healthcare data sharing agreement to strike the right balance in this trade off. For example, when there are trusted parties, there is a reduced need for additional privacy-preserving countermeasures, and the parties may opt for ML models with optimal e-performance. On the other hand, for federated learning that occurs among parties that may not all be trustworthy, additional measures may be

required to mitigate data security risks. Such additional measures may include, for example, advanced encryption of trained ML models, secure authentication and verification systems of all parties, differential privacy and protections against adversarial attacks.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Although generative AI has the potential to revolutionise the healthcare industry, parties seeking to use generative AI in the provisioning of digital health solutions should consider the following factors:

- Parties should be cautious of the overreliance of generative AI tools and products for digital health solutions. In particular, generative AI models are known to often produce false results (i.e., hallucinations). When treatment recommendations are based on such results, the effect on the user's health can be potentially catastrophic, and companies using the generative AI can be held liable.
- Generative AI models rely on large amounts of data for their development. Parties should determine whether such data includes PHI or any information that otherwise identifies known individuals. In particular, HIPAA requires Covered Entities to only use and disclose PHI for certain permitted purposes, which include (among other purposes) the use of such data for the patient's treatment, processing of payments and the organisation's healthcare operations purposes. Thus, the use of such data for the training of generative AI models would need to be justified under such permitted purposes. If a Covered Entity's use of PHI does not fall within a permitted purpose, the Covered Entity would need the patients' consent to use or disclose their identifiable data.
- As obtaining consent from each and every patient may be impractical considering the size of datasets typically used in generative AI models, parties may consider deidentifying the data in order to avoid falling under the purview of the HIPAA rules. However, parties should be aware of state privacy laws that have even more stringent data use requirements than HIPAA.
- Even after a generative AI is trained, a party using trained generative AI to provision a digital health solution to a user should be aware of any input received form the user. The input may itself be considered a PHI under HIPAA or other data worthy of privacy protection under more stringent state laws.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

The FDA plays a primary role in regulating SaMD, which includes healthcare products that are AI/ML-enabled, as the FDA's purpose is to protect the public health by ensuring the safety, efficacy and security of drugs, biological products and medical devices.

The HHS OCR also enforces regulations related to healthcare data use and collection.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

For the FDA, issued guidance/discussion through, for example, the SaMD proposed regulatory framework (2019 paper), the SaMD action plan (2021 paper) and the marketing submission recommendations for PCCP for SaMD (2023 paper) all highlight an aggressive commitment to developing a regulatory framework around AI/ML-enabled medical devices (including software).

The OCR enforces HIPAA in order to protect against improper use and collection of patient healthcare data.

Details on HIPAA and FDA Guidance related to AL/ML-enabled SaMD are discussed at length above.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Current U.S. law requires that patents and copyrights can only be owned by human inventors and authors, respectively.

For patents, 35 U.S.C. §100, the Manual of Patent Examining Procedure and recent Federal Circuit cases (*Beech Aircraft Corp. v. EDO Corp.*, 990 F.3d 1237, 1248 (Fed. Cir. 1993); and *Univ. of Utah v. Max-Planck-Gessellschaft zur Forderung der Wissenschaften e.V.*, 743 F.3d 1315 (Fed. Cir. 2013)) have held that only natural persons can be inventors for patents.

For copyrights, §306 of the Compendium of U.S. Copyright Office Practice states that "(t)he U.S. Copyright Office will register an original work of authorship, provided that the work was created by a human being".

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

A variety of considerations must be addressed when licensing data for use in ML for digital health solutions, including, for example:

- Data Set Definition:
  - The contents of the data (e.g., genomic, proteomic, EHRs, etc.) being shared.
  - The type of data (e.g., PHI, deidentified, anonymised, etc.) that is being shared.
  - The file format of the data being shared.
- Data Use Case:
  - Data used to train ML algorithm of digital health solution.
  - Geographic location(s) for data use.
  - Fields (e.g., oncology, ophthalmology, etc.) that the data can be used in.
- Data Rights:
  - Ownership of the data and subsequent data generated from the data.
  - Amount of time that the data can be used for.
  - Sub-licensing rights.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Standard AI (e.g., traditional or predictive AI) uses structured data and predefined algorithms to analyse information and make predictions. Examples of digital health technologies and products using standard AI include ML models for disease prediction or anomaly detection in medical images. Generative AI uses deep learning models (e.g., large language models) to generate new content, such as new text, new images or synthetic data. Examples of generative AI applications in digital health include the use of generative AI to draft patient notes, engage patients in telemedicine (e.g., via chat bots), generate explanations of medical conditions, and generate potential molecular structures for new treatments.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

The first major issue is accuracy and reliability. Generative AI can potentially create false or misleading medical information (e.g., via hallucinations), which is particularly concerning for healthcare. A second issue is the reliability of data used to train the generative AI model. If the generative AI relies on biased or incomplete data, the resulting digital health products may potentially reinforce health disparities. Related to both the first and second issue is the lack of clarity on who would be responsible if a digital health technology employing the generative AI is found to be defective (e.g., the technology leads to an unfavourable medical outcome). Would liability fall on the AI developer, the healthcare provider using the technology, or an institution employing the healthcare provider? A third issue relates to the risk of compromising sensitive or proprietary information in the process of the digital health product generating new content via its generative AI model. For example, it is likely that digital health technologies applying generative AI models are trained on the PHI of patients, and must therefore be compliant with relevant privacy laws (e.g., HIPAA, GDPR, etc.). However, there is a risk that the new content generated by the AI model may inadvertently reveal sensitive information about the patient. Similarly, there is a risk that the new content may be too similar to a copyrighted or other IP-protected work based on the training data including such work. The use of the new content may result in IP infringement.

Various legal considerations may help mitigate the aforementioned issues. For example, it may be useful to rely on de-identified, encrypted and/or synthetic data instead of PHI to train AI models, in order to reduce privacy risks. To the extent PHI is used, it is important to obtain patient consent in accordance with HIPAA, the HITECH Act and state privacy laws. To the extent the dataset includes any proprietary or IP-protected data, it is crucial to obtain the necessary licences to use the dataset. Additionally, it may be useful to train generative AI models on datasets that are diverse and representative to reduce bias and create a more effective product. Furthermore, human oversight in AI-generated medical recommendations may be critical in preventing harm to a user, averting hallucinations, reducing tort and other legal risks, and gaining the public's trust and acceptance of the generative AI-enabled digital health product.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

The FTC is starting to employ a penalty referred to as algorithm disgorgement to punish companies who use improperly sourced data in algorithm development and training. This penalty requires companies to delete or destroy algorithms and models that were developed using illegally obtained data. This essentially means that the company must remove any products built on data it should not have used, effectively taking away the benefits gained from improper data collection practices.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Theories of liability include: contract breach (e.g., data agreements, data transaction, consent agreements); violation of U.S. federal, U.S. state, and ex-U.S. laws related to the protection of PHI and personal data generally; negligence (e.g., by the product provider, the health provider, or the payer); product liability and Consumer Protection Law in the U.S. and abroad; Corporate Practice of Medicine; and Anti-Kickback laws (even with recent legislation increasing safe harbour).

9.2 What cross-border considerations are there?

Please see question 9.1 above as many of these liability categories are analogues in ex-U.S. territories. Jurisdictional issues may arise due to the digital nature of the industry, but other more established liability categories (e.g., tort laws) will generally be applicable in various countries for which business is conducted.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

As previously discussed, data used in the training and development of generative AI for digital health solutions may include PHI and other sensitive data protected under various state privacy laws. When obtaining authorisation from the respective patients or individuals is impractical or impossible, it is advisable to deidentify such data to the extent possible, or otherwise make sure that the use of such data in generative AI model training complies under various privacy laws (e.g., HIPAA, state privacy laws, etc.). For example, HIPAA requires that PHI can only be used for various permitted purposes. Such data should also be handled with extreme care, for example, by strengthening cybersecurity and implementing measures to prevent reidentification.

Companies should safeguard against the overreliance of data output from generative AI models. For example, to protect users from and minimise liability risks associated with false data (i.e., hallucinations), companies should provide disclaimers that the generative AI models are merely recommendations and the recommendations may change based on the dataset in which the models are being trained.

Furthermore, if a company relies on another partner for the use or implementation of a generative AI tool, the company should ensure that there are privacy policies and data security procedures in place to clarify data ownership and specify how the partner is to use the generative AI tool.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

The FTC can utilise algorithm disgorgement, discussed above. The HHS OCR can require corrective action plans under HIPAA, where Covered Entities would be required to adopt plans to address compliance deficiencies. There are also civil monetary penalties under HIPAA, with a wide range of money damages per violation. In fact, state attorneys can bring civil actions themselves. Under HIPAA, there can be criminal violations, and corresponding criminal penalties, carried out by the Department of Justice. These penalties can include both fines and imprisonment.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

As discussed herein and above, digital health (regardless of whether it is cloud-based), bring several potential legal issues related to, for example, data use, data rights, data security/cybersecurity (e.g., hacking, loss, breaches), data loss and PHI. These issues can arise in the U.S., in several U.S. states, and internationally as well. Cloud use can also bring forth issues depending on data location, which can be in various places around the world depending on entity location, customer location, and so on.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

As discussed above, digital health is a convergence of typically disparate industries: tech; and healthcare. Each industry encounters unique issues. The extremely highly regulated and appropriately risk-averse nature of healthcare can lead non-healthcare companies to have strategic (often legal) "blind spots" based on their experience leading up to the digital health endeavour. For example, non-healthcare companies, unlike healthcare companies, have not typically had to contemplate various legal issues. These can include, for example, FDA, HIPAA/HITECH Act, state health data laws, international health data laws, reimbursement, corporate practice of medicine and anti-kickback considerations.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

As a continuation of question 10.2, not only are there various legal and strategic issues commensurate with converging two typically disparate industries, each having their own unique issues, these issues and their corresponding strategy should be sophisticatedly addressed and dealt with concurrently by a digital health venture. These issues include, primarily, IP, FDA/regulatory, data use/privacy/security (including HIPAA), reimbursement and healthcare transactions. These issues are interrelated and unless a cohesive strategy, from the off, addresses a plan for each of these issues, a potential investment target may have a "blind spot" that can significantly delay launch, diminish revenue, or slow or reduce adoption. It must be noted that each of these issues cannot always be "handled" by early-stage companies immediately at once. Rather, these issues should be considered, and a strategy developed that will be tested, executed and regularly reassessed so that each issue can be moved forward to resolution concurrently with the other issues.

Moreover, given the converging nature of digital health, investors should not assume that founders are broadly educated on all these subjects. Early diligence as to strategy is essential as there are not many serial digital health entrepreneurs given the youth of the digital health industry. This can rear its head, not only with understanding how to address the issues above, but also how to transact with partner entities (e.g., health systems and large pharmaceutical companies of typically greater experience and leverage), which can saddle new ventures with contract terms that affect future growth potential.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

There are two spectrums to the hurdles affecting widespread clinical adoption. On the one hand, the industry of digital health is young from an adoption standpoint. Many patients, particularly the elderly, have extensive experience and likely comfort with in-person treatment. Moreover, the parties involved in deciding on a digital health solution are very likely new to the industry as well, making robust diligence difficult to achieve on potential digital health solutions. On the other hand, due in part to COVID-19, digital health entrants have increased dramatically in the last few years. As a result, digital health consumers, already ramping up their knowledge in this space, now have to deal with a wealth of options. Which to choose? How do I navigate all these potential solutions?

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

With the dramatic increase in digital health solutions entering the market, and the aforementioned diligence shortfalls that can accompany customers, formal endorsements are one way of differentiating your solution from your competitors. Add to that the difficult financial situation in the U.S., one that may continue for a substantial period of time, and customers will be even more circumspect in analysing solutions, and may look for any designation that can mitigate the risk of purchasing a subpar solution.

Key digital health-related certification bodies in the U.S. include: the American College of Radiology; the American Board of Medical Specialties; the American Medical Association; and the American Board of Professional Psychology.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

From a U.S. industry standpoint, payors continue to observe inconsistency in regard to the reimbursement of digital health-related therapies and treatments. Further, from a government payor programme perspective, government review of proposed regulations continues in an effort to ascertain how best to determine whether a particular digital health-related device is clinically beneficial to or reasonable and necessary for a government healthcare programme beneficiary. The result is healthcare providers seeking reimbursement for digital health-based care must utilise the coverage, coding and billing requirements of the respective payor programmes (whether government or private based) that are currently available and that vary by payor programme. Providers seeking reimbursement must also comply with the respective enrolment, registration and licensing requirements of such payors as they would with any healthcare treatment reimbursement submission.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Innovations in digital health often involve the use of multiple entities. For example, personalised medicine may involve the use of organisations that collect data to be used for the training of AI/ML models, computing systems performing the development and training of the AI/ML models, computing systems deploying and utilising the trained AI/ML models to discover insights for drug development, and labs developing the drugs. The presence of multiple entities, even for a single innovation, raises unique challenges for enforcing or protecting against legal claims, whether it is data privacy violation, IP infringement or product liability. For example: patent claims may need to be prepared with an eye toward the different entities practising various aspects of the innovation; data maps would need to be developed for each entity, to uncover the myriad areas in which breaches could occur; and product liability would need to be investigated through each entity's vantage point.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

This is not applicable.



Roger Kuan is a Partner at Norton Rose Fulbright and US head of the Digital Health and Precision Medicine Practice, where he counsels companies that are uniquely positioned in the convergence of the life/medical sciences and technology industries on how to successfully navigate the complexities of the IP, data rights and regulatory challenges they encounter.

Roger has extensive experience in IP strategy and portfolio management (utility/design patents, trademarks, copyrights, and trade dress), data rights strategy, licensing and technology transactions, freedom-to-operate clearances, enforcement, monetisation, IP due diligence, and dispute resolution. His practice is focused in the life sciences sector (e.g., research tools, analytical instrumentation/software, digital therapeutics, medical devices, diagnostics, biomanufacturing equipment, etc.) with an emphasis in emerging technologies such as precision medicine (e.g., genomic sequencing platforms, AI/ML, computational genomics/bioinformatics, molecular diagnostics, companion diagnostics, etc.), digital health (e.g., mobile apps, clinical decision support, software, AI/ML imaging diagnostics, wearables, etc.) and 3D printing/bioprinting.

Norton Rose Fulbright
1 Embarcadero Center, Suite 1050
San Francisco, California 94111-3698
USA

Tel: +1 628 231 6810
Email: roger.kuan@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/roger-kuan-1b5b824



Jason Novak advises companies of all sizes on legal issues arising from emerging technologies, with a particular emphasis on AI/ML. His practice centres on "convergence" technologies – such as digital health, precision medicine, and alternative protein – that sit at the intersection of multiple industries. Drawing on cross-disciplinary training and deep in-house experience, Jason helps organisations navigate the complex legal and strategic challenges that come with blending traditionally distinct sectors.

Jason's work focuses on IP and data rights strategy, which are of particular importance and complexity in "convergence" fields. With data rights, data must be treated as an offensive asset. To that, Jason supports clients on transactions, protection, and strategic long-term planning. Jason's IP experience includes patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in- and out-licensing, freedom-to-operate, due diligence, IP training, risk management, and dispute resolution.

Before moving into this practice, Jason served as IP Director at Thermo Fisher Scientific, overseeing global IP strategy for genetic sciences instrumentation and software, including qPCR, dPCR, and capillary electrophoresis. He managed extensive patent portfolios, led teams of attorneys and agents, directed licensing programmes, supported diligence efforts, and handled both domestic and international patent challenges.

Earlier in his career, Jason worked as a research engineer at Kraft Foods, leading product and process redesigns, reformulations, and launches. This role required close collaboration with operations, finance, marketing, and regulatory teams, giving him a practical understanding of how R&D and legal functions intersect within complex organisations.

Norton Rose Fulbright
1 Embarcadero Center, Suite 1050
San Francisco, California 94111-3698
USA

Tel: +1 628 231 6811
Email: jason.novak@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/jason-novak-002102b



Apurv Gaurav is a USPTO-registered lawyer and a senior counsel in the IP Transactions and Patent Prosecution group at Norton Rose Fulbright. Apurv is passionate about helping his clients form, protect, enforce and utilise patents and other IP assets in a manner that advances his clients' long-term business strategy. Leveraging his technical background in electrical engineering and molecular and cell biology, and his advanced coursework and certification in machine learning, Apurv has worked on various legal matters spanning a wide spectrum of technologies, but is uniquely well-positioned to advise in digital health, precision medicine and other areas at the convergence of software and life sciences.

Norton Rose Fulbright
1045 W. Fulton Market, Suite 1200
Chicago, Illinois, 60607
USA

Tel: +1 312 964 7775
Email: apurv.gaurav@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/apurv-gaurav-39611454

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full-business law service. We have more than 3,500 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

Recognised for our industry focus, we are strong across all the key industry sectors: financial institutions; energy, infrastructure and resources; transport; technology; life sciences and healthcare; and consumer markets. Through our global risk-advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

NORTON ROSE FULBRIGHT

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including Houston, New York, London, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

nortonrosefulbright.com

The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.

Norton Rose Fulbright © 2026. All Rights Reserved
69338-US- 01/26