NORTON ROSE FULBRIGHT

International Comparative Legal Guides

Practical cross-border insights into digital health law

Digital Health 2023

Fourth Edition

Contributing Editor

Roger Kuan

US Head of Digital Health and Precision Medicine Practice

Norton Rose Fulbright

ICLG.com

COMPARE & RESEARCH THE LAW, WORLDWIDE.

NORTON ROSE FULBRIGHT

As digital health and precision medicine continue to integrate into the healthcare industry around the world, companies face new challenges and opportunities in multiple jurisdictions.

Our digital health and precision medicine lawyers are part of the global life sciences and healthcare team, providing a full range of legal advice to innovative pharmaceutical, biotechnology and health insurance companies, technology startups and industry investors. We advise our clients on a broad range of legal, regulatory and commercial issues, drawing on our extensive multidisciplinary experience in intellectual property, data rights, technology and commercial transactions and life sciences, healthcare and pharmaceuticals litigation.

Our global presence allows us to closely track international market and industry trends and cutting-edge technology developments so we may provide clients with proactive risk management and strategic counsel in the rapidly evolving landscape of precision medicine and digital health.

Law around the world

nortonrosefulbright.com

ISBN 978-1-83918-252-5
ISSN 2633-7533

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Deputy Editor
Maya Tyrrell

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Health 2023

Fourth Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

Digital Edition Chapter

From the Publisher

Dear Reader,

Welcome to the fourth 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, five expert analysis chapters cover investing in digital health, the global landscape of digital health in the United States, Europe and China, data protection and data-driven digital health innovation, emerging trends in the global regulation of digital health and hospital innovation pathways in the USA, UK, Germany and France.

The question and answer chapters, which in this edition cover 21 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.

James Strode
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 five years (even prior to the COVID-19 pandemic) has transformed how healthcare is delivered to the masses. The promise of digital technologies continues to transform the healthcare delivery model from a traditional model based on a "one size fits all" practice of medicine that was characterised by a provider-centric approach with information silos, to a new model that is focused on patient-centric treatment personalisation with high data accessibility and utilisation. The result is a highly personalised healthcare system that is focused on data-driven healthcare solutions and individualised delivery of therapeutics and treatments to patients using information technologies (IT) that enable seamless integration and communication between patients, providers, payors, researchers and health information depositories. 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

There are five primary constituents that make up the Digital Health Ecosystem.

Life Sciences Companies – are the companies that develop and make products such as therapeutics, diagnostics, medical devices and the like that are used to help treat a patient's health or wellness condition.

Pharmacies – are the supply chain, people and companies that sell the products that life sciences companies develop to end users such as patients and providers.

Providers – are the doctors, clinics, hospitals and healthcare systems that provide healthcare services to patients by leveraging off the products produced by the life sciences companies.

Payors – are the group of entities (e.g., private insurance companies, government sponsored insurance programs, national healthcare systems, etc.) that pay for the products and healthcare services provided to patients.

Patients – are the people who all the collective entities (Life Sciences Companies, Pharmacies, Payors and Providers) try to serve as part of the Digital Health Ecosystem.

The Digital Health Ecosystem constituents sometimes struggle to transact in a seamless manner with each other; and Digital Health Solutions provide the key to building effective channels and improving efficiencies between them.

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, many of those technical hurdles have been overcome. 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 artificial intelligence (AI) (more specifically machine learning (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 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, digital therapeutics, 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. 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.

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/she 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.

Electronic Health Record (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

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 programs, including: 510(k) certification; Premarket Approval (PMA); Software as a Medical Device (SaMD); Digital Health Software Pre-certification Program (Pre-Cert Program); and 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 and thus poses particular challenges for the FDA as the current regulatory regime is based on software being static by design. The FDA recently launched a Digital Health Center of Excellence 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 practice 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; Wyoming; and 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

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 be even 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
URL: www.nortonrosefulbright.com

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
URL: www.jnj.com

Investing in Digital Health


Thomas Kluz


Jason Novak


Rachel Wilson

Norton Rose Fulbright
Venture Lab NGK SPARK PLUG

1 Introduction

Although the digital health market did not escape the 2022 venture-investing downturn, there is light ahead. As the sun emerges, digital health companies with strong value propositions and strategic milestone choices should be able to ride post-pandemic tailwinds through the incipient recession. Simultaneously, investors and investees must pay special attention to legal issues put front and center by the digital evolution of healthcare.

2 Digital Health Investing

The market for digital health investing has seen dramatic changes in the last three years. Here we examine the impacts of the coronavirus pandemic, headliner fund losses and recession.

2.1 COVID's impact on digital health

COVID not only drove the digital health explosion, but also acted as a timely accelerator for the opportunities created by converging technology with healthcare. Consider virtual care growth: telehealth utilization saw an explosion from 0.1% to 70% utilization and eventually plateaued to 40%. Not only did the pandemic teach consumers how to think about their healthcare needs in an accelerated manner, it also taught health systems providers, insurance companies, and digital health vendors how to calibrate a healthy balance between virtual care and brick-and-mortar care.

COVID pushed providers to think outside the box and test the limits of virtual care – now remote patient care offerings are succeeding in this tailwind. Moving forward, remote monitoring gives providers an economically sustainable way to keep up with their patients and effectively triage patient populations.

2.2 Digital health investing in a recession

Much like how COVID was an accelerant towards certain healthcare drivers, economic recession accelerates the failure of unsustainable business models. A recession acts like a filter on the digital health market, as with most markets; companies that do not have a sustainable business model often cannot raise money and naturally sunset. Without a completely dialed-in value proposition, a recession can undermine a company. In comparison, companies with clear value propositions and customer targets can weather the storm. As such, investors will likely focus on portfolio management and supporting thoughtfully structured portfolio companies.

In order to overcome this filter, digital health companies may have to run an obstacle course of interrelated hoops – all while juggling value propositions, differentiation, price points, and exclusivity. Differentiation based on a clear value statement within the competitive landscape and an aligned pricing model may improve the odds. Strong intellectual property road maps built prior to a recession further insulate against inflexible times. (See Section 3.2 for further explanation.) Depending on the sector and price point, exclusive licensing can be a valuable tool.

Consider a biotech startup evaluating an exclusive license. Licensing to Distributor X may make a positive market assertion and take a faster route to market, but in exchange the startup is beholden to Distributor X as its sole licensee. The startup's pricing power will diminish over time and must be balanced against the quantity of the upcoming sale cycle in order to make the license worthwhile.

In 2023, as panic due to the pandemic and Softbank losses fade into the rearview mirror, the M&A market should be vibrant. Benchmarks are shifting during the recession; institutional investors are slowing deployment of capital, focusing on portfolio company management and seeking liquidity. Gone are the days of trading on two-to-three years of projected revenue – now, investors are trading on the last 12 months and perhaps the next 12 months. While some markets are holding steady, like the home care ecosystem, commodity assets are trading at 20–30% decline in valuation. Sky-high valuations common during the pandemic have dipped, and will continue to dip in non-core areas.

As the recession interrupts funds' four-to-six year funding cycles, expect existing and new funds to react differently. Well-established funds with strong reputations and an existing LP (limited partner) base will likely focus on their existing portfolio and deploy capital on their current cycle – with perhaps slight pullback on commitment or fund size. These funds will not have as much trouble raising the next fund thanks to their existing LP base. In comparison, first- or second-time funds are struggling to raise capital in this risk-averse environment. These funds are less likely to incept and will push out fundraising. In both circumstances, sales cycles are longer and capital needs of portfolio companies are higher, so the capital is being pushed

out one way or another. Willingness to invest in any company by any fund – whether first, second, or sixth – is tough, but an opportunistic play nonetheless.

To adjust to these circumstances and continue to raise funds, choose milestones strategically: target assets that are meaningful to investors *and* achievable for the company. In the digital health space, percentage of investment is not proportional to percentage of success – perhaps a $20 million round allows a startup to reach a milestone while a $10 million round would only get 10% of the way there. Focus on clear differentiators, for once the storm clears, rebounds will occur. Weathering the fundraising storm and inception of a fund in a down cycle produces an excellent vintage in a buyer's market.

Consider a startup that filed only seven patent applications in the last four years but now has 12 issued patents in this year alone. The startup has produced better results by budgeting for fewer, high-quality applications than it would have produced by filing more, low-quality applications. Now, the startup's investors see more value from the 12 issuances than they would have seen from excessive but unsuccessful applications.

3 Legal Considerations for Digital Health

Given the funding situations in the current economic climate, using a solid legal strategy to exploit a company's differentiators is a must, now more than ever. To this point, the legal considerations for digital health companies and investors include key data-rights strategies and IP strategies.

3.1 Due diligence in digital health

Digital health companies considering due diligence should prioritize data-rights strategy and IP strategy. We also consider open-source data within this context.

1. Data-rights strategy: Digital health companies must map their data from cradle to grave; from where it originates, through upstream handling by other entities, and to downstream deployment, a company must know the consents attached to the data at each stage. The company must also secure the necessary data rights to use and deploy the data as it sees fit. If any of the data lines are broken by bad data rights agreements or lack of (or proper) consent agreements, the AL/ML model trained by the data will be in peril.
   Consider a startup spun out of a university research institute. Initially, the researchers identify new biomarkers for a disease state by pulling data from Clinic X to train an AI model. This AI model then becomes a diagnostic tool used by the spun-out startup. However, if the data privileges from Clinic X were only for non-commercial use (e.g., research use only), the startup's diagnostic is non-commercializable.
2. IP strategy: Often, IP strategy flows from data strategy, since patents and trade secrets are regularly developed off the backs of the data and corresponding analytics. However, IP strategy centered on proper timing stands alone when a tool is not data-based. In developing a product towards a commercial purpose, IP will or will not emerge; filing patents for the sake of investors alone can harm company credibility. Instead, demonstrating a strong IP strategy centered on an 18–24 month road map of data and IP protection can build investor confidence. IP strategy timed on product development aligns investors with the company's underlying motivations. This includes Freedom to Operate (FTO) analyses, which often should not be properly conducted until the product is substantially developed. Investors often pressure companies for FTOs, but early analyses on uncompleted products do not adequately protect the final product and incur additional costs for additional analyses later on.

3.2 Patent strategy in a recession

Digital health companies can balance their IP needs with a controlled budget by properly prioritizing their filings, thinking strategically about patent cost, and choosing wisely how to balance patent and trade secret protection.

In prioritizing patent filings, consider product, competitors, and ingenuity. First, allocate budget to creating a strong bubble around the product before it reaches the market. Second, consider filings which extend past the core innovation to ancillary solutions that can be easily adopted by competitors. Third, file on creative, ingenious inventions that are not necessarily attributed to a product or known competitor.

In considering patent cost, be strategic about the cost difference between preparing a patent application and prosecuting an application. One application can be prosecuted in multiple major territories including the US, Europe, China, and Japan. Control costs by first generating a high-quality application and then thoughtfully selecting territories in which to prosecute.

In protecting a product, choose wisely between patents and trade secrets – the two coexist in digital health tools. If a feature, solution, or product is patent eligible, reverse engineerable, and disclosed in some form or fashion, it should be patented. However, if the information is innovative but not any of the above three, keeping that feature, solution, or product as a trade secret is worth considering. Trade secrets exist by virtue of remaining secret – so if the inventive information can be known to a competitor via public disclosure, press release, user manuals, websites, or independent discovery, it may be better protected as a patent. The digital health industry faces the unique issue of required disclosures with regards to both adoption and FDA approval, both of which drive disclosure of a tool's underlying workflows and why the tool actually works. As such, between adoption dynamics and FDA approval processes, digital health companies need to balance both trade secret and patent protection in their IP strategy.

4 Conclusion

Thoughtful and vigilant business, data and IP strategies will help digital health companies exit the receding pandemic and weather the emerging recession. Advisors and startups should focus on strong value propositions, strategic milestones, clear data-rights paths, and aligned IP priorities to de-risk potential collaborations.

Thomas Kluz serves as Managing Partner at NGK NTK Ventures where he leads investments or sits on the boards of companies such as AliveCor, DispatchHealth, Neoplas and NOTA Laboratories. Prior to NGK, he served as General Partner at dRx Capital, a joint venture fund between Qualcomm Ventures and Novartis, where he led investments or sat on the boards of companies such as AliveCor, Aktana, Doctor on Demand, Noom, Omada and Welltok. As part of his role at dRx, Thomas also served as the Global Head of Healthcare Investing at Qualcomm Ventures and the Qualcomm Life Fund.
Thomas started his venture capital career as an investment professional at Providence Ventures, one of the leading digital health and medtech corporate venture capital funds, and Adams Street Partners, a $52B growth equity and venture capital fund manager.

Venture Lab NGK SPARK PLUG
3979 Freedom Circle #401
Santa Clara, California 95054
USA

Tel: +1 847 452 9694
Email: tskluz@ngksparkplugs.com
URL: www.ngkntkventure.com

Jason Novak's practice was specifically created to focus on advising entities, both large and small, on the various legal issues that can arise with emerging technologies in the healthcare, food and life sciences industries, with a particular and targeted focus on "convergence" technologies (e.g., digital health, personalised/precision medicine, alternative protein) that operate at the intersection of multiple industries. Jason has extensive experience in IP and data rights strategy. For data rights, Jason advises clients on transactions, protection and general strategy. On the IP front, Jason's experience extends to patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in- and out-licensing, freedom-to-operate, various types of due diligence, IP training, risk recognition and management and dispute resolution.

Norton Rose Fulbright
555 California Street, Suite 3300
San Francisco, California 94104-1609
USA

Tel: +1 628 231 6811
Email: jason.novak@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

Rachel Wilson's practice with Norton Rose Fulbright focuses on patent prosecution and technology transactions. She has an undergraduate degree in chemical engineering and three years of research experience in immuno-oncology process development. As a research scientist, her projects involved CAR T-cells, electroporation, non-viral gene delivery platforms, multiplexed patient products, mRNA production, and physiologically relevant cell growth environments. Her legal experience includes freedom-to-operate analyses, landscape analyses, industry-to-industry licensing, university-to-industry licensing, subsidiary management, and joint venture contracts.

Norton Rose Fulbright
555 California Street, Suite 3300
San Francisco, California 94104-1609
USA

Tel: +1 628 231 6826
Email: rachel.wilson@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

Norton Rose Fulbright is a global law firm. We provide the world's pre-eminent 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

The Venture Lab was established in April 2018 as an open innovation and collaboration team to partner with and invest in the brightest creative and entrepreneurial minds around the world.
Through internal innovation projects and startup partnerships, our global team of more than 300, backed by a $100M fund, is transforming the industries of mobility, food, energy, clean air, wound care, women's health, and home health to build a better future for all of us.

www.ngkntkventure.com

The Global Landscape of Digital Health: A Comparative Regulatory Analysis of Real-World Evidence, Health Data, and Artificial Intelligence/ Machine Learning in the United States, Europe, and China


Lincoln Tsang


Kellie Combs


Katherine Wang

Ropes & Gray LLP

Introduction

The landscape of digital health has changed dramatically in recent years, accelerated by the COVID-19 pandemic, which necessitated an increased reliance on technological tools to manage complex and multifaceted healthcare systems. Digital transformations and other related analytical tools are increasingly being applied to render basic and translational research more efficient by simplifying data collection, analysis, storage, and data mining throughout the product lifespan.

Digital health is the field of knowledge and practice associated with the development and use of enabling digital technologies to improve health. The field encompasses the concept of eHealth for managing healthcare delivery and health surveillance, as well as other digital health technologies, such as the internet of things, artificial intelligence ('AI'), big data, and robotics. These technologies will become more important in the way people manage their own health and in the way they receive care. A more detailed discussion of the variable roles of technology in healthcare, as well as a general overview of the regulatory landscape, can be found in the book chapter titled *Global Landscape of Digital Health: Impact on Healthcare Delivery and Corresponding Regulatory and Legal Considerations* (2021).[1]

The digital health market was valued at over US$200 billion in 2022, and it is projected to expand at a compound annual growth rate of 18% from 2023 to 2030. Strains on healthcare delivery are becoming more pertinent as we enter a global recession, fuelled by inflationary pressures and geopolitical uncertainty. Moreover, all countries face major challenges to prepare their health and social systems for demographic shifts stemming from rising life expectancy. An aging population is correlated with certain complex health states, which can be medically challenging. Digital tools can help assess the impact of higher chronic disease prevalence, design systems that will improve the quality of patient care, and evaluate the effectiveness of specific medical interventions.

This chapter describes the evolving regulatory landscape in three major developing areas – real-world evidence ('RWE'), health data, and AI/machine learning ('ML') – across the key jurisdictions of the United States, Europe, and China.

RWE

RWE is playing an increasingly important role throughout the medical product life cycle. RWE can serve as mutually complementary evidence to those evidence generated from prospectively designed, randomised-controlled studies ('RCTs') to inform an evaluation of the safety and clinical effectiveness or clinical performance of a new drug or new medical technology. RWE can help determine the therapeutic value of a medical intervention for the purpose of supporting coverage and reimbursement determinations. RWE can also support post-market surveillance activities, optimising the safe and effective conditions of use of an approved product or technology.

Regulatory authorities, including payers and health technology authorities, recognise RWE as a complementary data source to support the development, approval, and surveillance of new innovative products. Its place in safety monitoring and disease epidemiology is well established. The wider application of RWE is gaining some traction, notably for demonstrating safety and effectiveness of prophylactic vaccines, such as those approved for use in primary immunisation programmes. However, the quality and reliability of the data sources are critical elements in determining whether the data can safely inform regulatory decision-making.

In contrast with RCTs, which are conducted on highly selective populations, RWE is collected from diversified data sources that are outside the scope of RCTs and cannot be obtained through a clinical-trial setting. RWE comprises real-world data ('RWD'), which may be compiled from electronic health records ('eHRs'), medical-claims databases, patient registries, patient-reported outcomes, prescription-claims data, wearable-device data, and companion apps, among other sources. Digital health tools are critical to the generation and collection of RWD. However, the quality of RWD varies considerably, and whether and how it may be useful for various purposes, such as use in a regulatory submission, will depend on numerous factors, including transparency around data sources, the manner in which data are analysed, and the data's fitness for purpose. For example, RWD may be used in eHealth applications to help discover digital health biomarkers to evaluate the effects of an intervention on certain physiological functions, e.g., heart rate; digital interventions using connected devices may be developed using RWD; and digital health technologies can help conduct clinical trials by collecting data, recruiting participants, managing data, and reducing costs. Fundamentally, RWD and RWE should not be viewed as a replacement for data generated from traditional clinical trials, though greater availability of RWD, increasing

comfort by regulators, and legislative and policy changes in key jurisdictions will undoubtedly contribute to more widespread acceptance of RWD and RWE in the near future.

United States

The Food and Drug Administration ('FDA') approves new drugs and medical devices according to varying evidentiary standards. For drugs, a sponsor must show substantial evidence of effectiveness, defined as 'evidence consisting of adequate and well-controlled investigations, including clinical investigations, evaluating the effectiveness of the drug'.[2] While drug applications must be supported with adequate and well-controlled studies, the evidentiary standard for approval or clearance of medical devices is significantly more flexible. Devices to be approved via a premarket application must demonstrate valid scientific evidence, defined as 'evidence from well-controlled investigations, partially controlled studies, studies and objective trials without matched controls, well-documented case histories conducted by qualified experts, and reports of significant human experience with a marketed devices, from which it can fairly and responsibility be concluded by qualified experts that there is reasonable assurance of the safety and effectiveness',[3] while those to be cleared via the 510(k) process must show substantial equivalence to a predicate device, which *may* require clinical data.

FDA has made clear that RWE may constitute an adequate and well-controlled study, and therefore form the basis for approval of a new drug or biologic product or indication, in certain circumstances. Reliance on RWE is most common in the rare disease context, although it is still fairly limited for drugs and biologics on the whole. RWE has been used to support FDA decision-making for drugs and biologics in a variety of ways, including safety signal evaluation, incorporation of RWD within the context of an RCT, use of synthetic control arms, and use of observational study data as evidence of efficacy for a new indication. The RWE used to support FDA's decision-making has come from a variety of RWD sources, including eHRs, registries, and medical-claims databases. Reliance on RWE to support product approval or clearance is significantly more prevalent for medical devices than for drugs and biologics. This disparity can, in large part, be attributed to the more flexible evidentiary standards applicable to medical device approval or clearance, although the increasing prominence of 'connected devices' from which RWD can be obtained is also an important factor. Such approved and cleared devices have been diverse in their usage of RWE, including RWE as the primary source of clinical evidence; prospective randomised trials nested within RWD sources; control arms and objective performance goals for evaluating the next generation of devices; and diverse RWD sources that may be combined to generate RWE.

In recent years, FDA has issued extensive guidance regarding the use of RWE to support regulatory submissions, driven by legislative requirements as well as increasing availability and use of RWD. The FDA guidance issued so far describes important high-level principles that sponsors should keep in mind when planning to utilise RWE in a regulatory submission, but does not provide much detail on what specific study designs, data sources or analytical methods may or may not be considered sufficient by the agency to meet evidentiary requirements. FDA has repeatedly underscored that sponsors should engage early and often with the agency during the product development process, because whether RWE will be sufficient to meet evidentiary standards largely remains a case-by-case assessment.

The guidance that has been released so far explains that, broadly speaking, FDA evaluates the use of RWE in marketing applications by considering: (i) whether RWD are fit for use; (ii) whether the trial or study design used to generate RWE can provide adequate scientific evidence or help answer the regulatory question; and (iii) whether the study conduct meets FDA regulatory requirements (e.g., for study monitoring and data collection). For both drugs and devices, RWD must be both relevant and reliable to support regulatory decision-making. Relevance pertains to whether the data capture relevant information about exposure, outcomes, and covariates, while reliability includes data accrual and data quality control. For study sponsors, this emphasis on relevance and reliability means that they must: thoroughly document and justify data source selection; finalise the study protocol and statistical analysis plan prior to reviewing outcome data and performing analyses; include an audit trail in datasets to monitor access to the data; consider approaches to ensure that necessary data can be obtained from the data source(s) selected, such as using data linkages, distributed data networks, and AI tools for handling unstructured data fields; and ensure patient-level data access can be provided to FDA as needed and that source data can be available for inspection. While use of RWD and RWE may provide more flexible approaches to product development, the bottom line is that sponsors should not expect RWD and RWE to provide a shortcut to product approval or clearance. Sponsors should work to: stay abreast of FDA guidance and approval precedent developments; design studies with the necessary rigour to meet applicable FDA evidentiary standards; select data sources with an eye to ensuring relevance and reliability; conduct diligence to ensure RWD sources have appropriate rights to data and have structured/curated data in accordance with study needs; and ensure that appropriate data arrangements and privacy controls are in place.

More guidance on RWD and RWE is expected throughout 2023, as well as a public workshop to discuss RWE case studies. The FDA is also commencing a programme, known as the Advancing RWE Pilot Program, that seeks to improve the quality and acceptability of RWE-based approaches to support a change in labelling for effectiveness or to meet post-approval study requirements; among other things, the pilot will provide dedicated, product-specific RWE guidance to sponsors who qualify for the programme and will facilitate public information-sharing regarding successful RWE approaches. Continued policy development is also expected for medical devices.

In addition to the regulatory standards and evaluations applicable to RWD and RWE, there are also a plethora of privacy issues that arise in this context (in any jurisdiction, not just the United States). Though we will not cover those in detail here, any sponsor looking to leverage RWD or RWE in a regulatory submission should be cognisant of the applicable laws and liabilities and ensure that appropriate steps are taken to preserve privacy for those whose data are being used.

While FDA has kept up a swift pace of issuing new guidance concerning RWD/RWE, key questions remain. For example, the specific situations in which FDA will be willing to rely on RWE in regulatory decision-making are not yet clear, and FDA has not clarified what study designs, analytical methods, and data sources will be acceptable in regulatory submissions.

Europe

In the United Kingdom ('UK'), the Medicines and Healthcare products Regulatory Agency ('MHRA') published its guidance in December 2021 on the use of RWD in clinical studies to support regulatory decisions. In January 2022, the National Institute for Health and Care Excellence ('NICE') published a Health Technology Evaluation Manual formalising the acceptability of RWE

as a source of evidence to inform cost-effectiveness assessment. In NICE's view, RWE can improve the understanding of health and social care delivery, patient health and experiences, and the effects of interventions on patient and system outcomes in routine clinical settings. NICE's Strategy 2021 to 2026, which sets out the entity's five-year vision, includes a plan to use RWE to resolve gaps in knowledge and improve patient access to new innovations. NICE published a RWE framework in June 2022 to build on this goal. The framework aims to identify when RWE can be used to reduce uncertainties and improve the health technology assessment, and to describe the best practices for planning, conducting, and reporting RWE to improve its quality. The framework's core principles are to: (i) ensure data is of good provenance, relevant, and of sufficient quality to answer the research question; (ii) generate evidence transparently and with integrity throughout the process; and (iii) use analytical methods that minimise the risk of bias and characterise uncertainty. These principles underpin guidelines on study conduct, assessing data suitability, and methods for real-world studies.

In July 2022, the EMA endorsed the joint statement of the International Coalition of Medicines Regulatory Authorities ('ICMRA') pledging to foster global efforts to further enable the integration of RWE into regulatory decision-making. The global collaboration efforts focus on four specific pillars, namely: (i) harmonisation of terminologies for RWD and RWE; (ii) regulatory convergence on RWD and RWE guidance and best practice; (iii) readiness to address public health challenges and emerging health threats; and (iv) transparency.

The EMA has recognised that patient registries could be rich data sources to collect uniform data over time on a population defined by a particular disease, condition, or exposure. Such registries can play an important role in monitoring the safety of medicines. Since the launch of the initiative for patient registries in 2015, the EMA together with the relevant external stakeholders has explored ways of expanding the use of patient registries by introducing and supporting a systematic and standardised approach to an evaluation of benefit-risk of medicines.

In November 2022, the EMA began the first RWE studies under its Data Analysis and Real-World Interrogation Network 'DARWIN EU' initiative. DARWIN EU will be key to European regulators' vision of enabling the use of RWE and establishing its value for regulatory decision-making on the development, authorisation, and supervision of medicines in Europe by 2025. This EU-wide network will allow the access and analysis of healthcare data from across the EU. The data available to DARWIN EU's first set of data partners – which include both public and private institutions – will be used for studies to generate RWE that will support scientific evaluations and regulatory decision-making. The first three studies will focus on: rare blood cancers; drug use of valproate; and antimicrobial resistance. DARWIN EU aims to have 150 such RWE studies per year by 2025.

China

In China, the National Medical Products Administration ('NMPA') has promulgated several guidelines on the use of RWD and RWE in recent years, including: Guidelines on Using Real World Evidence to Support Drug Development and Review (2020); Technical Guidelines on Using Real World Studies to Support Paediatric Drug Development and Review (2020); Technical Guidelines on the Application of Real World Data in Clinical Evaluation of Medical Devices (2020); Guidelines on Real World Data to Generate RWE (2021); and Guidelines on Communications for Real World Evidence Supporting Drug Registration Application (2023). These guidelines emphasise the quality of RWD and suggest that RWE derived from RWD could support clinical evaluation throughout the life cycle of both drugs and medical devices, including premarket and post-market clinical assessments. Echoing similar guidance from the FDA and EMA, the NMPA guidelines suggest that RWE may increasingly serve as supplementary evidence in medical device clinical evaluation, but it cannot replace the current clinical evaluation pathway. Additionally, a few challenges remain, including limited data accessibility and data sharing, as well as data accuracy, completeness, and consistency.

A unique opportunity for medical devices to gain faster market access in China is the Hainan Bo'ao Pilot Programme, which provides a pathway for importing new drugs and devices without Chinese approvals. In 2013, the People's Republic of China ('PRC') State Council decided to set up the Lecheng International Medical Tourism Pilot Zone ('BMTPZ') as a pilot zone for the promotion of international medical tourism. In 2018, the Chinese Central Government announced the entire Hainan Province (where BMTPZ is located) as the 12th free trade zone in China. The government also called for full implementation of the favourable policies granted to BMTPZ in 2013. These policies include: allowing importation of a small amount of drugs to meet urgent clinical needs for use in designated hospitals; allowing cutting-edge medical research projects, such as stem cell studies; and reducing tariffs on medical devices and drugs. Drugs imported under these policies can benefit from an accelerated special-approval process, and clinical data generated from this pilot programme can be used to support new drug applications in China. All drugs are entitled to zero-tariff treatment.

Unapproved medical devices that address urgent clinical needs can also be imported to Hainan for use in designated hospitals in the BMTPZ. In 2018, the Hainan People's Government issued the Interim Regulation on Administration of Importing Medical Devices for Urgent Clinical Use in BMPTZ. An updated version of this regulation was promulgated in 2020. This regulation provides detailed guidance on the application and approval process for medical devices that have been approved abroad but have not been approved in China and are not replaceable by medical devices already registered in China. RWD generated from the use of medical devices under this policy can be used to support imported medical device registration applications in China. Medical devices are not eligible for zero-tariff treatment unless they are for use by the owner only as manufacturing equipment, but their import duties may be reduced over time.

On 18 April 2022, China's Center for Medical Device Evaluation ('CMDE') and the Hainan Medical Products Administration jointly issued the Communication Procedures for Pilot Medical Devices Real-World Data Application Projects in BMTPZ (for Trial Implementation). Overseas manufacturers can apply to conduct real world studies to collect RWD as local clinical evidence to support their product registration in China. Because China does not have a formal pre-submission channel like the U.S. FDA, this guideline established a more formal communication process, as well as roles and responsibilities between CMDE and overseas manufacturers. Additionally, according to reports, a regional RWD database may be launched in Hainan to enable total product life cycle supervision.

RWD in Hainan is generated from multiple sources, including: electronic medical records when patients receive treatment in BMTPZ; information spontaneously reported by patients; diagnoses, treatment data, and follow-up visit data generated in the patients' place of residency; and information related to the device and its adverse events that is reported to the drug administrative authorities in Hainan.

The BMPTZ faces certain practical challenges; in particular, RWD is auxiliary to clinical-trial data in supporting marketing approvals in China. Most successful approvals have involved both BMTPZ RWD and overseas clinical data. Despite its challenges, the BMPTZ represents an important opportunity for international drug and device manufacturers and medical research institutions to swiftly enter China's growing medical market.

There is also much room for development in the area of international harmonisation across jurisdictions, though some collaborative momentum has been built in recent years due to the COVID-19 pandemic. For example, in summer 2022, ICMRA released a joint statement acknowledging the need for greater international alignment on RWE issues. The ICMRA members pledged to foster global efforts to further enable the integration of RWE into regulatory decision-making, highlighting the key areas of harmonisation of RWD and RWE terminologies, convergence on guidance and best practices, readiness, and transparency. Though efforts like these have significantly advanced the cause of international harmonisation, there is still a long way to go until true international harmonisation will be realised.

Health Data

Health data can be generated from various sources, ranging from hospital or clinic visits to mobile wearable devices and connected medical devices that can manage individual health and wellness. The sharing of such health data is key to the development of more personalised treatment and optimisation of treatment interventions. Health data contribute to the sustainability of health systems by improving decision-making regarding disease prediction and prevention and addressing public health threats. Hence, the use of health data in health care delivery has expanded rapidly in the past few years.

In the United States, wearable monitoring devices can track and transmit health data to a patient's health care professional ('HCP') in real time; in the European Union ('EU'), a centralised data store where EU citizens can access their health information and ePrescriptions, called MyHealth@EU, is live in 10 Member States. Further, pilots are in the pipeline, particularly in view of the recent European Commission's proposal to regulate different types of electronic health data. In the UK, digital growth charts pioneered by the Royal College of Paediatrics and Child Health rely on open-source coding to instantaneously calculate child growth predictions; and in China, large databases contribute to aspects of the health care system ranging from commercial health insurance to critical care medicine.

The frameworks governing health data, at both national and international levels, continue to evolve. Major jurisdictions continue promulgating guidance on cross-border transfer mechanisms for personal data, reflecting the increasingly global nature of health care delivery and clinical research. Data privacy concerns and cybersecurity risks have intensified over the course of the COVID-19 pandemic, and an increasing number of medical devices are susceptible to such threats. In recent years, multiple jurisdictions have issued new guidance on minimising such risks.

United States

In the United States, while there is no federal general data privacy law, health data are governed by the Health Insurance Portability and Accountability Act of 1996 ('HIPAA'). Further, at the state level, the United States has increasingly seen states passing their own privacy laws. California, Virginia, Colorado, Connecticut, and Utah have already passed comprehensive data privacy bills, and many more states are considering passing data privacy bills, including bills addressing health privacy and automated decision-making.[4] The increasingly complicated patchwork of state laws has led to some rumblings that a new U.S. federal privacy law could be in the cards, but the legislative action seems to be at the state level for now.

At the international level, the European Commission may soon recognise the United States as having an adequate data protection framework. Such an adequacy decision would allow a broad range of health-related companies with a United States presence, including pharmaceutical, medical device, and digital health companies, to more easily transfer health data from the European Economic Area.[5] This issue is particularly salient for entities involved in clinical research and telemedicine; for example, the lack of adequacy decision has complicated the U.S. National Institutes of Health's ability to obtain data from studies that contain European participants. In October 2022, President Biden issued an Executive Order implementing a new US-EU data transfer framework called the Transatlantic Data Privacy Framework. In December 2022, the European Commission issued its proposed adequacy decision for the United States based on President Biden's Executive Order. The Transatlantic Data Privacy Framework would allow organisations to transfer personal data freely from the European Economic Area to the United States, without relying on transfer mechanisms such as the EU Standard Contractual Clauses.[6] The European Commission's draft adequacy decision will now undergo a review process by the European Data Protection Board, EU Member States, and the European Parliament, which can take six months or longer. Some experts predict the release of a finalised adequacy decision in summer 2023.

With respect to security more generally, in April 2022, the FDA released the draft guidance document 'Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions'. This draft guidance, which applies to medical devices broadly and is not limited to the digital health context, provides details about how device manufacturers should integrate cybersecurity considerations into their quality systems, and about what cybersecurity information should be included in premarket submissions to demonstrate a reasonable assurance of safety and effectiveness.[7] Additionally, in November 2022, the FDA updated the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, which 'outlines a framework for health delivery organisations ('HDOs') and other stakeholders to plan for and respond to cybersecurity incidents around medical devices, ensure effectiveness of devices, and protect patient safety'.[8]

Europe

In response to increasing use of big data derived from various sources to support regulatory and market access decision-making, greater scrutiny will be placed on the quality of the data sources to determine whether the data can be relied upon to inform regulatory decision-making.

Additionally, in May 2022, the European Commission proposed a regulation which would create a health data ecosystem known as the European Health Data Space ('EHDS'). If adopted, the EHDS would fully harmonise electronic patient records throughout the EU and facilitate the portability of patient records across Member State borders. This colossal database could be accessed for the purpose of providing health care as well as secondary purposes such as policymaking and research by industry. Each use would be underpinned by clear rules,

common standards and practices, infrastructure, governance, security, safety, and privacy. The Commission has ambitiously communicated that its 'target is for the Health Data Space to start functioning by 2025'. However, significant challenges will need to be overcome before the launch of the EHDS. Currently, the proposal is in draft form awaiting the Committee's decision.

In the EU and UK, personal data are governed by the EU General Data Protection Regulation ('EU GDPR') and its UK counterpart, the Data Protection Act 2018 ('UK GDPR') (collectively, 'GDPR'). GDPR is a sweeping data privacy law: EU GDPR represented the biggest ever change to data privacy laws, and it applies broadly – any organisation operating within the EU, as well as any organisations outside of the EU which offer goods or services to customers or businesses in the EU, is subject to EU GDPR. UK GDPR has a similar extraterritorial reach.

While representing a sea change in the protection of personal data, GDPR also has shortcomings. For example, within the healthcare space, GDPR fails to answer whether the training data used to develop ML systems can be retained after the project is complete and reused for other purposes, or whether such data can be shared with third parties. Currently, parties determine the use of such data through contractual negotiations. However, due to the sensitive nature of health data, some critics suggest that regulations should carve out the health care industry and apply additionally stringent rules that do not allow for certain commercial arrangements.

GDPR has set out the global regulatory standard for data protection for several years, governing data processing and cross-border data transfer in particular, but the tide appears to be turning.[9] In addition to major jurisdictions like China promulgating their own data protection laws (as discussed in more detail adjacent), new laws within Europe are also either under negotiation or taking effect soon. Cybersecurity has been a particularly hot topic, notably in light of recent high-profile cyberattacks, such as a 2022 attack on an IT service provider that affected National Health Service ('NHS') resources. In January 2023, for example, the EU's Network and Information Security 2 Directive entered into force; this cybersecurity legislation will implement security and reporting requirements across EU states. Further, the proposed European Cyber Resilience Act would regulate cybersecurity requirements for products with digital elements. The main objectives are two-fold: (i) to facilitate the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's life cycle; and (ii) to allow users to take cybersecurity into account when selecting and using products with digital elements.

Cybersecurity is also a priority in the UK. The UK government announced in November 2022 that it would strengthen the UK's Network and Information Systems regulations, which were established in 2018. The objective of the legislative proposal was to improve the UK's cyber resilience. Under the proposed changes, digital service providers will face fines of up to £17 million if they fail to put in place effective cybersecurity measures. The legislative proposals included seven policy measures seeking to address the increasingly sophisticated and frequent cybersecurity threats facing UK companies. The proposed changes will bring providers of outsourced IT and 'managed service providers' into the scope of the existing regulations.

Finally, in 2022, NICE unveiled its Early Value Assessment for Medtech ('EVA') programme, which is an innovative new approach to assessing digital health products that best reflect system need and demand. This programme offers a rapid assessment on the clinical effectiveness and value-for-money of such products. The methodological approach will explore in detail the potential of technologies to: (i) address unmet medical need; (ii) assess existing evidence; and (iii) identify key gaps in the market place. Once a technology receives a conditional recommendation through EVA, NICE will work with manufacturers to develop a plan to gather detailed evidence while the product is in clinical use. The benefit of EVA is to support earlier patient access to technologies that have the potential to meet system needs. Unlike existing NICE guidance processes, EVA would not require selected technologies to have generated a large amount of evidence. Rather, the data would be generated incrementally once the technology has been recommended for use in the NHS.

China

The PRC's data governance regime has evolved in recent years, including the additions of the Cybersecurity Law in June 2017 (which regulates cybersecurity and the construction, operation, maintenance, and use of networks in China); the Biosecurity Law in April 2021 (which regulates activities related to biosecurity, such as the safety management of biological materials and data derived therefrom); and the Data Security Law in September 2021 (which applies to data processing activities in China). Additionally, the Human Genetics Resources ('HGR') Regulation (2019) governs the processing of HGR data (defined as data that derives from organs, tissues, cells, or other biospecimens that contain human genome or genes). The processing of clinical-study data is subject to the HGR Regulation. On 22 March 2022, the Ministry of Science and Technology released draft Implementing Rules on the Administrative Regulations on Human Genetic Resources for public comment. These draft rules will provide clearer guidance on how foreign entities can make use of Chinese HGR. Most recently, the Personal Information Protection Law ('PIPL') came into effect in November 2021. In addition to applying across the PRC, PIPL also has extraterritorial applications, including: telemedicine services offered to patients in the PRC; collaborating with researchers in the PRC; and acting as a lead site for a multi-national clinical trial with PRC-based sites. PIPL applies (i) where the processing is for the purposes of providing products or services to individuals located in China; (ii) where the processing is for analysing and evaluating the behaviour of individuals located in China; and (iii) under circumstances prescribed by laws and administrative regulations.

PIPL governs any 'analysing or assessing activities of natural persons inside the borders' of the PRC, even if the handling activities take place outside of the PRC.[10] Accordingly, conducting clinical research with research sites or research subjects located in the PRC could involve activities that may constitute 'analysing or assessing activities' of data subjects. For example, PIPL applies to studies conducted through mobile applications whereby subjects are enrolled remotely and the app collects data on the subject's physical condition or geographic location through the subject's mobile phone; or to wearable devices that transmit health and other data to another country for use in research. Health and biometric data qualify as 'sensitive personal information' under PIPL and qualify for additional protections, including a requirement to collect separate consent for processing such personal data.

PIPL requires all personal-information controllers that need to transfer personal information out of Mainland China to either: (i) pass a security assessment organised by the Cyberspace Administration of China ('CAC'); (ii) undergo certification by specialised certification agencies in accordance with

relevant regulations; or (iii) conclude a standard contract designated by China cyberspace regulators with the overseas recipient. In September 2022, the Measures for the Security Assessment of Outbound Data Transfers promulgated by CAC came into effect. This regulation specifies that a security assessment application must be filed with CAC if: (i) the data to be transferred abroad are important data; (ii) a critical information infrastructure operator or a personal-information handler who has processed more than 1,000,000 persons' personal information intends to transfer personal information abroad; or (iii) a personal-information handler who has transferred the personal information of 100,000 persons or the sensitive personal information of 10,000 persons cumulatively since 1 January of the previous year intends to transfer personal information abroad. In December 2022, the National Information Security Standardisation Technical Committee released the Practical Guide to Cybersecurity Standards – Specifications on Security Certification for Cross-Border Personal Information Processing Activities V2.0. Further, in February 2023, the CAC released the Provisions on Standard Contracts for Cross-border Transfer of Personal Information, which will become effective on 1 June 2023. Moving forward, personal-information controllers and overseas recipients are expected to conclude the standard contract for data transfer outside of China using the standard contractual clauses affixed to the Provisions. These guidelines supplement and clarify PIPL's personal information protection certification regime. These developments are reminiscent of cross-border data transfer mechanisms under GDPR and suggest that we may continue to see legislation detailing such transfer mechanisms from major jurisdictions.

Evolving Landscape of AI and ML

ML – which uses statistical pattern-recognition capabilities – and AI have increasing health care and life sciences applications, and the regulation of AI as a medical device ('AIaMD') and software as a medical device ('SaMD') has rapidly evolved. SaMD and other non-device software is used in the treatment and diagnosis of diseases and conditions underpinned by AI and ML, and apps are now able to produce imaging analytics, connect HCPs with one another, monitor medication adherence, and communicate felt experience during treatment with HCPs. For a more thorough discussion of the regulatory framework governing AI and ML in these key jurisdictions, see *A Cross-Border Regulatory and Public Policy Analysis of Machine Learning and Artificial Intelligence: The Future of AI in Life Sciences* (2022).[11]

A key concern from a global perspective is the lack of generalisability of AI/ML across jurisdictions. For example, the exact definitions of AIaMD and SaMD vary across jurisdictions, which poses challenges to regulators who may wish to pursue a more unified global approach with such technologies. Additionally, regulators have grappled with how to handle the inevitable changes in AI/ML-enabled devices as they learn and develop. However, better validation, documentation, and testing of AI/ML-enabled devices will generally facilitate acceptance of such devices across jurisdictions.

United States

FDA guidance directly on point to the regulation of SaMD with AI and ML components has to date been fairly limited, given that such software is an emerging area of development. However, the guidance that has been made available signals significant agency investment in allowing AI and ML to be integrated into SaMD as a general matter, while developing flexible regulatory mechanisms by which device changes due to AI/ML components can be appropriately pre-approved as long as they do not too significantly alter the functioning of the device.

In 2021, FDA released its *Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan*, highlighting that such technologies 'have the potential to transform health care delivery', with the agency anticipating that 'with appropriately tailored total product life cycle-based regulatory oversight, AI/ML-based [SaMD] will deliver safe and effective software functionality that improves the quality of care that patients receive'. This action plan followed the 2019 publication of FDA's *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)*, which underscored that though FDA's historical typical sign-off has been on AI/ML-based SaMD with 'locked' algorithms – ones that do not change once released into the market – the future lies in adaptive products that 'learn' with time and increasing numbers of inputs.

These guidance documents anticipate FDA review, during the initial premarket review for an AI/ML-based device, of a 'Predetermined Change Control Plan'. Such a plan would detail information about both the types of anticipated modifications to the software and the methodology underlying algorithm changes, to ensure that the device remains safe and effective after the modification. FDA's proposed framework further clarifies, however, that subsequent regulatory reviews may still be required, depending on the type of modification being made.

Greater clarity on this topic is coming soon, as in mid-February 2023 FDA sent a draft guidance document titled 'Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning-Enabled Device Software Functions' to the White House for review and potential publication clearance. The guidance, if issued, will come on the heels of a recent statutory amendment, which granted the FDA the authority to proactively sign off on device changes, if consistent with a predetermined change control plan.

Europe

As part of the EU's AI Strategy, the Commission has proposed a first-of-its-kind regulatory framework on AI comprising a Regulation laying down harmonised rules on AI (the 'AI Act') and a Directive on its associated non-contractual civil liability profile (the 'AI Liability Directive'). In its current draft, the AI Act distinguishes between uses of AI that create unacceptable risk, high risk and low/minimal risk. If adopted, high-risk AI systems will need to meet comprehensive requirements, such as those related to data governance, recordkeeping, transparency, accuracy, and security. Low/minimal-risk uses of AI will need to abide by transparency obligations. The AI Liability Directive seeks to give businesses legal certainty on their exposure to liability, while simultaneously ensuring that the legal framework is fit for the increasingly digitised economy. The new regime lays down uniform rules for access to evidence and alleviation of the burden of proof in relation to damages caused by AI systems, thus establishing broader protection for an injured party to seek redress. It also introduces a presumption of causality against the developer, provider, or user. Given the novelty of these proposals, their impact on businesses, and their cross-sector application, it is anticipated that the progression of the AI Act and the AI Liability Directive through the legislative process over the course of 2023 will receive a great deal with scrutiny.

In contrast to the EU, the UK is currently pursuing a decentralised approach to the regulation of AI. Industry regulators,

such as the MHRA, are charged with developing regulatory regimes specific to the industries they regulate. In its Roadmap of 17 October 2022, the UK MHRA published its Guidance on Software and AI as Medical Device Change Programme Roadmap. The guidance builds on the Government responses to consultation on the future regulation of medical devices in the UK and follows on from the Software and AI as Medical Device Change Programme, which was published in 2021. Among other issues, the guidance aims to ensure that SaMD can be accurately distinguished from other products and promises to update the national Borderlines Manual. However, some key issues discussed in our recent publication[12] remain under consultation, including the need to formally define the concept of a manufacturer for SaMD. For example, as apps often use open-source code, any entity making modifications to the code may inadvertently take on the responsibilities of the manufacturer of this modified code if the software classifies as SaMD.

The UK Government's Roadmap sets out a number of 'Work Packages' addressing specific aspects of such devices, including qualification, classification, premarket evaluation, post-market surveillance, and cybersecurity. Several of the Work Packages address AIaMD, specifically: Work Package Nine 'AI RIG' aims to clarify how AIaMD can best meet medical device requirements for products utilising AI; Work Package 10 'Project Glass Box' aims to improve user functionality and transparency in AIaMD in the UK; and Work Package 11 'Project Ship of Theseus' focuses on the adaptability of AI across digital health. MHRA intends to publish the specific guidance in a step-wise manner.

A report published by the UK Regulatory Horizons Council in November 2022 outlines the need to make the AIaMD regulatory process more open and transparent, to increase the involvement of patients and public, and to improve regulatory clarity for manufacturers and users. The report recommends building a critical mass of AIaMD experts across all key industry gatekeepers (in the UK, this would include MHRA, NICE, the Health Research Authority, and the Care Quality Commission), to enable appropriate and sufficient scrutiny of products entering into the marketplace.

China

China does not have legislation specifically regulating AIaMD and SaMD; rather, the general medical device regulations apply to medical device software products. However, the CMDE introduced new Guidelines for Registration Review of AI-enabled Medical Device in March 2022, which clarify the registration process and standardise the technical review requirements for AIaMD. These guidelines define AIaMD as medical devices that use AI technology to analyse medical device data to achieve a medical use; the guidelines do not consider products that base their output on non-medical data or have non-medical uses to be AIaMD. These systems' value is judged by their generalisability, which the NMPA monitors as an ongoing concern with requirements focusing on:

- data acquisition: adequate and diverse data; the rationality of data distribution; and the quality control of data collection, data set construction, and annotation;
- algorithm design: algorithm selection must be clear; training data volume evaluation must prove the adequacy and effectiveness of algorithm training; and the analysis of data outputs such as false negatives and positives, repeatability, robustness, real-time performance, and reproducibility; and
- validation and qualification: clinical validation; and a comprehensive analysis of the algorithm's performance.

The guidance also highlights specific data and information security practices that companies should use to protect their proprietary information, including diversifying patent portfolios and streamlining the technical features of patent claims. The guidelines add to a robust body of rules issued by NMPA regarding the development and maintenance of SaMD.

Conclusion

The digital health revolution has transformed the delivery and management of health systems. The enabling technologies also transform how health-related data are collected, processed, and captured to inform decision-making and improve patient outcomes. Health data could also be potential secondary data sources for clinical research in a real-world setting. Data are considered health-related if they provide information on health status or prognostic characteristics of individuals or populations at large. ML and other digitalised analytical tools could substantially improve data mining for the detection and surveillance of a health-related event or emerging disease. Research based on such applications could provide insights into causal relationships between a treatment and its effects on human subjects.

Such sweeping technological and methodological advances are bringing about a sea change in the global regulatory environment. Regulators from around the world are rethinking their approaches, adopting regulatory models that are agile, iterative, and collaborative to address the considerable challenges posed by disruptive digital health technologies and methodological approaches. In general, regulators are moving towards outcome-based regulations, aiming to strike the right balance between the need to foster innovation and the need to enforce the regulators' statutory role – to protect public health by preventing unintended consequences of emerging technologies and novel analytical approaches. To enable the exchange of health data within the increasingly globalised healthcare and life sciences ecosystems, interoperability and cross-border collaboration on developing internationally agreed standards will become a necessity in order to identify data sources that are findable, accessible, interoperable, and reusable. All these endeavours will likely be the next frontier for better regulation of the healthcare and life sciences sector.

Acknowledgments

The authors are very grateful to Bo (Alice) Du ('BD'), Julie Kvedar ('JK') and Helen Ryan ('HR'), who are associates respectively based in Shanghai, New York and Washington D.C., for their contributions to this chapter. BD advises life sciences companies on a wide range of regulatory and compliance matters. JK's practice focuses on cross-border healthcare transactions and regulatory compliance matters. HR advises on life sciences regulatory compliance.

Endnotes

1. Tsang L., *et al.*, *Global Landscape of Digital Health: Impact on Healthcare Delivery and Corresponding Regulatory and Legal Considerations* (2021).
2. 21 U.S.C. § 355(d).
3. 21 C.F.R. § 860.7(c)(2).
4. https://www.ropesgray.com/en/newsroom/podcasts/2023/january/the-data-day-world-data-protection-day-trends-hot-topics.
5. https://www.ropesgray.com/en/newsroom/podcasts/2023/january/decoding-digital-health-trans-atlantic-transfers-of-health-data.

6. https://www.ropesgray.com/en/newsroom/alerts/2022/october/white-house-issues-executive-order-outlining-key-points-of-the-transatlantic-data-privacy.
7. https://www.ropesgray.com/en/newsroom/alerts/2022/may/fda-updates-guidance-on-cybersecurity-responsibilities-for-medical-device-manufacturers.
8. https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.
9. https://www.ropesgray.com/en/newsroom/podcasts/2023/january/the-data-day-world-data-protection-day-trends-hot-topics.
10. PIPL Art. 3.
11. Tsang L., *et al.*, *A Cross-Border Regulatory and Public Policy Analysis of Machine Learning and Artificial Intelligence: The Future of AI in Life Sciences,* 34 Intell. Prop. & Tech. L.J. 10, 3–11 (2022).
12. *Ibid.*

Dr. Lincoln Tsang is partner and head of Ropes & Gray's European Life Sciences Practice. A former senior regulator, he is qualified as a lawyer and a pharmacist with post-graduate training in toxicology and cancer pharmacology, and concentrates his practice on UK, EU, and cross-border regulatory compliance and enforcement, including litigation, internal investigations, and public policy matters affecting the life sciences industry. Lincoln advises clients on research and development strategies, product life cycle management, product acquisition, and risk and crisis management. He also regularly represents clients before various regulatory bodies on a wide range of matters, including clinical trials, product approval, advertising and promotion, manufacturing, safety vigilance, and health-technology appraisal relevant to pricing and reimbursement decision-making for medicines and medical devices. He has also appeared before various legislatures as an independent expert on product approval and market access of medical products.

Ropes & Gray LLP
60 Ludgate Hill
London EC4M 7AW
United Kingdom

Tel: +44 20 3201 1500
Email: lincoln.tsang@ropesgray.com
URL: www.ropesgray.com

Kellie Combs, partner in Ropes & Gray's FDA regulatory practice group and co-chair of the firm's cross-practice Digital Health Initiative, provides legal and strategic advice to pharmaceutical, biotechnology, medical device, food, and cosmetic manufacturers, as well as hospitals and academic institutions, on a broad range of issues under the Food, Drug, and Cosmetic Act and the Public Health Service Act. Kellie is currently advising several clients on issues related to the COVID-19 pandemic, including the deployment of digital health and telemedicine tools and the marketing of products authorised pursuant to FDA's Emergency Use Authorisation process. She routinely advises on matters implicating FDA promotional rules and the First Amendment, life cycle management, regulation of clinical research and post-approval compliance. In addition, Kellie conducts regulatory due diligence in connection with transactions involving drug, device, dietary supplement, cosmetic and other consumer product manufacturers, and she has advised on many government investigations of FDA-regulated companies.

Ropes & Gray LLP
2099 Pennsylvania Avenue, NW
Washington, D.C. 20006-6807
USA

Tel: +1 202 508 4600
Email: kellie.combs@ropesgray.com
URL: www.ropesgray.com

Katherine Wang is a partner in Ropes & Gray's life sciences group. Widely regarded as a leading life sciences regulatory lawyer in China, Katherine assists pharmaceutical, biotechnology, and medical device companies on a wide range of matters, including early-stage discovery, product registration, regulatory/GxP compliance, pricing, reimbursement, clinical studies, promotional practices, and product safety issues. Katherine provides day-to-day counselling on issues that life sciences companies face in relation to their interaction with agencies including the National Medical Products Administration (NMPA, formerly the CFDA), the National Health Commission (NHC), the State Administration of Market Regulation (SAMR), and the Human Genetic Resources Administration of China (HGRAC), among others. She also assists institutional investors and corporate clients in structuring transactions and conducting regulatory due diligence, including good laboratory practice (GLP), good clinical practice (GCP), good manufacturing practice (GMP) and pharmacovigilance, on investment targets and prospective business partners in China.

Ropes & Gray LLP
36F, Park Place, 1601 Nanjing Road West
Shanghai 200040
China

Tel: +86 21 6157 5200
Email: katherine.wang@ropesgray.com
URL: www.ropesgray.com

Ropes & Gray is a preeminent global law firm with approximately 1,400 lawyers and legal professionals serving clients in major centres of business, finance, technology and government. The firm has offices in New York, Boston, Washington D.C., Chicago, San Francisco, Silicon Valley, London, Hong Kong, Shanghai, Tokyo, and Seoul, and has consistently been recognised for its leading practices in many areas, including private equity, M&A, finance, asset management, real estate, tax, antitrust, life sciences, healthcare, intellectual property, litigation & enforcement, privacy & cybersecurity, and business restructuring.

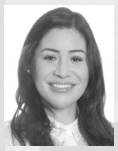
www.ropesgray.com

ROPES & GRAY

Data Protection and Data-Driven Digital Health Innovation


Dr. Nathalie Moreno


Lydia Loxham


Harriet Bridges

Addleshaw Goddard LLP

Introduction

The United Kingdom (**UK**) enjoys a dynamic digital health market characterised by innovation and growth, and encompassing both the private and public sectors. However, the development of new digital health technologies (**DHTs**) and solutions continues to face a challenging and multifaceted legal and regulatory landscape, including data protection laws, set for reform.

The past year has seen organisations in the UK continue to innovate, with a significant increase in the development, production and implementation of data-driven medical technologies and medical devices (**MedTech**), DHTs and digital transformation initiatives within the healthcare sector.

These trends are set to continue into 2023, with constant new ways for DHTs and devices to collect, track, analyse and utilise personal data, including arguably more revealing personal data such as specific genetic biomarkers and biological samples, on course to progress accordingly.

The impact of continued developments within the digital health sector will undoubtedly be significant, from both a patient- and industry-supply perspective. Increased access to these novel data-driven products could revolutionise the healthcare system in the UK. Promoting digital transformation across the health and social care system, the Government aims to embed digital technologies in the system. Such ambitious reforms include: digitising health and social care records; enabling digital diagnoses; expanding the functionalities of the two principal national digital channels, the NHS App and the NHS.uk website; devising clearer policies for accrediting DHTs that are likely to be adopted nationally by the NHS with the National Institute for Health and Care Excellence (**NICE**); and piloting a new early value assessment (**EVA**).

Aspiring to unlock the power of data, it is no surprise that the Government would seize the opportunity to rethink and support radical reforms. In the past year, significant changes to the data protection regime in the UK have been contemplated, from both a regulatory and a legislative perspective. At the heart of these proposed changes is the Government's drive to promote data-driven innovation and to reduce regulatory burden in the post-Brexit and post-pandemic UK landscape.

As highlighted by the Information Commissioner's Office (**ICO**) – the UK's data protection supervisory authority – the effectiveness of any data-driven innovation relies on user engagement and public trust. To ensure that patients are suitably protected and to maintain public support for the continued development of such technologies and solutions, organisations must continue to take proactive steps to understand and meet their obligations under the current data protection regime, including those required by the UK General Data Protection Regulation (**UK GDPR**), the Data Protection Act 2018 (**DPA 2018**) and the Privacy and Electronic Communications Regulations 2003 (**PECR**), while also staying abreast of the potential impact of the Government's proposed reforms in the digital health sector.

Remote Patient Monitoring in Healthcare

The COVID-19 pandemic has seen many healthcare systems around the world come under unprecedented strain due to staff shortages, budget cuts and other financial pressures. Many healthcare providers, including the NHS in the UK, have therefore adopted digital health solutions, such as remote patient monitoring (**RPM**) initiatives, to respond to these challenges.

RPM initiatives collect patient data via DHT platforms, MedTech and other digital products. The data collected is then shared with a healthcare professional for clinical assessment and diagnosis. The COVID-19 pandemic saw the adoption of RPM initiatives by many hospitals around the world as a new way of monitoring patients after their discharge from hospital, and in 2022, these RPM initiatives were utilised in other healthcare contexts, such as the management of chronic medical conditions. RPM initiatives and similar technologies are also increasingly featuring in the NHS's plans to transform the UK healthcare system; their use has been a focus in both the NHS 2022 delivery plan for tackling the backlog of elective care post-pandemic,[1] and in the recent NHS publication[2] on the steps taken to increase operational resilience in preparation for winter 2022/23.

Alongside their clear clinical benefits, including reduced patient wait times, RPM initiatives come with a range of data protection and privacy concerns; in particular, the sharing of patient special-category data. To navigate this hurdle, NHS England's Transformation Directorate has published practical, governance-focused guidance[3] for the use of RPMs which highlights the importance of undertaking Data Protection Impact Assessments (**DPIA**) prior to implementation, and of ensuring

that contractual data-sharing terms are put in place with RPM providers and relevant care partners, particularly given that the processing is likely to result in a high risk to the rights and freedoms of patients. The guidance further sets out that DPIAs should be continuously reviewed and updated while the RPMs are in use.

The large volume of data obtained by RPMs and similar technologies allows developers to establish a strong evidence base to analyse their performance and effectiveness. It also allows the NHS to analyse the levels of public engagement and to consider what improvements could be made in future service design and delivery. However, much of the data obtained is special-category (health) data relating to patients, so the lawful bases and legal grounds under which the data can be used for other purposes, including commercial purposes, are still limited at this time.

Artificial Intelligence (AI)

AI technology has huge potential to revolutionise healthcare in expediting diagnosis and treatment as well as minimising costs of delivery. The UK Government has recognised that "AI-driven technologies have the potential to improve health outcomes for patients and service users, and to free up staff time for care".[4] Recent developments have enabled a breakthrough in heart disease screening,[5] the prompt identification of people with high-risk factors of hepatitis C (which is otherwise difficult to detect at an early stage)[6] and the proactive screening of tumour regrowth in cancer patients to enable earlier treatment and improve outcomes.[7]

However, the potential for huge medical gain is matched by high risks from a data protection perspective, which practitioners need to be alive to and be able to mitigate. Various studies have shown the importance of quality data input and the potential for inherent bias in the data pool which can skew outcomes.[8] A study conducted by the University of Oxford in relation to image-recognition technology that was developed based on AI algorithms to enable the classification of skin lesions showed that, as the data input was largely based on Caucasian patients, the tool struggled to identify lesions in patients with darker skin.[9] Likewise, research on oximeters to spot early signs of falls in oxygen levels, used increasingly during the COVID-19 pandemic, indicated that they performed better on lighter skin[10] and therefore delivered less favourable outcomes for ethnic minority patients. Data obtained from spirometers, which measure lung capacity, had also tended to indicate that ethnic minority users had lower lung capacity, an assumption that arose from racial biases in the data inputs into the AI tool. The ICO has rightly indicated that, due to these risks to the privacy rights and freedoms of individuals, AI will be one of its priority areas for regulation in 2023.

The ICO has also highlighted various considerations, directly derived from certain of the data protection principles, to ensure that the processing of personal data through AI is fair and lawful when designing a tool based on AI technology, including:[11]

- **Privacy by design and default**: Consider whether the use of AI is necessary or whether the end goals can be achieved by another, less high-risk, means. If AI is the preferred route, then an assessment of the risks involved should be carried out and appropriate safeguards put in place to mitigate the privacy risks.
- **Transparency**: Provide clear explanations of the decisions being made by AI-technology systems to individuals affected by such decisions.
- **Data minimisation**: Limit the amount of data used, and, to the extent possible, techniques such as perturbation or the use of synthetic data or federated learning should be employed.
- **Mitigations**: Implement appropriate safeguards to clean and define the labelling criteria for the data inputs at the outset, particularly given the potential for inherent bias in the collection of data.
- **Security measures**: Implement appropriate technical and organisational measures, such as the debugging of AI models, as a means of minimising the risk of unsatisfactory outputs.
- **Human review of AI decisions**: Build into the tool the possibility for meaningful human review of decisions made by AI, to be conducted by adequately trained and suitably senior staff with authority to override an automated decision.

It is widely recognised that the legislative framework currently in place to regulate AI in healthcare and more broadly is deficient as it was put in place before AI technology was contemplated. The European Commission has attempted to address this deficiency with its proposal for an AI Regulation (April 2021),[12] which seeks to more closely regulate high-risk AI systems with a sliding scale of rules based on the perceived risk to individuals.

For high-risk AI technology, the draft Regulation proposes to embed the need for human oversight of decisions made by AI tools and to promote data governance management practices that support the use of quality data inputs. It also proposes to impose penalties of up to €30 million or 6% of worldwide annual turnover for non-compliance,[13] which surpass the maximum penalties under the UK GDPR. Although the Regulation is still in draft form, it could become the blueprint for other regulators seeking to introduce similar legislation, so AI developers should monitor the progression of the Regulation as a matter of priority.

In the UK, the Government has indicated its intention[14] to diverge from this legislative approach and to adopt a sector-focused, non-statutory, light-touch regime which would seek to regulate the use of AI through industry guidance and codes of conduct. It would address high-risk concerns without placing unnecessary obstacles in the way of innovation. The National AI Strategy anticipates many AI-centric publications and consultations over the next decade, including a policy paper and white paper covering the Government's pro-innovation position on the governance and regulation of AI in the UK. However, the Department for Digital, Culture, Media & Sport (**DCMS**) is yet to provide further detail of its plans, so it remains to be seen whether this proposed divergence from the approach in Europe will materialise.

Consumer Healthtech

Year on year, there is a significant increase in the use of MedTech, DHTs and digital initiatives by consumers, including wearable technologies and health apps that track physical activity and monitor various health conditions. This trend has continued post-pandemic with a steady stream of new products and technologies joining the market.

While healthtech products are increasing in popularity and becoming more common, there are several key considerations that developers need to consider when designing and maintaining their products in order to meet their obligations under UK data protection laws. This is because the vast majority of healthtech products operate by continuously collecting and processing large volumes of personal data (including special-category health data). Designers and developers should therefore ensure that users of their healthtech devices are fully informed of what personal data is being collected about them, and how it will be used and shared. They should also be able to identify an appropriate lawful basis

to cover the processing activities carried out by the product. In addition, any algorithmic processing and AI used in conjunction with consumer healthtech should be accurate, fair and fully assessed to mitigate the risk of systemic bias.[15]

The ICO's Code of Practice for Consumer Internet of Things (**IoT**) Security also sets out practical steps for manufacturers of IoT devices to improve the security of the products and any associated services.[16] These steps include keeping software updated, securely storing credentials and security-sensitive data, ensuring personal data is protected, making systems resilient to outages and making it easy for consumers to delete personal data.

That said, healthtech is likely to be affected by the reforms proposed to the UK data protection laws. Amongst other things, the Data Protection and Digital Information Bill (**DPDI**)[17] sets out that moving forwards, references to processing special-category personal data under Article 9 of the UK GDPR for the purposes of scientific research will mean "any research that can reasonably be described as scientific". This is expected to benefit those organisations designing and developing healthtech as it is expected to be an easier threshold to meet than the existing Article 9 wording which requires such processing to also be "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual".

The DPDI also proposes to include a general data processing consent for areas of scientific research where it is not possible to fully identify the scientific purposes (subject to certain conditions). This proposed position will allow organisations to expand their processing activities relating to special category data collected via healthtech, without the restriction of needing to obtain express and specific consent for all purposes from consumers upfront, which may not be possible.

Medical devices

A number of reforms on the horizon in the UK are due to impact the regulation of medical devices specifically. In particular, the Medicines and Healthcare products Regulatory Agency (**MHRA**) has announced plans to strengthen the regulation of medical devices to improve patient safety and encourage innovation.[18] The proposed reforms are due to come into force in July 2024 and will include the following measures:

- **Strengthening the MHRA's power to act** to keep patients safe.
- **Making the UK a focus for innovation** to become a world leader for developing and introducing innovative medical devices.
- **Addressing health inequalities** and mitigating biases throughout medical device product lifecycles.
- Introducing proportionate regulation which supports medical device businesses via new **access routes that build on both EU and wider global standards**.
- **Setting world leading standards** and building the new UKCA certification mark as a global exemplar.

Alongside these proposed reforms, the MHRA also announced the Software and AI as a Medical Device Change Programme[19] last year. Updates to the Programme introduced in October 2022 set out that, in respect of software as a medical device, specific cyber-security requirements will be introduced to mitigate the risks of both cyber-security vulnerabilities and issues presented by legacy software, medical devices and systems to patient safety and privacy.[20]

As the existing medical device regulations in the UK do not currently provide sufficient safeguards in respect of novel and emerging medical device technologies, the reforms proposed by the MHRA to strengthen the regulation of medical devices are essential, both in ensuring patient safety and privacy and in continuing to encourage innovation. Medical device businesses should therefore actively monitor the medical device regulatory landscape and ensure that they have appropriate business and development plans in place to mitigate the impact of these proposed reforms.

NICE EVA

NHS England and NICE are also developing a policy framework which will include a new commissioning pathway for several types of healthtech products. The new policy framework will apply to broader MedTech and DHTs, such as medical devices and diagnostics, as well as purely digital technologies such as software and apps.

Until now, there has been no clear commissioning pathway for healthtech in the UK, so there has been a lack of clarity for developers regarding (i) what evidence is required to demonstrate that their product is clinically sufficient and cost-effective, and (ii) how to present such evidence in pursuance of a NICE recommendation for adoption across the NHS. There has been a similar lack of clarity for clinicians and commissioners on which DHTs should be recommended to patients, and which can be NHS-funded, so patients are often unable to access the most beneficial technologies for managing their health. The introduction of the policy framework and a new commissioning pathway therefore hopes to remedy this.

One of the biggest changes proposed in the new commissioning pathway is the introduction of an EVA as a means of allowing healthtech products with smaller or emerging evidence bases to obtain a conditional NICE recommendation for use across the NHS without having to undergo a full NICE assessment. As healthtech products are required to demonstrate a mature evidence base before they are eligible to undergo a full NICE assessment, the hope is that healthtech assessed via the EVA could benefit NHS patients sooner than via current evaluation methods. Healthtech developers will then be encouraged to use the time while their product is under the conditional NICE recommendation to generate additional evidence of the product's clinical and cost-effectiveness and to address any gaps identified during the EVA.

NICE are planning to pilot the EVA across a range of healthtech products and use cases and data-collection infrastructures as a means of identifying and resolving any specific concerns, such as patient-related privacy and data protection concerns, with the new commissioning approach. At the time of writing, the policy framework and the new commissioning pathway (including the EVA) are due to be launched in Spring 2023.

Data Protection: Proposed Reforms

Many of the changes proposed to the UK's data protection reform consultations in the past 12 months will continue to progress in 2023. These proposed changes will have a significant impact on businesses in the digital health sector, particularly for those processing large volumes of special-category personal data and/or using AI tools or automated decision-making within their processing activities.

The DPDI

On 17 June 2022, the DCMS published its response to the "Data: A New Direction"[21] consultation. Annex A of the response

confirmed which of the proposed reforms to the UK's data protection regime would be taken forward, which would not, and which still required further consideration as part of the Government's plan to update and introduce legislation in this area.

Shortly after the DCMS published its response, the DPDI was laid before Parliament, with the aim of simplifying the UK's data protection regime post-Brexit by amending, not replacing, existing UK data protection legislation, including the UK GDPR, PECR and DPA 2018.

Some of the more pertinent proposed reforms for the digital health sector within the DPDI which the Government plans to take forward include:

- **Creating a statutory definition of scientific research** based on recital 159 of the GDPR. The Government intends to simplify the legal requirements around research so that scientists and researchers are no longer impeded by "overcautious and unclear rules" on how they can use people's personal data for scientific research, which will have a significant impact on the breadth and scope of scientific research in future.
- Incorporating **broad consent for scientific research** purposes within the data protection legislation. This will allow scientists and researchers to use a person's personal data for scientific research purposes without the need to obtain that person's specific consent to the purposes of processing.
- **Removing the requirement on organisations to conduct DPIAs** or undertake prior consultation with the ICO in relation to high-risk processing, and instead, allowing organisations to adopt different approaches to identify and minimise data protection risks that better reflect their specific circumstances. Removing this regulatory burden will likely have a large impact on organisations within the digital health sector where high-risk processing (such as using novel data collection methods to collect and process large volumes of sensitive patient data) is frequent.
- **Removing the requirement to obtain user consent in relation to the use of analytics cookies and/or similar technologies**. The DPDI sets out a proposal to treat analytics cookies and/or similar technologies in a similar way as "strictly necessary" or "essential" cookies which can be set without a user's consent. Similarly, the DPDI proposes to remove the requirement to obtain user consent for the use of analytics cookies and/or similar technologies in instances where an organisation either (i) uses such cookies or technologies in compliance with an ICO-approved sector code or regulatory guidance, or (ii) demonstrates a legitimate-interest legal basis for processing any data obtained by the cookies and/or technologies. This proposed reform could have a substantial impact for those in the digital health sector as it will streamline digital development and allow organisations that use such cookies, for example to measure traffic to a webpage or app, or to improve service offerings to users, to obtain consent from users prior to deploying such cookies.
- **Increasing fines under PECR**. The DPDI also proposes to increase the fines under PECR to align with the maximum penalties set out in the UK GDPR and DPA 2018. This increase would enable the ICO to issue organisations with fines of up to £17.5 million or 4% of global turnover for breaches of certain regulations under PECR, and up to £8.7 million or 2% of its global turnover for other breaches of PECR, which could have a significant impact in the digital health sector where initiatives such as digital tracking technologies and electronic communications feature heavily.
- **Reforming and enabling the DCMS Secretary of State's adequacy-making powers**. This suggestion sets out a proposed deviation from the European Commission's third-country adequacy test, towards a new and more flexible data protection test where the standard required from a third country is not that it must have an "essentially equivalent" standard of data protection to the country of export, but rather that it must not have a "materially lower" standard of data protection. This divergence with the EU's approach to international transfers could jeopardise the UK's adequacy decision and could ultimately result in new restrictions on international transfers between the UK and the EU being implemented.
- **Enabling businesses to use sensitive personal data for the purpose of managing the risk of bias in their AI systems** by providing legal clarity on how such sensitive personal data can be used to carry out bias monitoring, detection and correction. This proposed reform will be subject to appropriate safeguards, such as limitations on re-use and the implementation of security- and privacy-preserving measures when processing for this purpose.

  Although the DPDI was scheduled to have its second reading on 5 September 2022, it was determined that further consideration of the proposed reforms was needed, so the second reading did not take place as scheduled and a new date is still awaited.

The impact of the reforms set out in the DPDI, if and/or when they come into effect, therefore remain to be seen; however, for organisations wishing to monitor this development, progress of the bill through the relevant parliamentary stages can be tracked via the UK Parliament website.

UK international data transfers

Following the ICO's public consultation on how best to protect individual's personal data when transferred outside of the UK, and following Parliamentary approval, the following new data-transfer mechanisms came into force in the UK on 21 March 2022:

- The International Data Transfer Agreement[22] for use by data exporters in the UK, which serves as an alternative to the EU Standard Contractual Clauses, as issued under the European Commission Implementing Decision (EU) 2021/914 (**EU SCCs**).
- The international data transfer addendum to the EU SCCs (**UK Addendum**)[23] for use by data exporters in the UK where the data being exported is from both the EU and the UK and which is utilised in conjunction with the EU SCCs.
- Transitional provisions (**Transitional Provisions**)[24] for use by data exporters in relation to contracts entered into on, or before, 21 September 2022, which permit the continued use of standard data protection clauses in such contracts until 21 March 2024, provided that the contract includes the appropriate safeguards referred to in Article 46(1) of the UK GDPR and that the processing activities that are the subject matter of the contract remain unchanged.

The ICO further introduced a new transfer risk assessment (**TRA**) tool, following the CJEU's judgment in 2020 of case C-311/18 (**Schrems II**), which organisations looking to rely on one of the UK data-transfer mechanisms must carry out.

A TRA is required under UK data protection legislation as a means of demonstrating that an organisation has considered the risks to the rights and freedoms of natural persons and has

ensured that enforceable data-subject rights and effective legal remedies for data subjects are available in the country of import prior to making a data transfer.

Practically, the introduction of the UK data-transfer mechanisms, as well as the requirement to conduct a TRA in respect of them, may pose operational challenges for those organisations transferring large volumes of personal data outside of the UK on a regular basis; many organisations will likely need to conduct a substantial repapering exercise prior to the Transitional Provisions deadline, and many may need to reconsider their data protection governance with regards to international data transfers.

However, the main aim of each of the UK data-transfer mechanisms and the TRA tool is to facilitate the flow of data from the UK to non-adequate jurisdictions while maintaining high standards of protection of the data being transferred. Their introduction is expected to have a positive impact on the digital health sector by maintaining and creating trade opportunities with non-adequate countries, many of which are major players in the digital health sector such as China, North America, Australia, Brazil and India.

Conclusion

In light of the ongoing COVID-19 pandemic, the fallout of Brexit and the current economic climate, it is no wonder that there is an increased drive for the UK Government to promote data-driven innovation and ease the regulatory burden under which organisations currently operate. With the increased fiscal burden on the NHS, the use of data-driven technologies for healthcare purposes and scientific research looks set to continue.

The data protection regime and the use of data will therefore continue to play a pivotal role in shaping the development of digital healthtech. Individuals must have trust and confidence that their data will be processed in accordance with the data protection law framework. It is paramount for healthtech businesses, healthcare bodies and the UK Government to ensure that their legal and regulatory obligations are totally enshrined within their innovation processes at all stages and that appropriate steps are taken to stay abreast of the anticipated changes to the legal and regulatory landscape.

Acknowledgments

The authors are grateful to Johanna Saunders, Legal Director, and Annabelle Gold-Caution, Managing Associate, for their contributions to this chapter.

Endnotes

1. https://www.england.nhs.uk/coronavirus/publication/delivery-plan-for-tackling-the-covid-19-backlog-of-elective-care/.
2. https://www.england.nhs.uk/publication/next-steps-for-urgent-and-emergency-care/.
3. https://transform.england.nhs.uk/information-governance/guidance/virtual-wards/.
4. https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version.
5. https://www.theguardian.com/society/2022/oct/04/ai-eye-checks-can-predict-heart-disease-risk-in-less-than-minute-finds-study.
6. https://www.theguardian.com/society/2022/jul/31/exclusive-nhs-to-use-ai-to-identify-people-at-higher-risk-of-hepatitis-c.
7. https://www.theguardian.com/society/2022/apr/23/cancer-ai-tool-predicts-tumour-regrowth.
8. https://www.theguardian.com/society/2021/nov/21/from-oximeters-to-ai-where-bias-in-medical-devices-may-lurk.
9. https://www.cancer.ox.ac.uk/news/lack-of-data-available-to-detect-skin-cancer-in-darker-skin.
10. https://www.bbc.co.uk/news/health-58032842.
11. https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf.
12. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.
13. Article 71(3) of draft regulation 2021/0106/COD.
14. https://www.gov.uk/government/publications/national-ai-strategy.
15. https://ico.org.uk/media/about-the-ico/documents/4023338/ico-future-tech-report-20221214.pdf.
16. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf.
17. https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf.
18. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1085333/Government_response_to_consultation_on_the_future_regulation_of_medical_devices_in_the_United_Kingdom.pdf.
19. https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme.
20. https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap.
21. https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation.
22. https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf.
23. https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.
24. https://ico.org.uk/media/for-organisations/documents/4019534/scc-transitional-provisions.pdf.

Dr. Nathalie Moreno is a Data Protection and Cyber Security Partner at Addleshaw Goddard's London and Paris offices. She is a well-known and trusted adviser in the global privacy and data protection world, who brings 20 years of experience and extensive knowledge to European and global clients with a particular focus on the technology, healthcare and life sciences sectors. Nathalie's practice encompasses the full range of Data Protection, e-Privacy and Cyber Security issues including advisory, public policy advice to regulators and governments, transactional and pre-contentious advice in the areas of life sciences (pharma, biotech and medical devices) as well as health technology, technology-enabled healthcare, digital health services and mobile health (powered by AI, IoT and IoMT).

Addleshaw Goddard LLP
Milton Gate, 60 Chiswell Street
London, EC1Y 4AG
United Kingdom

Tel: +44 20 7160 3179
Email: nathalie.moreno@addleshawgoddard.com
URL: www.addleshawgoddard.com

Lydia Loxham is a Commercial and Privacy lawyer based in Manchester. She advises organisations on a range of commercial contract, cybersecurity and data issues in the digital, retail and consumer sectors. She is experienced in advising on, negotiating and drafting agreements for the provision of goods and services, distribution agreements and consumer terms. Her recent experience includes advising global service providers in relation to cross-border data transfers and advising businesses in the retail and consumer sector in relation to data protection and consumer law compliance.

Addleshaw Goddard LLP
One St Peter's Square
Manchester, M2 3DE
United Kingdom

Tel: +44 161 934 6202
Email: lydia.loxham@addleshawgoddard.com
URL: www.addleshawgoddard.com

Harriet Bridges is a Data Protection and Privacy lawyer based in London. She advises organisations in the digital, retail & consumer, and healthcare & life sciences sectors on a wide range of data protection issues, including policy drafting, regulatory compliance (including pharmaceutical, cybersecurity, e-Privacy and data protection) and international data transfers.

Addleshaw Goddard LLP
Milton Gate, 60 Chiswell Street
London, EC1Y 4AG
United Kingdom

Tel: +44 20 7160 5012
Email: harriet.bridges@addleshawgoddard.com
URL: www.addleshawgoddard.com

Emerging Trends in the Global Regulation of Digital Health: Fragmented Frameworks Aiming to Catch up with Technological Advancement


Eveline Van Keymeulen


Elizabeth Richards


Nicole Liffrig Molife


Oliver Mobasser

Latham & Watkins

Introduction/Overview

Technological advancements in the healthcare industry create an enormous opportunity to improve and transform healthcare delivery and access, reduce healthcare costs and advance public health as a whole. Digital health technologies have become more common, and are increasingly being used in new ways that are accessible to patients and providers alike. For example, these technologies have been used to impact how, where and when care is delivered to patients, such as through telehealth. They have also been used to expand patient access to clinical research opportunities through "decentralisation" of clinical trials, with remote monitoring of patients to capture health-related data at home. Advancements in digital health have also established new ways or mechanisms to document and transfer electronic health records and enable correspondence between providers. These technologies have improved the ability to predict or characterise sub-clinical signs of disease to assist providers in determining that their patients would benefit from earlier preventive care. Digital health technologies have also been used to promote general health and wellness, such as through mobile applications and wearables intended for everyday use. Consequently, digital health's applications are boundless and full of promise.

The explosion of these technologies, however, is tempered somewhat by the laws and regulations that were not developed with the advancements in digital health in mind. Governmental and regulatory authorities have thus had to grapple with balancing the strict application of their existing legal frameworks in a new world of digital health, while enabling continued advancement in the field. In this chapter, we discuss certain key legal constructs that digital health companies and investors must consider, and the emerging legal trends impacting applications of digital health in the United States ("US"), European Union ("EU") and United Kingdom ("UK").

Key Legal Constructs for Digital Health Companies

Medical device considerations

One of the key legal constructs that companies and investors in the digital health industry must consider is the framework applicable to medical devices across jurisdictions.

US

In the US, the Food and Drug Administration ("FDA") is the primary authority to regulate medical devices. The law defines a device to mean "an instrument, apparatus, implement, machine, contrivance, implant, *in vitro* reagent, or similar or related article, including any component, part, or accessory, which is" among other things, either "intended for use in the diagnosis of disease or other conditions or in the cure, mitigation, treatment, or prevention of disease" or "intended to affect the structure or any function of the body" and "does not achieve its primary intended purpose through chemical action" and is "not dependent on being metabolised to achieve that purpose".[1] Certain software functions that might otherwise fall within the scope of this broad definition are excluded by law from being regulated as a device. For example, in general, a software function intended for "maintaining or encouraging a healthy lifestyle and [that] is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition" will not be regulated as a device.[2]

With the exception of those software functions deemed to be shielded from the FDA's medical device oversight by statute as a matter of law, the law paints a broad brush; it sweeps many digital health technologies, including certain software – which may not traditionally be viewed as a "device" or "product" – within the FDA's reach. Because the medical device framework was established prior to the relatively recent advent of digital health technologies, it is not tailored to their intricacies and is often a poor fit. Indeed, the FDA and industry alike have recognised that the existing regulatory framework for medical devices can present a barrier to innovation and stifle or slow the potential for digital health technologies' use in improving public health.

To address this conundrum, the FDA has issued a variety of guidance documents and exercised flexibility in applying its regulatory scheme to this new class of technologies. For example, the FDA has issued guidance on software functions and mobile medical applications,[3] general wellness products[4] and clinical decision support software[5] in an effort to establish a clearer line between certain digital health technologies that are subject to FDA oversight and those that are not. In some cases, the FDA has applied a policy of enforcement discretion, noting that although the technology may technically constitute a medical device subject to FDA oversight, the FDA has declined to assert its medical device authority and requirements over such technologies. Consistent with its increased focus on digital health and the regulatory flexibilities these technologies require, in September 2020 the FDA announced the launch of its Digital Health Center of Excellence to "establish a comprehensive approach" to digital health technology to "set[] the stage for advancing and realizing the potential of digital health".[6]

The FDA has also engaged in a number of actions in recent years to address certain novel digital health technologies, including artificial intelligence and machine learning ("AI/ML")

in medical applications.[7] Specifically, the FDA has proposed the establishment of a new regulatory framework to enable a more flexible approach to regulating these technologies, which are designed to make real-time improvements after distribution and use. The FDA recognises that the existing regulatory framework, which was not constructed to account for the ever-changing nature of products using AI/ML technology, must be reworked to enable the technology's built-in ability to evolve, adapt and improve healthcare in the real world.

EU

Similarly, in the EU, regulatory authorities may consider digital health technologies to be regulated as devices, pursuant to Regulation (EU) 2017/745 on medical devices ("MDR") or Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices ("IVDR"). The MDR and IVDR clarify that software that is intended by the manufacturer to be used for one of the medical purposes listed in these regulations will be classified as a medical device or *in vitro* diagnostic medical device, respectively. These regulations could therefore capture many digital health solutions, including software incorporating AI when intended for use for medical purposes. As such, to be placed on the EU market, these solutions must be compliant with general safety and performance requirements as a prerequisite for European conformity, or "CE" marking, without which medical devices, including *in vitro* diagnostic medical devices, cannot be marketed or sold in the EU. To guide manufacturers, the Medical Device Coordination Group has issued guidance on the qualification and classification of software under the MDR and IVDR,[8] and the Manual on borderline and classification in the EU regulatory framework for medical devices contains many examples related to qualification of software and mobile applications.[9]

Today, more than 25% of medicines assessed by the European Medicines Agency ("EMA") incorporate a medical device component, which increasingly include digital technologies (such as "digital pills"). In a recent guideline, the EMA addressed the challenges related to the development of these combination products that use emerging technologies by recommending that developers engage with the relevant medicines authorities and notified bodies in a timely manner, e.g., by requesting formal scientific advice, or through an Innovation Office.[10]

As related to AI, on April 21, 2021, the European Commission published a proposal for what may become the world's first regulatory framework on AI ("AI Act"). The proposed AI Act would apply to AI in all sectors, including the health sector. Under the proposed AI Act, most AI systems that are part of medical devices and *in vitro* diagnostic medical devices, or are themselves such products, would be classified as high risk and require a conformity assessment by a notified body (e.g., a device, such as a pacemaker, that uses an AI system to identify the user's normal cardiological parameters and thus monitor the proper functioning of the patient's heart). As most software-based medical devices and *in vitro* diagnostic medical devices are already subject to conformity assessment by MDR- or IVDR-notified bodies, there is a possibility they would have to undergo a second conformity assessment procedure under the proposed AI Act, which could lead to increased cost, resources, documentation and regulatory scrutiny. In addition, such a requirement could create additional constraints for those notified bodies designated under the MDR and IVDR, which are already experiencing enormous backlogs. Given the overlap between the medical device and AI frameworks, further clarification is necessary to ensure that the proposed AI Act advances innovation in the digital health space, rather than stifles it.

UK

As a result of Brexit, the MDR and IVDR do not apply in Great Britain, though they are applicable in Northern Ireland pursuant to the Northern Ireland Protocol. On June 26, 2022, the UK Medicines and Healthcare products Regulatory Agency ("MHRA") published its response to a 10-week consultation[11] on the future regulation of medical devices in the UK. The aims of the consultation included exploring amendments to the current Medical Devices Regulations 2002 with a view to creating an innovative framework for regulating software and AI as medical devices. The new regime was originally scheduled to come into force in July 2023, but has recently been postponed to July 2024. For the most part, the proposed changes in many of these areas align with the new EU regime under the MDR and IVDR.

On October 17, 2022, the MHRA published guidance on "Software and AI as a Medical Device Change Programme – Roadmap",[12] a programme aiming to reform the regulation of these technologies and ensure that the regulatory requirements for software and AI are clear and that patients are protected. The programme consists of proposals to make key reforms across the lifecycle of these products, including qualification, classification, pre- and post-market requirements and cybersecurity.

As regulators in the US, EU and UK continue to refine their approaches to digital health technologies, including when and how such technologies should be regulated as medical devices, the legal and regulatory frameworks are likely to shift. This changing landscape can present difficulties for companies in the digital health industry when assessing the regulatory burdens that may apply across the lifecycle of their products and services. Furthermore, despite regulators' attempts to adapt to technological innovation in a flexible manner, future advancements in digital health may continue to outpace the legal frameworks, with regulators seemingly playing a constant game of catch-up.

Telehealth considerations

Digital health technologies that pertain to the delivery and use of telehealth to deliver care require a thorough evaluation of another set of healthcare regulatory laws outside of the FDA and comparable medical device regulations globally.

US

No uniform federal law governs the delivery of telehealth services. Instead, telehealth is regulated at state level, and digital health companies need to evaluate a patchwork of state laws to understand the restrictions that impact how healthcare providers and healthcare entities use technology, and how each step in the care delivery model can be structured to comply with varying state laws. Because state standards were developed when care was predominantly provided through in-person encounters, state laws lag behind innovation and do not fully contemplate the range of available technology that is changing the healthcare delivery model.

Each state has developed its own licensing requirements and standards governing: (i) the general practice of telehealth and the ability for remote delegation, supervision and prescribing; (ii) whether the delivery of care can be synchronous or asynchronous; and (iii) the scope of clinical care, coordination and management that can be delivered digitally. Specialty societies are stepping in to shape the standards of practice and spur policy discussion. For example, the American Medical Association ("AMA") has developed a Digital Health Implementation

Playbook[13] and has defined the concept of "augmented intelligence", focusing on AI's assistive functions.[14] The AMA has also proposed a policy on augmented intelligence, with the goal of advancing high-quality, clinically validated augmented intelligence in patient care.[15]

In addition, state licensing laws limit the geographic reach of licensed healthcare professionals ("HCPs") by requiring them to be licensed where the patient resides, unless the care was provided directly to another HCP (rather than to the patient) or in an emergency situation. The onset of the COVID-19 pandemic prompted states to temporarily loosen licensure restrictions on the practice of telehealth and apply waivers from these requirements, accelerating the use and acceptance of telehealth services and allowing HCPs to provide services to patients across state lines. However, many of the state waivers that were implemented during the pandemic have not been extended, resulting in a setback in the advancements in telehealth that were gained over the past few years. Efforts to reduce these licensure barriers continue, including state licensure compacts, such as the Interstate Medical Licensure[16] and Psychology Interjurisdictional Compact,[17] which are designed to streamline the licensing process for HCPs who wish to be licensed in multiple jurisdictions.

Lastly, leveraging technology to deliver remote care or augment an HCP's ability to diagnose and treat patients through AI implicates another set of laws, called state corporate practice laws. These laws generally prohibit lay, unlicensed entities from delivering healthcare or exercising undue influence or control over the delivery of healthcare services. These laws may require companies to implement certain corporate structures or safeguards to ensure that HCPs maintain unfettered control over clinical decision-making.

EU

The European Commission defines telehealth as "the provision of healthcare services, through the use of [information and communications technology], in situations where the health professional and the patient (or two health professionals) are not in the same location" and involves "secure transmission of medical data and information, through text, sound, images or other forms needed for the prevention, diagnosis, treatment and follow-up of patients".[18] As in the US, the regulation of telehealth services in the EU remains fragmented, as such services are essentially regulated at a national level. The most relevant effort to regulate health services across the EU is Directive 2011/24/EU on patients' rights in cross-border healthcare (the "Cross Border Healthcare Directive"), which ensures continuity of care for European citizens across borders (e.g., e-prescribing) and dates back many years.

A 2018 European Commission market study on telemedicine concluded that "most telemedicine solutions are deployed at the national or regional level" and that "this is due to the significant differences in national regulations and social security schemes".[19] The study recommended that "EU countries… harmonize their legal frameworks in order to make solutions compatible and to enable cross-border telemedicine practices".[20] The recent European Commission proposal for a Regulation on the European Health Data Space included provisions seeking to harmonise and encourage cross-border telemedicine,[21] but these provisions appear to have been removed by the European Council during the ongoing legislative process. While recent developments at the EU level in this space remain limited, it is worth noting that in November 2022, the World Health Organization ("WHO") issued a consolidated telemedicine implementation guide, which provides an overview of the key considerations for implementing telemedicine globally.[22]

UK

No specific laws govern telehealth in the UK. However, the provision of health or social care (including by remote means) in England is primarily governed by the Health and Social Care Act 2008 and the Health and Care Act 2022. Similar legislation covers Wales, Scotland and Northern Ireland. The Electronic Commerce (EC Directive) Regulations 2002 (the "eCommerce Regulations"), which impose certain requirements for the provision of online services, may also apply to the provision of telemedicine services.

The provision of health and social care is regulated on a regional basis by different agencies. For example, in England, the Care Quality Commission ("CQC") regulates telehealth providers under the regulated activity of "transport services, triage and medical advice provided remotely". Telemedicine service providers (including individuals or corporate entities) are required to register with CQC or the equivalent body in Scotland, Wales or Northern Ireland.

While these regulators have authority over healthcare service providers (i.e., the individual or the entity), individual providers are also subject to licensing and enforcement by their professional bodies. In particular, the General Medical Council has licensing and enforcement authority in respect of doctors, and the General Pharmaceutical Council has such authority in respect of pharmacists. The obligation to be appropriately qualified and registered with a professional governing body applies regardless of whether the service is provided remotely or in person. As a result of Brexit, the "country-of-origin" principle under the eCommerce Regulations – which allow European Economic Area ("EEA") online service providers to operate in any EEA country, while only following relevant rules in the country in which they are established – and the rules on cross-border care from the Cross Border Healthcare Directive no longer apply. This means that professionals providing telemedicine services from the UK to patients in the EEA may also need to be licensed in the country where the patient is located.

Coverage and reimbursement considerations

Beyond the legal considerations applicable to compliance of digital health technologies with the medical devices framework and telehealth restrictions and requirements, companies must consider the laws and regulations applicable to coverage and reimbursement for their digital health technologies, or coverage and reimbursement of healthcare services provided using digital health technologies.

US

Coverage and reimbursement for health services that use digital health technologies (like telehealth) are often determined on a payor-by-payor basis, which can make it difficult for companies to navigate the payor landscape and achieve certainty with respect to payor adoption of their technologies. While the US does not have a single payor system that establishes uniform reimbursement and coverage for healthcare services that use digital health technologies, policies established by the Centers for Medicare & Medicaid Services ("CMS") – which administers Medicare, the nation's single largest public insurance programme – are particularly important because they often influence coverage and payment policies adopted by other payors.

In recent years, CMS has expanded coding and payment policies for remote monitoring services, allowing for increased flexibility with respect to the types of patients who are eligible for remote monitoring and the level of physician supervision required in order for clinical and auxiliary personnel to perform

remote monitoring services. However, several Medicare Administrative Contractors ("MACs") recently announced that they are convening a Contractor Advisory Committee ("CAC") in February 2023 to evaluate "the strength of published evidence on remote physiologic monitoring ("RPM") and remote therapeutic monitoring ("RTM") for non-implantable devices, and that they are seeking compelling clinical data to assist in defining meaningful and measurable patient outcomes (e.g., decreases in emergency room visits and hospitalisations)" for Medicare beneficiaries.[23] Although not binding on the MACs, the CAC's assessment could result in the adoption of additional coverage limitations for RPM and RTM services, which could limit the use and adoption of these services for certain segments of the population.

In addition, Congress and various federal and state agencies have continued to provide expanded flexibilities to enable coverage and reimbursement for telehealth services during the declared COVID-19 public health emergency ("PHE"), including policies allowing certain telehealth services to be reimbursed at the same rate as equivalent in-person services. While some of these flexibilities have been extended through the end of 2024,[24] others are expected to terminate when the COVID-19 PHE ends. The explosion of telehealth and digital health offerings in the US healthcare system as a result of these policies has been paralleled by an increasing number of enforcement actions, scrutiny by federal regulators and the issuance of a special fraud alert around the use of telehealth services.[25] It is important that digital health companies stay abreast of this increased regulatory scrutiny, and the evolving regulatory scheme, as they structure their operations.

EU

The reimbursement landscape for digital health tools is fragmented across the EU, given that reimbursement decisions are made at a national or even regional level, and not by EU authorities. This poses particular challenges to both the manufacturers that are developing digital health technologies and the health authorities that are evaluating them. In particular, these authorities' traditional methods to evaluate products for coverage and reimbursement do not focus on aspects that are relevant to digital health technologies (e.g., interoperability, privacy, data security and ethical considerations). Moreover, because these technologies are often updated more quickly than traditional devices (especially when incorporating AI/ML), they require similarly speedy evaluation decisions. As a consequence, national reimbursement schemes for digital health technologies are inconsistent across the EU, including with respect to the type of evidence that is accepted as sufficient, and little guidance is available to assist manufacturers in navigating the requirements. Certain countries have implemented specific frameworks for reimbursement decisions with respect to digital health technologies. Germany, for instance, is the first EU country to have recently implemented a "fast track" reimbursement for certain digital medical products, such as wearable devices or mobile applications.

The EU Health Technology Assessment ("HTA") Regulation (2021/2282), which for the first time introduces a permanent legal framework for joint HTA work (i.e., joint clinical assessments and scientific consultations) by EU member states, is an important step toward a more uniform assessment of innovative high-risk medical devices, including digital health technologies. In preparing for the regulation's phased implementation from 2025 onwards, several national HTA bodies in Europe have recently joined forces with EU-level organisations, such as the European Network for HTA, to develop recommendations on harmonised evaluation guidelines for digital medical devices. For instance, in October 2022, a European taskforce was launched by nine EU Member States with the objective to reach a mutual understanding between national HTA agencies for digital medical devices in order to harmonise assessment criteria and clinical evidence requirements and improve access to digital health technologies in the EU.[26]

UK

The National Health Service ("NHS") funds the majority of digital health products and services provided to patients in the UK. In addition, there exists a smaller, but growing, private healthcare sector, which is funded through private insurance or directly by patients. There are a number of routes for products to be made available for reimbursement by the NHS, including selling directly to NHS trusts or primary care organisations, or procurement through the NHS supply chain or public tenders. In addition, digital health products can undergo a technology appraisal from the National Institute for Health and Care Excellence ("NICE"), and the NHS is obligated to fund and resource treatments recommended by NICE.

The NHS has published a "guide to good practice for digital and data-driven health technologies",[27] which is designed to help innovators understand the NHS requirements when the NHS buys digital and data-driven technology. NICE has published the "Evidence standards framework for digital health technologies",[28] which describes the standards for digital health technologies to demonstrate their value in the UK healthcare system.

Data privacy and data use

Data and digital health go hand-in-hand, whether they involve the analysis of large and complex datasets by an AI/ML tool or the collection of an individual's health and lifestyle data through a wearable device. As such, navigating the complex and continually evolving web of privacy and cybersecurity laws is critical to the deployment of any digital health solution.

US

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regulates the use and disclosure of sensitive health information. Specifically, the HIPAA requires certain "covered entities" to comply with privacy and security requirements, including providing notice of how an individual's protected health information ("PHI") will be handled as well as the statutory rights patients hold in relation to the handling of their PHI.

The data protection landscape is rapidly growing and evolving on a state level. For example, the California Consumer Privacy Act of 2018 requires companies that process information on California residents to make certain disclosures to consumers about their data collection, use and sharing practices. The law also allows consumers to opt out of certain data sharing with third parties and exercise certain individual rights regarding their personal information, providing a new private right of action for data breaches and penalties for noncompliance. In addition, the California Privacy Rights Act was recently passed and will impose additional data protection obligations on covered businesses, including additional consumer rights processes, limitations on data uses, new audit requirements for high-risk data and opt-outs for certain uses of sensitive data. Similar laws have been passed in Virginia, Colorado, Connecticut and Utah and have been proposed in other states and at federal level, reflecting a trend toward more stringent privacy legislation in the US.

Furthermore, the Federal Trade Commission ("FTC") and many state Attorneys General continue to enforce federal and

state consumer protection laws against companies for online collection, use, dissemination and security practices that appear to be unfair or deceptive. Recent FTC guidance on AI/ML has focused on the potential risks to fair and transparent consumer transactions represented by opaqueness in automated decision-making and predictive analytics. The FTC is also concerned about misleading representations to consumers regarding a company's data collection and handling practices that underwrite the data sets on which algorithms are trained. The FTC has highlighted the particular risks to healthcare consumers in unfair or deceptive data practices leveraging AI as an area of developing regulatory concern. Of particular relevance to the digital health sector are potential harms to patients introduced as a result of improper oversight when AI tools are used for automated decision-making, leading to discriminatory clinical or treatment outcomes.

EU

In the EU, the processing of personal data is primarily governed by Regulation (EU) 2016/679 ("GDPR"). The GDPR imposes comprehensive data-privacy compliance obligations in relation to the use or "processing" of information relating to an identifiable living individual or "personal data". The GDPR applies not only to entities established in the EU, but also to entities established outside the EU if they offer goods or services to EU individuals or monitor their behaviour. Organisations deploying digital health solutions to individuals across the EU and the UK may therefore need to comply with both the GDPR and the UK data protection regime. While the GDPR was intended to harmonise data protection laws across the EU, national implementing laws diverge in certain areas, such as the processing of personal data for public health or scientific research purposes. Therefore, companies must navigate not only the GDPR, but also national implementing and supplementary legislation as well as legal, ethical and professional rules designed to protect patient confidentiality.

Although the GDPR was enacted to be technology-neutral, the advent of the digital health industry has led to challenges in the interpretation and application of the GDPR. For example, some digital health applications such as wearables have led to questions on the distinction between health data (which is considered "special-category data" under the GDPR and subject to enhanced protections) and other non-health "lifestyle" data. This distinction, in turn, leads to potential compliance challenges, such as identifying appropriate legal bases for processing such health data and other personal data under the GDPR and ensuring that individuals are adequately informed of the processing of their data.

Other applications of digital health, such as AI/ML algorithms, have raised difficult questions regarding transparency and how data subjects can be informed in easy-to-understand terms of how the algorithm processes their data. Where personal data has been used to train an algorithm, withdrawal of a subject's consent (where consent has been used as the legal basis for such processing) to limit further use of their data may not be practical or possible and could affect the integrity of the algorithm. In such cases, the developer will need to consider whether it can continue to legitimately use that data, such as whether it has been effectively anonymised or aggregated. Ensuring data accuracy and the absence of bias are also key considerations for these types of tools.

Another increasingly tricky area for digital health operators is in relation to international data transfers. Where personal data are transferred from the EU to a country that is not considered to provide an "adequate" level of protection for the data, such transfer is prohibited unless a relevant derogation applies or certain safeguards are implemented. Recent legal developments in the EU have created complexity and uncertainty regarding such transfers, particularly in relation to transfers to the US.[29] The shifting sands of data transfers can be difficult to navigate and companies must pay close attention to the complex data flows that are often involved in digital health solutions.

Many digital health solutions, such as wearables and apps, may use cookies or other tracking technologies. While cookies that are strictly necessary for the device, site or app to function correctly can be used without opt-in consent, others such as analytics or advertising trackers will require specific opt-in consent under EU Directive 2002/58/EC ("ePrivacy Directive") and national implementing laws, which may not be straightforward depending on the nature of the device. User data collected from devices is also subject to the GDPR. The use of cookies, tracking technologies and user profiling is subject to increasing regulatory scrutiny and enforcement, particularly around the use of individuals' data for marketing and advertising.

Beyond the general requirements to ensure the security of personal data in the GDPR, there is a trend toward increasing regulation of cybersecurity through sector-specific or device-specific rules. For example, the MDR requires the manufacturing of certain devices to take into account information security principles. In addition, on November 28, 2022, the EU adopted Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU ("NIS-2 Directive"). The NIS-2 Directive establishes cybersecurity risk-management measures and reporting requirements for critical sectors, including manufacturers of medical devices. The draft EU Cyber Resilience Act also proposes a framework of consistent security standards for digital products, applicable through the whole product lifecycle.

In parallel with the trend toward increased regulation and scrutiny, there is a trend toward enabling greater sharing and reuse of data, particularly for research and innovation. For example, on May 3, 2022, the European Commission launched its proposal for a Regulation for the European Health Data Space to "unleash the full potential of health data", facilitating the systematic digitisation of health records and secondary use of clinical data for research purposes. In addition, the proposed EU Data Act, which seeks to regulate the sharing and use of data generated by connected devices, would include new rights for users of connected services, introduce data portability obligations, impose restrictions on the use of user data and regulate data sharing contracting.

Across the EU, there is a trend toward increasing enforcement of data protection laws and ever-larger fines. There is also increasing scrutiny and enforcement from a broader range of regulators – including data protection regulators, consumer protection authorities and competition regulators – and increasing coordination efforts around data and digital platforms.

UK

Following Brexit, the GDPR has been mirrored in UK law as the "UK GDPR", which together with the Data Protection Act 2018 form the UK's data protection regime. The UK Information Commissioner's Office has introduced specific data-transfer mechanisms to safeguard transfers of data out of the UK, namely the International Data Transfer Agreement and the International Data Transfer Addendum to the EU's standard contractual clauses.

The UK government has proposed wide-ranging reforms to UK data protection laws, set out in the UK Data Protection and Digital Information Bill (which was introduced to Parliament in July 2022). The bill largely maintains the GDPR framework in UK law, albeit with modifications reflecting the government's intention to move away from prescriptive requirements and

toward a more risk-based approach. While the UK has signalled a more business-friendly and flexible approach, which would be welcomed by operators in the digital health sector, it remains uncertain where the post-Brexit UK privacy landscape will land.

On June 29, 2022, the UK government published a policy paper titled "A plan for digital health and social care",[30] which sets out its far-reaching plans for the digital transformation of health and social care in England. The plan includes proposals for the systematic digitisation of health and social care records, and the creation of a life-long health and social care record. The proposal also aims to equip the NHS with the capacity to develop image-sharing and other technical capabilities based on AI, to enable "digitally-supported diagnoses" and to establish a network of trusted research environments to support research and development.

Conclusion

Digital health companies must stay attuned to the emerging trends in the global regulation of these technologies, with the recognition that the frameworks are continuing to evolve. As demonstrated in the US, EU and UK, a myriad of legal requirements create a spider's web for companies and investors to carefully navigate in order to avoid compliance issues and maintain momentum in a competitive marketplace. By remaining aware of the key legal constructs and staying abreast of proposed changes in these frameworks, stakeholders can play a part in shaping the legal regimes applicable to their digital health solutions. Moreover, they can reduce the risk of a compliance misstep, which may be more likely in an industry in which technological advancements outpace the legal frameworks and innovators, in many cases, operate in uncharted territory under the law.

Endnotes

1. 21 U.S.C. § 321(h)(1) (2022).
2. *Id.* § 360j(o).
3. U.S. Food & Drug Admin. (FDA), Policy for Device Software Functions and Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff (2022), https://www.fda.gov/media/80958/download.
4. U.S. FDA, General Wellness: Policy for Low Risk Devices: Guidance for Industry and Food and Drug Administration Staff (2019), https://www.fda.gov/media/90652/download.
5. U.S. FDA, Clinical Decision Support Software: Guidance for Industry and Food and Drug Administration Staff (2022), https://www.fda.gov/media/109618/download.
6. U.S. FDA, *Digital Health Center of Excellence*, https://www.fda.gov/medical-devices/digital-health-center-excellence (last visited Jan. 21, 2023); U.S. FDA, *About the Digital Health Center of Excellence*, https://www.fda.gov/medical-devices/digital-health-center-excellence/about-digital-health-center-excellence (last visited Jan. 21, 2023).
7. *See, e.g.,* U.S. FDA, *Artificial Intelligence and Machine Learning in Software as a Medical Device*, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device (last visited Jan. 29, 2023).
8. Med. Device Coordination Group (MDCG), Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR (2019), https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf.
9. Eur. Comm'n, Manual on Borderline and Classification in the EU Regulatory Framework for Medical Devices (2022), https://health.ec.europa.eu/latest-updates/manual-borderline-and-classification-community-regulatory-framework-medical-devices-september-2022-2022-09-07_en.
10. European Medicines Agency (EMA), Guideline on Quality Documentation for Medicinal Products When Used with a Medical Device (2021), https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-quality-documentation-medicinal-products-when-used-medical-device-first-version_en.pdf.
11. Medicines and Healthcare Regulatory Products Regulatory Agency (MHRA), Consultation on the Future Regulation of Medical Devices in the United Kingdom (2021), https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom.
12. MHRA, Software and AI as a Medical Device Change Programme – Roadmap (2022), https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap.
13. American Medical Association (AMA), *Digital Health Implementation Playbook Series*, https://www.ama-assn.org/practice-management/digital/digital-health-implementation-playbook-series (last visited Jan. 30, 2023).
14. AMA, *Augmented Intelligence in Medicine*, https://www.ama-assn.org/practice-management/digital/augmented-intelligence-medicine#:~:text=The%20AMA%20House%20of%20Delegates%20uses%20the%20term%20augmented%20intelligence,intelligence%20rather%20than%20replaces%20it (last visited Jan. 30, 2023).
15. AMA, *Policy: Augmented Intelligence in Health Care*, https://www.ama-assn.org/system/files/2019-08/ai-2018-board-policy-summary.pdf (last visited Jan. 30, 2023).
16. Interstate Medical Licensure Compact, https://www.imlcc.org/ (last visited Jan. 30, 2023).
17. Psychology Interjurisdictional Compact (PSYPACT), https://psypact.org/page/About (last visited Jan. 30, 2023).
18. Eur. Comm'n, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Telemedicine for the Benefit of Patients, Healthcare Systems and Society (2008), COM(2008)0689 final, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008DC0689.
19. Eur. Comm'n, Market Study on Telemedicine (2018), https://health.ec.europa.eu/system/files/2019-08/2018_provision_marketstudy_telemedicine_en_0.pdf.
20. *Id.*
21. Eur. Comm'n, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (2022), COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197 (The original Article 8 set out that: "If a Member State accepts the provision of telemedicine services, it shall, under the same conditions, accept the provision of similar services by healthcare providers located in other Member States.").
22. World Health Org. (WHO), Consolidated Telemedicine Implementation Guide (2022), https://www.who.int/publications/i/item/9789240059184 (last visited Jan. 26, 2023).

23. CGS Medicare, *Multi-Jurisdictional Contractor Advisory Committee (MJCAC) Meeting Regarding Remote Physiologic Monitoring (RPM) and Remote Therapeutic Monitoring (RTM) for Non-Implantable Devices on February 28th, 2023 – 6:00 – 8:00 PM ET* (Nov. 10, 2022), https://www.cgsmedicare.com/partb/pubs/news/2022/11/cope3231.html (last visited Jan. 30, 2023).
24. Consolidated Appropriations Act, 2023, H.R. 2617, 117th Cong. (2022).
25. Office of Inspector General, U.S. Dept. of Health and Human Services (HHS), Special Fraud Alert: OIG Alerts Practitioners To Exercise Caution When Entering Into Arrangements With Purported Telemedicine Companies (2022), https://oig.hhs.gov/documents/root/1045/sfa-tele-fraud.pdf.
26. Haute Autorité de Santé (HAS), Towards a European Evaluation Framework for Digital Medical Devices (DMDs) in the European Union — Launch of a European Taskforce (2022), https://www.has-sante.fr/jcms/p_3382241/en/towards-a-european-evaluation-framework-for-digital-medical-devices-dmds-in-the-european-union-launch-of-a-european-taskforce (last visited Jan. 26, 2023).
27. Dept. of Health and Social Care (DHSC), U.K. Nat'l Health Serv., A Guide to Good Practice for Digital and Data-Driven Health Technologies (2021), https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (last visited Jan. 30, 2023).
28. Nat'l Inst. for Health and Care Excellence (NICE), Evidence Standards Framework for Digital Health Technologies (2022), https://www.nice.org.uk/about/what-we-do/our-programmes/evidence-standards-framework-for-digital-health-technologies (last visited Jan. 30, 2023).
29. In March 2022, the US and EU announced a new regulatory regime intended to replace the invalidated Privacy Shield; however, this new EU-US Data Privacy Framework has not been implemented beyond an executive order signed by President Biden on October 7, 2022 (Administration of Joseph R. Biden, Jr., 2022 Executive Order 14086-Enhancing Safeguards for United States Signals Intelligence Activities, Daily Comp. Pres. Docs. 1 (2022)).
30. DHSC, U.K. Nat'l Health Serv., A Plan for Digital Health and Social Care (2022), https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care/a-plan-for-digital-health-and-social-care (last visited Jan. 30, 2023).

Eveline Van Keymeulen advises multinational companies and start-ups in the pharmaceutical, biotech, medical devices and digital health sectors on a broad variety of complex European, domestic and cross-border regulatory matters, including clinical trials, product approvals, regulatory incentives, market access, promotion and advertising, post-market obligations and general compliance matters. Eveline is widely recognised for her regulatory life sciences expertise by *Chambers* (2020–2022), *The Legal 500* (2018–2022) and *Who's Who Legal Life Sciences* (2016–2022). She was voted European "Advisory Lawyer of the Year" by *LMG Life Sciences* (2021) and won their "Impact Case of the Year" award (2021–2022) for her work in the groundbreaking CJEU Kanavape case, for which she equally received the *Financial Times* European Innovative Lawyer Award (2022).

Latham & Watkins
Boulevard du Régent, 43–44
Brussels, B-1000
Belgium

Tel: +32 2 788 6000 / +33 1 4062 2060
Email: eveline.vankeymeulen@lw.com
URL: www.lw.com

Elizabeth Richards advises clients in all facets of oversight and regulation by the FDA, helping clients navigate regulatory frameworks governing the digital health and medical device, pharmaceutical, biotechnology, food, dietary supplement and cosmetic industries. She is attuned to her clients' business objectives while guiding them through compliance, enforcement, transactional and legislative matters, traversing the legal labyrinth required to bring new products to market and maintain compliance once commercialised. Her practice spans all stages of the product life cycle, and she has been recognised as a leading industry lawyer by multiple publications, including *Chambers USA*, *The Legal 500 US*, *LMG Life Sciences* and *The Diversity Journal*.

Latham & Watkins
555 Eleventh Street, NW, Suite 1000
Washington, D.C., 20004
United States

Tel: +1 202 637 2130
Email: elizabeth.richards@lw.com
URL: www.lw.com

Nicole Liffrig Molife advises emerging companies as well as commercial companies in the digital health, pharmaceutical, medical device and technology sector. She leverages her deep knowledge of fraud and abuse laws as well as telehealth and other healthcare regulatory laws to guide companies as they develop their product development and launch strategies and business models, providing solutions that mitigate regulatory risk while fostering innovation. Nicole's practice includes counselling on sales and marketing activities and relationships with referral sources, evaluating industry collaborations, structuring key commercial agreements at all stages of development and advising on life sciences transactions.

Latham & Watkins
555 Eleventh Street, NW, Suite 1000
Washington, D.C., 20004
United States

Tel: +1 202 637 2121
Email: nicole.liffrig@lw.com
URL: www.lw.com

Oliver Mobasser has particular expertise in the healthcare and life sciences sectors, advising multinational pharmaceutical, biotechnology and medical technology companies and their investors on complex licences, collaborations, acquisitions, divestments, commercial contracts, intellectual property matters and regulatory and privacy matters. Oliver's experience covers: product licensing and acquisitions; complex commercial contracts and collaborations; technology and life sciences transactions; business carve-out transactions; digital health; and data protection.

Latham & Watkins
99 Bishopsgate
London, EC2M 3XF
United Kingdom

Tel: +44 20 7710 4738
Email: oliver.mobasser@lw.com
URL: www.lw.com

Hospital Innovation Pathways in the USA, UK, Germany and France


Stephen Hull


Gilles Launay


Kirstin Ostoff


Louise Cresswell

Hull Associates LLC

Abstract/Synopsis

It has been well established that specialty pharmaceuticals, which grew to represent over 70% of non-retail drug spending by 2021, are a rapidly growing cost driver of US healthcare (ASPE, Sept. 2022). Specialty drug spending from 2016 to 2021 increased by 43%, despite only a 0.5% increase in the number of prescriptions (ASPE, 2022). In part, this shift may coincide with greater numbers of physician-administered therapies for rare and difficult-to-treat diseases. Analyses of US drug spending on inpatient drugs have found that annual spending increased by almost 10% per hospital admission from 2015 to 2017 (NORC, 2019).

But are the systems of reimbursement for inpatient care designed to address these costs? Because many hospital environments are reimbursed via bundled payment methods, innovator companies selling to hospitals must address a completely different set of challenges from those selling prescription pharmaceuticals – in particular, previously determined fixed payments for hospital stays, and in some markets, capped annual budgets that limit overall spending on such products.

Globally, the most common type of hospital payment is the Diagnosis-Related Groups (DRG) system which pays a predetermined amount for an entire patient discharge, which reflects the primary diagnoses and procedures provided to the patient. However, DRG systems create disincentives for adoption of new therapies and diagnostics since hospitals often cannot cover their additional costs. Starting with the USA in 2000, special pathways to address the high additive costs of new innovative drugs were developed in a number of DRG payment systems (106th Congress, 2000).[1] England, Germany and France all subsequently implemented systems of add-on payment for certain inpatient innovations as part of their DRG-type systems.

Drugs that achieve supplemental payment are often indicated for rare or severe diseases. However, different requirements and lack of transparency in health technology assessments (HTAs) for these products varies by country, which can lead to delays in reimbursement and patient access to new drugs (Akehurst, 2017).[2]

This chapter describes the special pathways established for high-cost, inpatient specialty drugs in the USA, Germany, France and England, along with recent developments that directly impact the evidence portfolios that manufacturers need to anticipate to succeed in today's markets.

Country	Inpatient Reimbursement System	Mechanism for New Innovation Payment
Germany	Inpatient: G-DRG System	"NUB" Innovation Clause, ZE Supplements
France	Inpatient: GHS System	*Liste en Sus*, add-on payment for drugs
England	Inpatient/ Outpatient: HRGs	High-Cost Drugs List, Cancer Drugs Fund
USA	Medicare: DRGs Commercial: DRGs, *Per Diem*, Discounted Charges	Medicare: New Technology Add-on Payment (NTAP) Commercial: Negotiated rates

USA Reimbursement Schemes – Inpatient Hospital Setting

Medicare

In the USA, the cost of Medicare inpatient care is covered by a patient's DRG payment for each admission in over 3,000 hospitals nationwide (Centers for Medicare & Medicaid Services, 2020).[3] Because DRGs pay for admissions with a pre-determined, bundled payment that is calculated using the prior year's data, there is a time lag in the update to payments for new innovations. Hence, new innovations may struggle to gain adoption until DRG payment rates for admissions reflect the added costs of the drug. For small-volume therapies, it is quite possible the DRG rates for large-volume conditions will never adjust sufficiently to compensate their costs.

Section 533 of the Medicare, Medicaid and SCHIP Benefits Improvement and Protection Act of 2000 (BIPA) mandated that Medicare implement an add-on payment to adequately cover the costs of new innovations introduced in the hospital setting (106th Congress, 2000).[4] The core concept of the USA legislation was to create a bridge for promising innovations to receive an add-on to the DRG payment, while Medicare collected data on the overall costs of admissions so it could then make a permanent assignment to an appropriately paying DRG.

While the original statute required Medicare to pay additionally for qualified new drugs, it did not specify the exact criteria

for eligibility. This was refined in 2001 when the Centers for Medicare & Medicaid Services (CMS) used its authority under the statute to provide the process and criteria for new technology add-on payments (NTAP) (Centers for Medicare & Medicaid Services, 2001).[5] Additional modifications to the statute were implemented under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) which amended the NTAP criteria (Medicare Modernization Act, 2003).[6] The current eligibility criteria are:

1. the technology or drug uses the same or a similar mechanism of action when compared to existing technology to achieve a therapeutic outcome;
2. the technology or drug has been assigned to the same Medicare Severity Diagnosis-Related Group (MS-DRG) when compared to an existing technology to achieve a therapeutic outcome; and
3. the new use of the technology or drug involves the treatment of the same or similar type of disease and patient population when compared to an existing technology or drug. (Centers for Medicare & Medicaid Services, 2023.)[7]

"New" under CMS rules means within two to three years following market introduction (Centers for Medicare & Medicaid Services, 2001).[8] Drugs that are considered substantially similar to older technologies are not considered new (Centers for Medicare & Medicaid Services, 2010).[9]

Cost thresholds for each MS-DRG are published annually in each year's Inpatient Prospective Payment System (IPPS) final rule. Demonstrating inadequate payment involves a formula for the applicable DRG cost thresholds. This formula is the geometric mean plus the lesser of 0.75 of the national adjusted operating standardised-payment amounts (increased to reflect the difference between cost and charges) or 0.75 of one standard deviation of mean charges by MS-DRG. (Centers for Medicare & Medicaid Services, 2023.)[10]

Determining substantial clinical improvement under the Medicare definition can be complex. Drugs are considered eligible if:

1. The drug offers a treatment option for a patient population unresponsive to, or ineligible for, currently available treatments.
2. The drug offers the ability to diagnose a medical condition in a patient population where that medical condition is currently undetectable or offers the ability to diagnose a medical condition earlier in a patient population than allowed by currently available methods. There must also be evidence that the use of the new medical service or drug to make a diagnosis affects the management of the patient.
3. The use of the new medical service or drug significantly improves clinical outcomes relative to services or technologies previously available. (Centers for Medicare & Medicaid Services, 2023.)[11]

Applicants must submit data to CMS verifying that the average charge per case exceeds the MS-DRG cost threshold. CMS makes add-on payments only for individual cases that are more costly. The payment caps for traditional NTAP-approved drugs currently are the lesser of:

1. sixty-five per cent of the cost of the new drug; or
2. sixty-five per cent of the excess cost compared to the standard DRG payment. (Centers for Medicare & Medicaid Services, 2023.)[12]

Other Medicare special add-on payment pathways

NCTAP is a new technology add-on payment made available to COVID-19-specific products to help mitigate the public health emergency. To receive this reimbursement, the drug must be FDA approved or be authorised by the FDA for emergency use. CMS has set an NCTAP-eligibility threshold amount equal to the lesser of: (1) 65% of the operating outlier threshold for the claim; or (2) 65% of the amount by which the costs of the case exceed the standard DRG payment, including the adjustment to the relative weight under section 3710 of the CARES Act. As with the new technology add-on payment and outlier payments, the costs of the case are determined by multiplying the covered charges by the operating cost-to-charge ratio. The cost of the hospitalisation should exceed the MS-DRG payment including a 20% COVID-19 adjustment as was set forth in the CARES Act. (Centers for Medicare & Medicaid Services, 2023.)[13]

In 2020, CMS established an alternative pathway for NTAP approval for a special class of anti-microbial drugs designated by the FDA as a Qualified Infectious Disease Product (QIDP) (Department of the Treasury, Department of Labor, Department of Health and Human Services, 2021).[14]

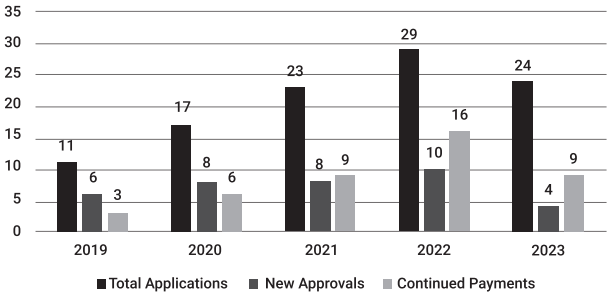
QIDPs are antibacterial or antifungal drugs for human use intended to treat serious or life-threatening infections, including those caused by antibacterial- or antifungal-resistant pathogens, including novel or emerging infectious pathogens, or any qualifying pathogens listed by the US Secretary of Health and Human Services (HHS) (United States House of Representatives, 2020).[15]

Under this alternative NTAP pathway, products given a QIDP designation by the FDA will be considered new and not substantially similar to an existing technology for purposes of NTAP payment under the IPPS, and will not need to meet the previously defined "newness" criterion that it represents an advance that substantially improves, relative to technologies previously available (Centers for Medicare & Medicaid Services, 2019).[16]

Key trends under the NTAP

As the NTAP legislation begins its third decade, there is debate as to its impact. In 2023, four out of five drug-related applications were approved. This compares with 10 approvals out of 13 applications in 2022, and in 2021 five out of nine applications were approved. In the past five years, the greatest awarded add-on payment was $289,533 to CARVYKTI and ABECMA.

Applications and Approvals for New Technology Add-on Payments (Drugs Only), United States FY 2019–2023



Medicaid

Medicaid reimbursement of hospital care varies by state, with some states applying a bundled, DRG system known as the All Patient Refined - Diagnosis-Related Groupings (APR-DRG) and others relying on a *per diem* or fee-for-service model (Henry J Kaiser Family Foundation, 2012).[17]

Each state government determines the amount of payment. Unlike commercial or Medicare plans, the payments are often considered to be below the cost of care (Reinhardt, 2009).[18]

Alongside the system of reimbursement for hospitals is the outpatient 340b drug-discounting program, which provides hospitals access to discounted drugs for low-income patients.

This program has been criticised as providing hospitals with undue financial margins, without any mandate to pass on savings to patients (US Government Accountability Office, 2011).[19] Hence, it may help hospitals adjust to disproportionately low Medicaid payments, but it does not help support manufacturer introductions of innovations in that setting.

Private commercial payers

Under commercial plans, payment for inpatient pharmaceuticals can also be bundled with no separate payment, although generally commercial payment rates are higher than Medicare rates. Private payers may utilise the APR-DRG, developed by 3M Health Information Systems and the Children's Hospital Association. A 2022 report estimates that 31 states currently use APR-DRGs. (Augenbaum, 2022.)[20]

The system of discounted charges has been criticised for providing hospitals with excessive margins for dispensing and prescribing drugs, both physician administered and prescription. One study found that on average, hospitals charge double the price for drugs also available in pharmacies. (AHIP, 2022.)[21]

Thus, the commercial payer methods of reimbursement may provide revenue that helps offset losses for the same drugs used for other patients whose DRG-based reimbursement is insufficient and shifts risk for the drug costs onto the hospital. The net impact of these two very different systems of payment regularly leads to the phenomena of "cost shifting" within hospitals, where the revenue for certain commercially insured patients helps to balance a hospital's books for capped reimbursement under DRG systems, both public and private.

The French *Liste en Sus* and Hospital Finding

In France, the High Authority on Health (*Haute Autorite de Sante*, HAS) review pathway is mandatory for hospital use of all new drug products. Manufacturers must submit a clinical dossier to the HAS Transparency Committee, which analyses the severity of the pathology, the drug efficacy, the side effects and positioning.

The HAS applies an evidence review process and assigns an appraisal of "Medical Services Rendered" (SMR) and "Improvement to Medical Services Rendered" (ASMR).

SMR reflects the seriousness of the pathology for which the drug is indicated and the effectiveness of the drug with regard to the objectives pursued. SMR is written for drugs at the time of the review, which can be confirmed, upgraded or downgraded for old drugs according to available clinical studies. New drugs also receive a rating (major/important, moderate/low, insufficient).

ASMR is an assessment of the added value of the drug as compared to a reference treatment. It measures the medical added value of the medicine – notably in terms of efficacy or safety. It may be rated major (ASMR level I), substantial (ASMR level II), moderate (ASMR level III), minor (ASMR level IV) or no improvement (ASMR level V), with the latter level corresponding to no therapeutic progress.

Access to reimbursement requires an evaluation by the HAS. The HAS evaluates the SMR and ASMR scores at the time of the first request for reimbursement and then every five years. This can be shortened if the HAS requests, for example, the launch of the results within a period of less than five years. If a manufacturer would like to request an evaluation for an additional indication, they must enter the five-year cycle or file a dossier before the date for the reevaluation.

It should be noted that in the absence of a request for reimbursement, drugs are not evaluated by the HAS. For drugs that are evaluated, a cost-effectiveness evaluation is conducted if expected drug sales are over €20 million a year. That economic evaluation is conducted by the CEESP (the *Commission d'Evaluation economique de santé Publique*) will likely be required.

If the HAS review is positive, the drug can either be listed on the list for community use (*Homologation assurés sociaux*) and/or on the list for hospital drugs (*Homologation collectivité*).

Finally, to determine the reimbursement amount, the *Comité économique des produits de santé* (CEPS), will review the economic dossier provided by the manufacturer:

- The CEPS will negotiate the tariff with the manufacturer. (Budget impact models are critical.)
- The CEPS will make a recommendation for registration of the drug on the *Liste en Sus*, to enable reimbursement on top of the GHS tariffs.
- In some cases, hospital pharmacies can deliver drugs to ambulatory patients for home use. These drugs are listed on the "Retrocession List".
- Reimbursement rates will depend on the SMR level.

For hospital adoption, each French hospital reviews new drugs via an internal technology appraisal committee and may take a few months to adopt the drug following approval of reimbursement in France. These committees include physicians, pharmacists and finance managers. Medico-economic evidence is welcomed by finance managers to understand incomes and costs of standard *versus* new protocols.

Price negotiations are more substantial in public hospitals than among private hospitals in France. Typically, there is little price negotiation with private hospitals, where acquisition prices are close to the *Liste en Sus Médicaments Remboursables* (Reimbursed Drug List). Conversely, in public hospitals, there are significant negotiations for some of the drugs listed.

Hospital inpatient payment for drugs

French inpatient units are financed through a payment-per-case prospective payment system, using two related groupings: GHM (*Groupes Homogènes de Malades*) and GHS (*Groupe Homogène de Séjours*).

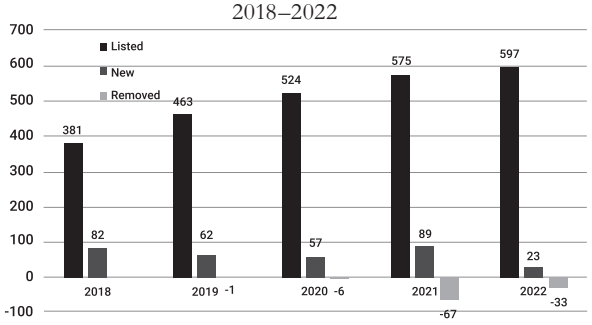
1. GHM is a diagnosis-related classification. The GHM assignment of each patient discharge reflects a combination of diagnosis (ICD-10 codes) and procedure (CCAM codes).
2. Each GHM has two fixed tariffs associated with a GHS – one for the public sector and one for the private sector. A total of 11,000 rates are available.
   - In public hospitals, the bundled GHS tariff for the patient discharge covers the physician fees and all hospital costs, including medical technologies.
   - In private hospitals, the GHS fee covers only hospital costs, supplies and nursing expenses. The Private hospital physician fees are paid separately under the Common Classification of Medical Procedures (CCAM), in addition to the GHS payment.

The financing of inpatient care in France is marked by a significant proportion of separate reimbursements for innovative drugs. These drugs are registered on the *Liste en Sus*, which is published annually.

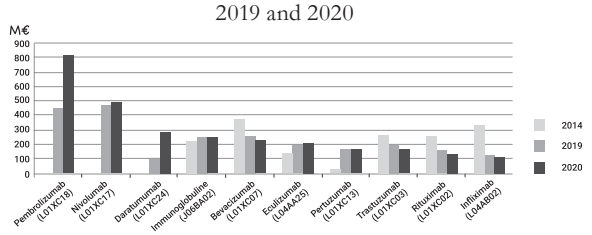
Unlike the USA and German temporary add-on payments, the *Liste en Sus* technically does not have a time limitation, as drugs are only reassessed every five years, and some products can remain listed for many years.

The *Liste en Sus* mostly includes anti-cancer, anti-inflammatory, auto-immune and immunoglobin drugs. In 2020, the 10 most expensive drugs on the *Liste en Sus* accounted for 61% of the total expenditure; nine of these listings were for anti-cancer drugs.

France *Liste en Sus* Drug Additions and Deletions, 2018–2022



Top 10 Most Expensive Drugs on the *Liste en Sus* in 2014, 2019 and 2020



Source: (The *Direction de la recherche*, 2022)[22]

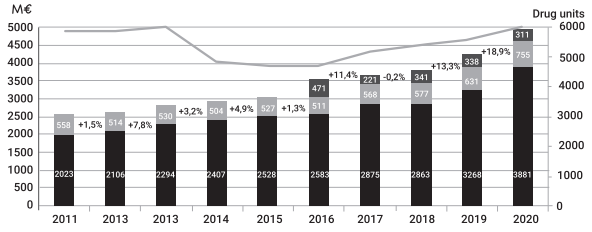
The five conditions that must be met for inclusion on the *Liste en Sus*, as published by (*Ministère des Affaires sociales et de la Santé*, 2018),[23] are as follows:

1. the drug must have a high SMR rating from the HAS;
2. the drug must have a high ASMR rating. Drugs with an ASMR level III or better (=I or II) are considered eligible. As an exception, drugs with an ASMR of IV or even V can be registered on this list if their comparator is already registered;
3. the frequency of the new drug's prescriptions within the hospital GHS must be below 80%;
4. the total incremental cost of the drug therapy must be more than 30% of the GHS tariff; and
5. the drug's cost must be similar to that of comparable products.

The value of drugs reimbursed separately from the GHS (*Liste en Sus*) increased to nearly €4 billion in 2020. In 2020, 84% of *Liste en Sus* drug expenditures were made in public hospitals and 17% in private hospitals.

A subset of *Liste en Sus* drugs are early access or compassionate-use drugs (ATUx and post-ATU).

Reimbursement of *Liste en Sus* ATUx and Post-ATU drugs. 2011–2020



Source: (The *Direction de la recherche*, 2022)[24]

Germany's NUB Process and Hospital Therapies

With European Union or national drug regulatory approval, a drug can be adopted by German hospitals. In 2011, the Act on the Reform of the Market for Medical Products (*Arzneimittelmarkt-Neuordnungsgesetz*, AMNOG) mandated a G-BA (Joint Federal Committee) review prior to local Statutory Health Insurance (SHI) reimbursement for all new drugs. The G-BA is the highest authority in German healthcare and is the key decision-maker for assignment of premium drug pricing. Otherwise, the new therapy is reimbursed at the level of the standard therapy.

Clinical evidence presented in the AMNOG dossier is usually the same evidence used for regulatory drug approval. The G-BA, with the support of the Institute for Quality and Efficiency in Health Care (IQWiG), subsequently analyses the potential additional patient benefit based on the following parameters:

- **Clinical**: mortality, morbidity, quality of life and side effects.
- **Economic**: Duration of therapy, dosage and cost of drug/yearly therapy cost, if applicable, size of target patient group based on clear definition of indication, any additional/accompanying health services needed with the new therapy.

The AMNOG dossier evaluation and subsequent discussion in the G-BA has a fixed timeframe of six months, including hearings with experts from industry, physicians' and patients' associations (Joint Federal Committe (G-BA), 2017).[25]

Hospital adoption initially depends on clinicians, but long-term adoption depends on adequate reimbursement. Larger university hospitals may adopt new drugs before reimbursement is established to ensure the availability of an innovative therapy to patients in need. Long term, all types of hospitals need to achieve cost-covering reimbursement via the German DRG system.

G-DRGs and NUB innovation payment

The German DRG system (G-DRG) for hospital payment was originally based on the Australian Refined DRG system, with a number of modifications, including the possibility of both short-term and permanent supplemental add-on payments for certain therapies.

One G-DRG payment usually covers all costs of a patient's hospital stay, including treatment, drugs and devices. As of 2020, nursing fees are excluded from this bundle and are paid as separate daily fees. Hospitals must also follow annual hospital budgets, which are calculated according to annual case mix.

Permanent implementation of new (and higher) tariffs for innovative drugs into the DRG system takes at least three years. Temporary bridge funding is possible for new hospital drugs under the NUB Innovation Clause (*Neue Untersuchungs- und Behandlungsmethoden*). NUB funding must be proposed each year, by each hospital using the new drug (Cornelia Henschke, 2013).[26] To qualify, drugs must fulfil the following criteria (InEK Institute for Remuneration System in the Hospital, 2018 to 2020):[27]

1. not be properly reimbursed via existing coding and fees;
2. have been used for less than four years in German hospitals; and
3. cause significant additional costs for the hospital stay (approximately €1,000).

InEK (*Institut für das Entgeltsystem Im Krankenhaus*), the agency that administers the G-DRG system, has never published a threshold for determining "additional cost", although a commonly known unofficial threshold is €600 per case.

Hospitals each apply individually for NUB funding through the InEK. Once approved, NUB status allows the hospital to negotiate one-year supplemental fees with local SHI funds (IGES, 2018).[28] Each hospital must reapply for each NUB supplement annually, and products are typically eligible for up to four years. Notably, there is no official time limitation on eligibility for NUB and it can widely differ between products.

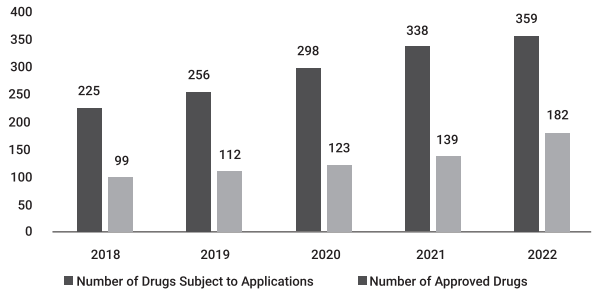
To date, oncologic drugs make up the majority of drugs approved for NUB. Severity of illness, demonstrated

proven-patient benefit and cost are the major success factors in obtaining NUB funding.

Following the NUB process, InEK then reviews data from "calculation" hospitals to determine the appropriate long-term integration into the G-DRG system based on the total cost of associated care. Hence, a drug may be integrated into the cost structure of identified G-DRGs or be assigned a permanent supplemental payment.

As depicted below, drug-related NUB applications, as well as approvals, have increased annually. Overall, applications from 2018 to 2022 have experienced a 44% success rate.

Drug-related NUB Applications and Approvals 2018–2022



ZE permanent supplemental payments

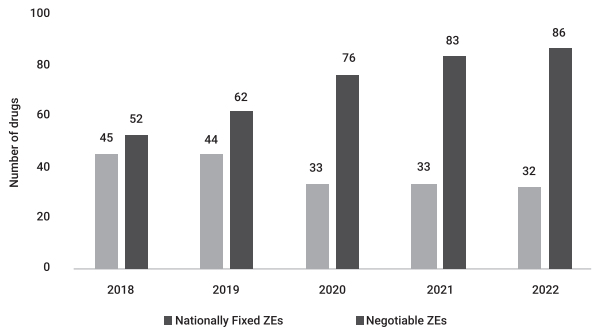
If drugs do not "fit" into the DRG structure, InEK may consider ZE (*Zusatzentgelt*) permanent supplemental payment, usually following a period of temporary NUB payment. ZE payments are used for drugs with multiple DRG assignments. ZE services are nationally designated but issued in two forms: one with a nationally fixed reimbursement price; and a second that is locally negotiated (similar to the NUB).

Eligibility requirements for a ZE are:

- clearly defined procedure (with OPS code);
- use with multiple DRGs without fixed association to any DRG; and
- relevant cost for the total DRG system, especially the hospitals rendering the service.

While permanent supplemental payments slightly decreased over the past few years, the number of negotiable ZEs for drugs are increasing. Drug-related ZEs often are published with a list of reimbursable amounts depending on dosage (if applicable) and are reviewed annually.

InEK ZE Assignments for Inpatient Drugs 2018–2022



Provision of High-Cost Drugs to the English NHS

In England, the Health Resource Groups (HRG) system is comprised of a case-mix payment system for all hospitals, both public and private. The National Tariff Payment System (NTPS) is a blended payment scheme for hospital inpatient and out-patient procedures reflective of averages nationwide. Each specific procedure is assigned a reference cost. In 2022/2023, 55 drugs are included in the NTPS. The 2022 Health and Care Act replaces the NTPS with the NHS Payment Scheme as of April 2023.

In 2022/2023, 642 drugs are directly commissioned by NHS England and are not reimbursed through the NTPS. (NHS England, 2022.)[29]

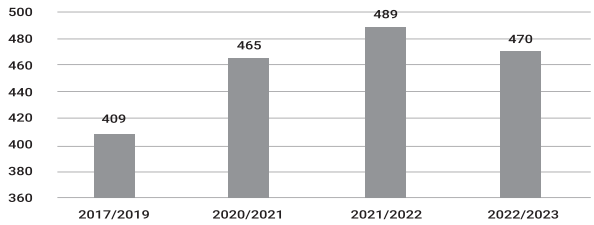
Hospital drug add-on payments are negotiated locally with Integrated Care Systems (ICS) or designated nationally for specialised services. The High-Cost Drugs List in the NHS is intended for specialised products whose use is concentrated in a relatively small number of centres and when a single patients' treatment costs are over £2,000 per annum, or the total anticipated expenditure will exceed £10,000 per annum. The purpose of this list is to enable additional payment by NHS England to the hospital trust for inpatient- or outpatient-dispensed, high-cost drugs managed as pass-through payments.

When commissioning high-cost drugs, commissioners use reference prices to incentivise provider uptake of the drug. Reference prices are set by NHS England based on the current best procured price achieved for a product or group of products by the NHS.

Where no reference price has been set, the actual drug cost or the nominated supply cost is used. The nominated supply cost is the cost payable by the provider if the high-cost drug was supplied in accordance with a requirement to use a specified supplier or distributor or via a framework contractual agreement.

The High-Cost Drugs List is reviewed annually. Drugs which no longer meet the criteria are considered for removal from the list (Department of Health and Social Care, 2012).[30]

High-Cost Drugs List, England, 2017/2019–2022/2023



- For 2017/2019, there were 409 drugs listed (NHS England and Monitor, 2017).[31]
- For 2020/2021, a total of 465 drugs were listed (NHS England and Monitor, 2020).[32]
- For 2021/2022, a total of 489 drugs were listed (NHS England and Monitor, 2021).
- For 2022/2023, a total of 470 drugs were listed on the High-Cost Drugs List (NHS England, 2022).[33]

Though it is encouraged, prior appraisal by the National Institute for Health and Care Excellence (NICE) is not a requirement for listing on the High-Cost Drugs List.

An online clinical decision support tool (known as "Blueteq") is used by NHS England for standard electronic contractual prior-approval for all high-cost drugs excluded from tariff.

Cancer Drugs Fund (CDF)

The CDF was established in 2011 as a trial program to enable access to specific cancer drugs not routinely available in the NHS. In 2016 this was moved to NHS England and a new appraisals approach was enacted (NHS England, n.d.).[34] The new process offers managed access arrangement to new treatments, while additional evidence is collected to address clinical uncertainty. The additional evidence is used to help NICE to decide if a new treatment should be routinely funded.

NICE appraises all new systemic anti-cancer therapy drug indications expected to receive a marketing authorisation. The process aims to publish draft guidance before a drug receives marketing authorisation, with final guidance published within 90 days of marketing authorisation. The appraisal process is based on the NICE Technology Appraisal, but with additional specific amendments for the CDF. (National Institute for Health and Care Excellence, 2014)[35] (National Institute for Health and Care Excellence, 2016).[36]

The process allows NICE to make one of three recommendations:

- yes: recommended for routine commissioning;
- no: not recommended for routine commissioning; or
- recommended for use within the CDF (new).

"*Recommended for use within the CDF*" can be applied for drugs for which NICE considers there to be "plausible potential" to meet the criteria for routine commissioning, but there remains significant clinical uncertainty.

For those drugs that have received either a "yes" or a draft recommendation for use within the CDF, interim funding is available at the point of marketing authorisation. However, in order to receive this funding, pharmaceutical manufacturers must agree to the expenditure control mechanism (NHS England Cancer Drugs Fund Team, 2016).[37]

Since the new approach to funding cancer drugs began in July 2016, approximately 71,000 patients have been registered to receive treatment with 91 drugs, treating 204 different cancer indications (NHS England Cancer Drugs Fund Activity Update, 2021).[38] As of January 2023, 54 drugs/drug combinations are listed on the CDF (NHS England, 2023).[39]

The CDF budget remains fixed at £340 million (NHS England Cancer Drugs Fund Activity Update, 2021).[40] If this fixed budget is exceeded, the additional cost is paid back by companies who generate income from the CDF via a proportional rebate to NHS England and NHS Improvement.

In addition to the CDF, NHS England's Innovative Medicines Fund has an annual budget of £340 million to provide funding through two further drug-access programs. The Early Access to Medicines Scheme has helped over 1,200 patients with life threatening or seriously debilitating conditions access drugs ahead of a marketing authorisation when there is a clear unmet medical need. (NHS England, 2023.)[41] In 2022/2023, 33 drug treatments are available via Managed Access Agreements where additional evidence is required to inform drug use. (National Institute for Health and Care Excellence, 2023.)[42] NICE recommends a managed access treatment to NHS England following an HTA.

Conclusions

While there is growing attention to the costs of prescription pharmaceuticals, hospital-dispensed specialty pharmaceuticals may face increasing challenges to justify premium prices under increasingly constrained methods of hospital payment. Notably, DRG payment systems are adding tighter controls on overall drug spending and may, in some markets, be very reluctant to provide supplemental add-on payment.

In the USA, hospitals help compensate under-reimbursement for some inpatient pharmaceuticals via higher markups on other patients. However, in single payer environments, such as Britain or Germany, no such cost shifting is possible.

Some systems have maintained special pathways to fund cancer drugs specifically, which has, to some extent, created a safe harbour in some markets. However, these pathways typically place limitations on drug prices.

In those markets in particular, manufacturers face a multi-tiered challenge and must prove therapeutic value from an economic standpoint at both societal and provider levels. Robust economic modelling, based on well-designed comparative clinical trials, has thus become a necessity for market success. In addition, for the newest generations of immune-oncology therapies, hospitals simply cannot afford acquisition of the products. In these cases, some manufacturers are obliged to negotiate direct payment agreements with insurers so that costs can be amortised over time, and in some instances, payments can be linked to therapeutic outcomes.

Endnotes

1. 106th Congress. (2000). H.R.5661 - Medicare, Medicaid, and SCHIP Benefits Improvement and Protection Act of 2000 (BIPA). https://www.congress.gov/bill/106th-congress/house-bill/5661.
2. Akehurst. (2017). Variation in Health Technology Assessment and Reimbursement Processes in Europe. *Value in Health 20, 67–76*.
3. Centers for Medicare & Medicaid Services. (2020). *Medicare Provider Utilization and Payment Data: Inpatient*. Retrieved from cms.gov: https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/Medicare-Provider-Charge-Data/Inpatient.
4. 106th Congress. (2000). H.R.5661 - Medicare, Medicaid, and SCHIP Benefits Improvement and Protection Act of 2000 (BIPA). https://www.congress.gov/bill/106th-congress/house-bill/5661.
5. Centers for Medicare & Medicaid Services. (2001). Medicare Program: Payments for New Medical Services and New Technologies under the Acute Care Hospital IPPS: Final Rule, *Federal Register 66 , no. 174*, 46902 –46925.
6. Medicare Modernization Act. (2003). MEDICARE PRESCRIPTION DRUG, IMPROVEMENT, AND MODERNIZATION ACT OF 2003, PL 108-173.
7. Centers for Medicare & Medicaid Services. (2023). *FY 2023 IPPS Final Rule Home* Page. Retrieved from CMS.gov: https://www.cms.gov/medicare/acute-inpatient-pps/fy-2023-ipps-final-rule-home-page#FinalRule.
8. Centers for Medicare & Medicaid Services. (2001). Medicare Program: Payments for New Medical Services and New Technologies under the Acute Care Hospital IPPS: Final Rule,. *Federal Register 66 , no. 174*, 46902–46925.
9. Centers for Medicare & Medicaid Services. (2010). FY2020 IPPS/RY 2010 LTCH PPS final rule. *Federal Register: 74*, 43813–43814.

10. Centers for Medicare & Medicaid Services. (2023). *FY 2023 IPPS Final Rule Home* Page. Retrieved from CMS.gov: https://www.cms.gov/medicare/acute-inpatient-pps/fy-2023-ipps-final-rule-home-page#FinalRule.
11. Centers for Medicare & Medicaid Services. (2023). *FY 2023 IPPS Final Rule Home* Page. Retrieved from CMS.gov: https://www.cms.gov/medicare/acute-inpatient-pps/fy-2023-ipps-final-rule-home-page#FinalRule.
12. Centers for Medicare & Medicaid Services. (2023). *FY 2023 IPPS Final Rule Home* Page. Retrieved from CMS.gov: https://www.cms.gov/medicare/acute-inpatient-pps/fy-2023-ipps-final-rule-home-page#FinalRule.
13. Centers for Medicare & Medicaid Services. (2023). *FY 2023 IPPS Final Rule Home* Page. Retrieved from CMS.gov: https://www.cms.gov/medicare/acute-inpatient-pps/fy-2023-ipps-final-rule-home-page#FinalRule.
14. Department of the Treasury, Department of Labor, Department of Health and Human Services. (2021). *Interim Final Rule with Request for Comments*.
15. United States House of Representatives. (2020, April). *United States Code Online - Title 21 "Food and Drugs"*. Retrieved from uscode.house.gov: https://uscode.house.gov/download/download.shtml.
16. Centers for Medicare & Medicaid Services. (2019, August 2). *CMS-1716-F and CMS-1716-CN2*. Retrieved from CMS.Gov: https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/AcuteInpatientPPS/FY2020-IPPS-Final-Rule-Home-Page-Items/FY2020-IPPS-Final-Rule-Regulations.
17. Henry J Kaiser Family Foundation. (2012). *Medicaid Benefits: Inpatient Hospital Services, other than in an Institution for Mental Diseases*. Retrieved from State Health Facts: https://www.kff.org/medicaid/state-indicator/inpatient-hospital-services-other-than-in-an-institution-for-mental-diseases/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D.
18. Reinhardt, U. E. (2009, January 23). How Do Hospitals Get Paid? A Primer. *New York Times*. Retrieved from Economix: https://economix.blogs.nytimes.com/2009/01/23/how-do-hospitals-get-paid-a-primer/.
19. US Government Accountability Office. (2011, September 23). *Drug Pricing: Manufacturer Discounts in the 340B Program Offer Benefits, but Federal Oversight Needs Improvement*. Retrieved from GAO.gov: https://www.gao.gov/products/GAO-11-836.
20. Augenbaum, S. (2022). *District of Columbia Medicaid Inpatient Hospital Payment Method: APR-DRG*. Department of Health Care Finance.
21. AHIP. (2022). *Hospital Price Hikes: Markups for Drugs Cost Patients Thousands of Dollars*. AHIP.
22. The *Direction de la recherche, d. é.* (2022). *Républicque Francaise*. Retrieved from Research, Studies, Evaluation and Statistics Branch.
23. *Ministère des Affaires sociales et de la Santé*. (2018). *Management of drugs in the hospital: details on the "list in addition" decree*. Retrieved from http://solidarites-sante.gouv.fr/archives/archives-presse/archives-breves/article/prise-en-charge-des-medicaments-a-l-hopital-precisions-sur-le-decret-liste-en.
24. The *Direction de la recherche, d. é.* (2022). *Républicque Francaise*. Retrieved from Research, Studies, Evaluation and Statistics Branch.
25. Joint Federal Committe (G-BA). (2017, December). *Law for the Reorganization of the Pharmaceutical Market AMNOG*. Retrieved from https://www.g-ba.de/institution/themenschwerpunkte/arzneimittel/nutzenbewertung35a.
26. Cornelia Henschke, M. B. (2013). Extrabudgetary ('NUB') payments: A gateway for introducing new medical devices into the German inpatient reimbursement system? *Journal of Management & Marketing in Healthcare*, 119–133.
27. InEK Institute for Remuneration System in the Hospital. (2018 to 2020). *New examination and treatment methods (NUB)*. Retrieved from https://www.g-drg.de/Neue_Untersuchungs-_und_Behandlungsmethoden_NUB.
28. IGES. (2018). *Reimbursement of Pharmaceuticals in Germany*. Berlin: IGES Institut GmbH.
29. NHS England. (2022, December 14). *NHS England drugs list*. Retrieved from NHS England: https://www.england.nhs.uk/publication/nhs-england-drugs-list/.
30. Department of Health and Social Care. (2012). *High Cost Drugs*. Retrieved from Gov.UK: https://www.gov.uk/government/news/high-cost-drugs--2.
31. NHS England and Monitor. (2017, April 1). *Annex A: The national prices and national tariff workbook*. Retrieved from National tariff payment system 2017/18 and 2018/19: https://improvement.nhs.uk/resources/national-tariff-1719/.
32. NHS England and Monitor. (2020). *Annex A: National Tariff Payment System 2020/2021: a consultation notice*. Retrieved from improvement.nhs.uk: https://improvement.nhs.uk/resources/national-tariff-2021-consultation/#annexes
33. NHS England. (2022, Nov 18). *NHS England national tariff payment system*. Retrieved from NHS England: https://www.england.nhs.uk/publication/national-tariff-payment-system-documents-annexes-and-supporting-documents/.
34. NHS England. (n.d.). *Cancer Drugs Fund*. Retrieved from https://www.england.nhs.uk/cancer/cdf/.
35. National Institute for Health and Care Excellence. (2014, September). *Guide to the processes of technology appraisal*. Retrieved from https://www.nice.org.uk/process/pmg19/chapter/acknowledgements.
36. National Institute for Health and Care Excellence. (2016, April). *Final amendments to the NICE technology appraisal processes*. Retrieved from PMG 19-Addendum A: https://www.nice.org.uk/Media/Default/About/what-we-do/NICE-guidance/NICE-technology-appraisals/process-and-methods-guide-addendum.pdf.
37. NHS England Cancer Drugs Fund Team. (2016, July 8). *Appraisal and Funding of Cancer Drugs from July 2016 (including the new*. Retrieved from NHS England: https://www.england.nhs.uk/wp-content/uploads/2013/04/cdf-sop.pdf.
38. NHS England Cancer Drugs Fund Activity Update. (2021, October 25). *NHS England Cancer Drugs Fund Activity Update, 2020-21*. Retrieved from NHS England: https://www.england.nhs.uk/publication/cancer-drugs-fund-cdf-activity-update/.
39. NHS England. (2023, January 12). *National Cancer Drugs Fund List*. Retrieved from NHS England: https://www.england.nhs.uk/publication/national-cancer-drugs-fund-list/.
40. NHS England Cancer Drugs Fund Activity Update. (2021, October 25). *NHS England Cancer Drugs Fund Activity Update, 2020-21*. Retrieved from NHS England: https://www.england.nhs.uk/publication/cancer-drugs-fund-cdf-activity-update/.
41. NHS England. (2023, January 13). *Early Access to Medicines Scheme*. Retrieved from NHS England: https://www.england.nhs.uk/aac/what-we-do/how-can-the-aac-help-me/eams/.
42. National Institute for Health and Care Excellence. (2023, January 13). *Managed Access*. Retrieved from NICE: https://www.nice.org.uk/about/what-we-do/our-programmes/managed-access.

Stephen Hull, MHS, is the President and Founder of Hull Associates LLC, a specialised global market-access strategy firm. Stephen has over 25 years of experience in health policy and medical product strategy, for pharmaceuticals, medical devices, diagnostics, and biotech products. He is a former Senior Vice President of the Advanced Medical Technology Association, and has served as chairman of the medical devices council of the International Society of Pharmacoeconomics Outcomes Research (ISPOR).
Stephen has an advanced degree in health policy from the Johns Hopkins Bloomberg School of Public Health, and a Bachelor's Degree in International Relations and French from Colgate University.

Hull Associates LLC
100 Ledgewood Place, Suite 202
Rockland, Massachusetts 02370
USA

Tel: +1 781 982 8600
Email: shull@hullassociates.com
URL: www.hullassociates.com

Gilles Launay, MD, is a Senior Consultant based in France. He has over 25 years of health industry experience, including pharmaceuticals, cell diagnostics and digital healthcare innovations in France. He was previously the Chief Sales Officer at Cerner France, where he was a member of the management committee and negotiated contracts with hospitals throughout France, including Nantes, Anvers, Ghent and Lens, and expanded the business into France, Benelux and Switzerland. Gilles spent three years as the Secretary General of the Academic Hospital of Montpellier, where he was responsible for leading the restructuring of clinical unit activities, and he designed the 2012–2016 medical scheme. He was also the Project Director for a Regional Health Agency (ARS) in France responsible for designing and implementing the new information system. He has received a Doctorate in Medicine and a Master's of Hospital Management (EHESP).

Hull Associates LLC
Greater Paris Metropolitan Region
France

Email: glaunay@hullassociates.com
URL: www.hullassociates.com

Kirstin Ostoff is a Senior Consultant based in Germany. She has 18 years of device industry experience and has carried out extensive work in financial analysis and management, forecasting, company restructuring and M&A activities. Previously, Kirstin was the Manager of Finance and Controlling at Edwards Lifesciences in Munich, and the Manager of Finance and Controlling/Administration at Baxter Ltd. She has worked in Germany and Spain in a broad range of roles over a seven-year period. Her experience includes: financial forecasting and budgets; quarterly reporting and auditing; and strategic assessments for financial management and corporate structuring. She was in charge of logistics and purchasing for Baxter Deutschland and has undertaken academic work in economics and computer science. Kirstin is fluent in three languages.

Hull Associates LLC
Greater Munich Metropolitan Area
Germany

Email: kostoff@hullassociates.com
URL: www.hullassociates.com

Louise Cresswell is an RN Senior Consultant based in the United Kingdom. She has over 35 years of progressive experience working within the healthcare sector as an NHS practitioner and within medical technology companies. Louise is currently the Managing Director at Visea Ltd in Worcestershire, where she focuses on commercial development for medical device manufacturers and suppliers, including overseas manufacturers. She is also the Joint Managing Director at Safer Options Ltd in Worcestershire. Previously, Louise was the Vice President at SOL-Millennium Medical Group, where she focused on Global Business Development and Corporate Accounts in the UK, Western Europe and Asia-Pacific Regions for hypodermic safety-engineered devices and related commodity products.

Hull Associates LLC
Tenbury Wells
England

Email: louise@hullassociates.com
URL: www.hullassociates.com

Hull Associates LLC is an international market-access consulting firm based in Boston, USA, and is active in 22 major markets around the world. Founded in 2007, Hull Associates serves international manufacturers with comprehensive strategy on market selection, evidence development, core product positioning and pricing strategy. Hull Associates is supported by senior-level consultants in all markets of the world and has served over 450 clients with targeted strategies. In addition to specialty pharmaceuticals, Hull Associates also serves *In Vitro* Diagnostic and Medical Device companies with a broad range of services.

www.hullassociates.com

Hull Associates LLC
MARKET ACCESS

Australia

Bernard O'Shea

Rohan Sridhar

Norton Rose Fulbright

1 Digital Health

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

Digital health is an umbrella term referring to a range of technologies that can be used to treat, diagnose and monitor patients and collect and share a person's health information.

Similar to other jurisdictions, the term "digital health" is still developing as technologies evolve. At one end of the spectrum, the term includes the delivery of telehealth services, while at the other end, the term connotes mobile apps and software as a medical device ('SaMD') used to deliver personalised and individualised medicine, with digital medical devices lying somewhere in between.

While digital health is not a defined legislative term, the Government has taken steps to define telehealth in order to include these services under the subsidised Medicare arrangement during the COVID-19 pandemic, and the national regulator, the Therapeutic Goods Administration ('TGA'), regulates some digital health technologies as medical devices.

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

The key emerging digital health technologies in Australia are:

- Telehealth: delivery of support by healthcare practitioners without the need for face-to-face appointments. In December 2021, the Federal Government announced that it would allocate A$106 million over four years to support permanent telehealth services. Additionally, from 1 January 2022, patient access to telehealth services is supported by ongoing Medicare Benefits Schedule ('MBS') arrangements.
- My Health Records: digitisation of health records to improve the quality and availability of health information.
- eScripts: digitisation of pharmacy prescriptions to allow easier access to certain medicines and ease processing on pharmacists. This fundamentally changes the long-standing requirements that all prescriptions must be provided physically and in writing.
- Genetic guidance of treatment: use of genomic testing to guide treatment pathways for a range of illnesses, including cancer and mental health issues. This is attendant with issues regarding the regulatory requirements of the testing process, as well as the end output, which typically informs decision-making by a healthcare professional.
- Big Data Analytics: use of historic data to provide consumers with tailored healthcare pathways and a better understanding of medication use.
- Secure Messaging: facilitating the secure, encrypted exchange of information between health professionals.
- COVID-19 digital certificates: a digitally accessible proof of COVID-19 vaccination administered in Australia.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health in Australia are applicability of and compliance with the regulatory framework and issues regarding privacy and data security. As digital health technologies develop and become more prominent, the means by which sensitive health data is collected, stored and shared must reflect this development. Following a recent high-profile privacy breach at a major health insurer, there is a heightened focus on ensuring digital health data is stored securely so as to prevent unauthorised access.

While the Australian digital health market is certainly growing post-COVID, the legislative and regulatory schemes are not yet sophisticated enough to deal with the nuanced issues arising in this market. To address this nuance from a privacy perspective, the Australian Government has undertaken a thorough review of Australia's principal privacy legislation, the *Privacy Act 1988* (Cth) ('Privacy Act'), which is expected to undergo significant reform throughout 2023.

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

The market for digital products and services in the healthcare sector is growing rapidly, especially post-COVID. Although the exact figure is not confirmed, in 2021, it was estimated that Australia's digital health market was worth about A$2 billion.

More generally, it has been estimated that AI could contribute more than A$20 trillion to the global economy by 2030.

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

Public information in relation to private companies is difficult to find. As such, it is necessary to consider publicly listed companies which typically report to the market. To our knowledge, the

five largest (by revenue) digital health companies in Australia are Telstra Health, Medical Director, Best Practice, Genius Solutions and Alcidion.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

There is a lack of sophistication in Australia's digital health regulatory framework. The current legislation that is broad enough to apply to digital health includes the *Therapeutic Goods Act 1989* (Cth) ('TG Act'), the *Therapeutic Goods (Medical Devices) Regulations 2002* (Cth) ('TG Regulations') and the *My Health Records Act 2012* (Cth) ('My Health Records Act').

The TG Act establishes the national controls which relate to the quality, safety, efficacy and availability of therapeutic goods that are used in Australia. It provides a uniform approach for all states and territories to adopt. The term therapeutic goods is given a broad definition and includes software-based medical devices and other digital health technologies. The level of regulation for these devices is dependent upon the disease they are designed to assist with, its 'risk rating' and severity of the consequences if the device were to fail. A number of items of software, such as those designed to assist in healthcare practice management, or clinical workflow management, are excluded from regulation in Australia. However, the system continues to suffer from a lack of refinement to cover emerging technologies. This creates difficulties in confirming which products need to be registered and to what standard, and what restrictions might be placed on their marketing, promotion and supply.

The My Health Record Act enables the operation of a national public health patient information system, by which health practitioners can access health records of individuals through a digital sharing platform. It is a singular platform, and is the only one of its kind. It relates solely to the processes pertaining to the My Health Record, which is a secure digital record of an individual's healthcare information. Operation of the My Health Records Act is supported by the My Health Records Regulation 2012 (Cth) and the Healthcare Identifiers Act 2010 (Cth).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Despite its general application, the Privacy Act applies to digital health in a number of ways. For example, the Privacy Act contains provisions that will apply if the digital health function uses, collects or distributes personal information. Personal information is any information that identifies, or is likely to identify, a person. If a digital health function uses personal information, it must ensure that it displays a privacy policy, notifies users that it is collecting their personal information and the purpose for which this information is being collected. Several State and Territory Governments have also enacted privacy legislation directed specifically to health records and other health information, whether held by healthcare professionals or by digital health applications. This legislation typically restricts transfer out of the particular State, making cloud and other offshore storage problematic.

If the digital health function collects health information, such as disability or specialist reports, then this will attract additional privacy protections compared to personal information. For example, any data in relation to the My Health Records scheme must be stored in Australia and under no circumstances is to be disclosed to cross-border entities.

Australia's consumer regulatory scheme, the *Competition and Consumer Act 2010* (Cth) ('CCA'), may also apply to digital health. The CCA establishes a national law that governs how all businesses in Australia must deal with their competitors, suppliers and customers. The CCA is designed to enable all businesses to compete on their merits in a fair and open market, while also ensuring businesses treat consumers fairly.

Under the CCA, any acts undertaken by digital health companies which are viewed as promoting an anti-competitive business strategy can face severe penalties. Further, any digital health products that are likely to cause consumers to be misled, or make misrepresentations about the quality, purpose or efficacy of the product can face regulatory action pursuant to the CCA. The penalties which the regulator can seek range from injunctive action and pecuniary penalties, to prison sentences for serious cartel conduct.

There are presently limited anti-kickback restrictions in Australia. These typically apply to doctors, pathology and diagnostic imaging services, and prevent certain payments being made between these professionals. These provisions apply where primary payments are made through Australia's public health system and the need to limit unnecessary referrals.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

To the extent that a consumer healthcare device or software is a medical device, it will need to conform to the TG Act and the TG Regulations. The specific nature of the compliance requirements differs based on the 'class' of the device. Medical devices are classified with regard to their intended purpose. In particular, the classification rules take into account the degree of invasiveness in the human body, the duration and location of use, and whether the device relies on a source of energy, which applies to virtually all digital health technologies.

There remains some tension between the definitions used in the TG Act and the actual intended use of technology. This is particularly acute in relation to wearables, as well as products aiming to provide guidance to doctors in the exercise of their professional judgment. In many cases, it is necessary to contemplate exactly what the supplier has said about the product as to whether it will be regulated or not. As noted above, the regulatory framework has not been updated to specifically cover the myriad of digital health technologies now in use. The TGA does use its existing framework to declare certain goods to be, and not to be, medical devices, and therefore within or outside the regulatory framework. In relation to software-based devices, the TGA has declared a number of types of technology to be excluded from the regulatory framework.

Additionally, all consumer products are regulated by the CCA. This regulation includes, amongst other matters, consumer protections, provisions applying to warranty disclosure, misleading advertising and fitness for any disclosed purpose.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The TGA, which is part of the Australian Government Department of Health, is Australia's regulatory authority for therapeutic goods. Broadly, the TGA is responsible for regulating the registration of therapeutic goods in Australia. The TGA regulates

therapeutic goods through pre-market assessment, post-market monitoring and enforcement of standards, and through the licensing of Australian manufacturers. The TGA can issue conformity assessment documents in respect of manufacturers of medical devices, though given the limited Australian manufacturing industry, many manufacturers rely on overseas certification of quality management systems, including notified bodies or Medical Device Single Audit Program ('MDSAP') certification.

Under the TG Act and the TG Regulations, the Secretary of the Department of Health can make decisions in relation to individual sponsors, manufacturers and advertisers. Some of these decisions are made in the event of non-compliance with regulatory requirements and others are made at the request of the sponsor or manufacturer. Regulatory requirements for which sponsors, manufacturers and advertisers can face liability for breaching include failure to properly label or advertise goods, or the importation of goods that are not registered correctly.

The Office of the Australian Information Commissioner ('OAIC') is responsible for the administration of the privacy provisions contained in the My Health Records Act and the Healthcare Identifiers Act 2010 (Cth).

Additionally, the Australian Competition and Consumer Commission ('ACCC') is responsible for enforcing the CCA and the Australian Consumer Law ('ACL'), which is set out in Schedule 2 of the CCA. The ACL includes a national law guaranteeing consumer rights when buying goods and services and a national product safety law and enforcement system. This includes the principal oversight of recalls of products, though often these are left to the TGA in relation to medical products.

2.5 What are the key areas of enforcement when it comes to digital health?

The primary areas that regulatory authorities are targeting are:

- Classification of devices, both to bring devices within the regulatory framework or to up-classify devices.
- Ensuring digital health products conform to consumer product standards.
- Ensuring digital health products are advertised in a TG Act-compliant manner.
- Protecting privacy and data security of personal and sensitive health information housed in data centres of digital health organisations. This is expected to become even more important following a number of significant data breaches.
- The digital economy, including consumer data issues in digital health, is an area of priority for the ACCC.
- Consumer product safety issues for young children, with a focus on compliance, enforcement and education initiatives.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

If the SaMD is captured by the medical device definition in the TG Act and is not within one of the exemptions or exclusions, it will need to conform to the typical medical device clinical requirements. This involves registering the medical device in the Australian Register of Therapeutic Goods ('ARTG') which is managed by the TGA. The device will need to be classified according to the TG Regulations, which is closely aligned with the classification system used by the European Union. The quality management system will also need to be certified as compliant with the relevant conformity assessment procedures, again closely aligned with the EU system.

Further, an Australian sponsor will need to be appointed, and a Declaration of Conformity must be submitted. The Sponsor must then submit various certifications, and applications to the TGA for review. In making its assessment, the TGA will assess the device against the Essential Principles contained in the TG Regulations. If the TGA approves the application, an ARTG listing number will be issued to the device, and it will be visible on the ARTG database on the TGA website. The SaMD may then be legally supplied.

It is also necessary to note that the sponsor of a therapeutic good, in Australia, is the person who imports the product into, or manufactures the product in, Australia. This creates a number of issues for software-based medical devices, since they are often made available by way of download from a central repository. In such a case, the download of the product may be considered the importation of the product in Australia, leaving the relevant 'downloader' as technically satisfying the sponsor definition. The TGA is concerned about this issue, particularly where consumers may be acting on recommendations generated by such software, but as yet it has not proposed a concrete solution.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

There are presently no special regulations applying to artificial intelligence ('AI')/machine learning ('ML') powered digital health devices or software solutions and their approval for clinical use. Where the devices or software solutions are classified as medical devices, the regulations applying to medical devices will apply. In such circumstances, the sponsor will need to apply to the TGA to have the device included on the ARTG prior to supply.

Given that Australia's digital regulatory landscape is evolving, it is likely that special regulations will be developed in the future which apply specifically to AI/ML powered digital health devices or software solutions. The TGA has previously contemplated this issue, but no changes have been made to date. The expectation would be that they would be likely to follow, in general terms, the approach adopted by the European Commission, with perhaps some local adjustments.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Data privacy and the protection of sensitive health data collected in the course of conducting telemedicine is a core issue. Additionally, websites and software packages can be classified as medical devices, imposing increased compliance requirements. Data sharing in the context of telemedicine is likely to be regulated by the My Health Record Act. There is also the need to ensure that the patient can be properly identified and consents to the provision of care by telemedicine, and that appropriate records are retained.
- **Robotics**
  Depending on their intended use, robotic technologies may be classified as medical devices under section 41DB of the TG Act. If this occurs, the sponsor will need to have the device registered before it can be advertised and sold.
  There may also be issues of tort liability where the robotic technology causes harm to a patient. Additionally, data

privacy issues arise where the robotic device collects personal information, though this can typically be mitigated by only allowing access to de-identified patient data.

- **Wearables**
  The core issue with wearables is whether they are inside or outside the regulatory framework. The issue often pivots on the sponsor's promotional material, as it indicates intended use. A consistent issue is who owns the data collected from the device wearers. Similarly, issues arise relating to the privacy and security of the data collected from the device wearers. This is an area where the boundary is being continually pushed as devices gather more data, apply sophisticated algorithms and provide users with various metrics by way of feedback.
- **Virtual Assistants (e.g. Alexa)**
  Issues arise where the virtual assistants begin providing diagnostic or therapeutic advice. Where this occurs, it is likely that the technology will be classified as a medical device, imposing greater compliance requirements.
  Further, issues arise relating to the rights to data collected by the virtual assistant. The technology sitting behind these assistants requires strict compliance with data protection laws and security requirements.
- **Mobile Apps**
  Separation of the apps from the platform on which they run is important. Like wearables, there is often a question of whether the product is within or outside of the regulatory framework. Given such products are often sourced through foreign "app stores", the question of who is properly regarded as the sponsor can be problematic.
  Ownership of the data collected by the mobile apps, data protection and security requirements, specifically for health and/or monitoring apps, and the issue of liability, are key. Depending on the intended use of the apps, they may be classified as a medical device. The TGA does not regulate health and lifestyle apps that do not meet the TG Act definition of a medical device.
- **Software as a Medical Device**
  The TGA regulates SaMDs. Where the software is classified as a SaMD, regulatory issues arise. These include classifying the device according to the level of harm it may pose to users or patients, obtaining a conformity assessment certification for the device and submitting a declaration of conformity. Note that the question of who is properly regarded as the sponsor can be problematic in the context of SaMDs, again as a result of their provenance and accessibility.
  It is also noted that the software is typically treated as separate from the platform on which it exists. There are, however, questions about the extent to which updates to an operating system render the approvals of the software invalid, or in need of an updated review, or in some cases, recall.
- **Clinical Decision Support Software**
  Clinical decision support software ('CDSS') that meets the definition of a medical device must be included in the ARTG unless otherwise exempt. Where the CDSS is responsible for storing data, issues of data privacy and security arise. There may also be issues of tort liability where the CDSS is responsible for adverse health outcomes. The regulatory treatment of CDSS remains quite a contentious area, critically depending on the functionality of such software. Clearly, a continuum exists from software which merely provides information for consideration by a healthcare professional, to software which provides a warning or recommendation, to software involved in clinical decisions. This is a key area where the regulatory framework has ambiguities.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Software that is powered by AI/ML is governed by the same legislation applying to other software. If the specific AI/ ML powered digital health solution satisfies the TG Act definition of medical device, it must comply with the TGA requirements, including obtaining a conformity assessment certification for the device and submitting a declaration of conformity.
  Additionally, the Australian Privacy Principles ('APPs') (see question 3.2) are designed to be technology neutral, flexible and principles-based, which can adapt to changing and emerging technologies, including AI. Despite this, it is critically important that personal information used to train AI systems is accurate, collected and handled in accordance with legal requirements.
- **IoT (Internet of Things) and Connected Devices**
  The issue with IoT is primarily an issue of categorisation. Very similar to CDSS, a continuum exists as to what the connected device is capable of doing. There are simple sensors which merely pass along information, through to more complex devices e.g. a mattress that detects movement and provides an alert. Aspects of intended use may impact categorisation, as may its role in a hospital ecosystem.
- **3D Printing/Bioprinting**
  The use of 3D printing brings in the regulatory framework concerning custom-made medical devices, which has recently undergone significant reform. Depending on the type of product being printed, and the frequency of its use, different regulatory obligations will apply. This includes differences in the need to register a product, as well as the need for ongoing reporting to the TGA. There is also a question regarding the consumables for such printing, their categorisation and place in the regulatory framework. There are also potential patent and design infringement issues associated with some categories of bioprinting.
- **Digital Therapeutics**
  Categorisation of these devices is important, as is their cyber-security. There are concerns around the ability of such devices to be hacked or interfered with, and the appropriate treatment of software updates, and the applicable regulatory oversight of these.
- **Natural Language Processing**
  Appropriate categorisation of the product as a medical device will be an issue for these, primarily the question of whether it satisfies the regulatory definition. We might expect that from a regulatory perspective the fallback of the relevance of the device to patient safety might be the determinative factor, with the TGA providing clarity through the use of included and excluded orders.

3.2 What are the key issues for digital platform providers?

Digital platform providers sit in a difficult space as to whether they are within the regulatory framework or not. There are also potential exposures under the ACL. Digital platform providers need to understand the precise scope of their platform and the extent to which such a platform falls within the definition of a medical device. It is also necessary to consider whether a relevant exemption might assist.

Another key issue for digital platform providers is the privacy and security of the data housed in the platform. Any information a digital platform provider collects, uses, stores or discloses, will need to comply with the APPs contained in the Privacy Act.

The APPs are legally binding principles that are the cornerstone of the privacy protection framework in Australia. The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

For digital platform providers, the APPs of greatest relevance regarding health information is the disclosure to other entities (APP 6), especially cross-border entities (APP 8). While disclosure can be legitimised by obtaining informed consent from the individual to which the information relates, it is important that digital platform providers also remain vigilant in complying with the APPs.

Digital platform providers must also ensure that they have appropriate data management systems and security measures in place, so as to protect against unauthorised access and misuse of personal information it collects. For companies, compliance is becoming even more important, following significant privacy breaches to a number of entities in recent times, and very significant increases in fines.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The use of personal data is subject to the APPs. The key issue in relation to collection, use, storage and disclosure of personal information is consent of the underlying individual, particularly where the data is collected from a third person (such as a healthcare professional). In such a case, the ability to demonstrate consent is problematic. The de-identification of patient data is also important, particularly where the information has served its purpose. However, there are often issues in terms of de-identification, particularly where other sources of information can provide sufficient information to re-identify the individual. Withdrawal of consent can also be problematic, particularly since the express right to be forgotten does not exist under Australian law. As such, the right to withdraw consent, or have information deleted, is typically imposed as a matter of voluntary obligation by way of a privacy policy. This creates issues as to how the information is deleted, particularly if it has been passed to third parties or otherwise linked to other data sources.

Given the sensitive nature of health data and identifiers, another important consideration is whether personal information has been adequately de-identified or anonymised prior to disclosure or use, particularly for digital health technologies. Providers also need to contemplate the extent to which some personal information, such as genetic information, can truly be de-identified, especially in a healthcare environment.

A critically important consideration is whether the data is being used for the primary purpose for which it was collected. Per APP 6, in the absence of the individual's consent, health data can only be used for the primary purpose for which it was collected, or for secondary uses that are directly related to the primary purpose. Essentially, any information collected in the context of the provision of health services will be sensitive information.

Where data is being used and shared in cross-border settings, it is important to consider whether the recipient is willing and able to comply with the requirements contained in the APPs. Often, transfers of data within a family of companies occurs without sufficient consideration of the privacy issues this might cause.

4.2 How do such considerations change depending on the nature of the entities involved?

In Australia, Government entities are held to a higher standard than regular entities. Additionally, contracts with Government entities often impose obligations on service providers to comply with the Privacy Act as though the party is a Government entity. Further, State and Territory Governments and their instrumentalities, such as the public hospital system, will often mandate compliance with separate State and Territory privacy laws, which are typically more restrictive in terms of data transfer.

Generally, an APP entity will not include a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State, though small businesses which hold or collect health information are fully subject to the Privacy Act.

4.3 Which key regulatory requirements apply?

The Privacy Act is the primary federal law related to protecting patient health information. It is important to note that Australia's Privacy Act has recently undergone a significant review and broad reforms are expected. The Privacy Act limits the use of key identifiers, such as a Medicare number (the key primary identifier used throughout the health systems), being used by private enterprises to identify a patient.

Additionally, the Commonwealth has recently passed the *Security of Critical Infrastructure Act 2018* (Cth) ('SOCI Act'). The SOCI Act applies to regulate Australia's critical infrastructure sectors and assets. Notably, the SOCI Act applies to the healthcare and medical sectors.

The SOCI Act requires the responsible entity for a critical infrastructure asset to have a critical infrastructure risk-management programme. Where a cyber-security incident occurs which has a relevant impact on a critical infrastructure asset, the responsible entity is required to notify Australia's Cyber and Infrastructure Security Centre.

The implications of this legislation are still being played out, and will likely be driven by the larger private, rather than public, hospitals pushing down a range of cyber-security-related requirements on to their providers of relevant digital healthcare solutions. A high-profile example of this is patient information systems, the failure of which can virtually render a hospital non-functional.

4.4 Do the regulations define the scope of data use?

Generally, data use must be for the primary purpose for which it was collected. This can typically be gleaned from disclosures made to the individual at the time of collection, in either a collection statement or privacy policy. This can create difficulty in the case of collection from a third party, since the scope of the primary purpose may be difficult to construe. In the context of healthcare there are frequently disclosures of personal information to service providers, such as pathology or radiology services, followed by expert review. These persons may have no way of contacting patients or obtaining consent, and therefore rely upon the primary collector making sufficient disclosures to the patient as to this purpose for collection.

Further, the data must be reasonably necessary for the business activities undertaken by the organisation. Whether the data is reasonably necessary is an objective test. It is important that whatever the purpose of use is, it is disclosed to the customer in the first instance. This over-capture and over retention of data is becoming a focus for regulators.

In the absence of specific consent, health information may only be used for secondary purposes directly related to the primary purpose for which it is collected. There is general regulator dislike of the collection of health information for purposes other than those directly related to the health function.

Further, health information may also be used where the secondary use is required or authorised by or under an Australian law or a court/tribunal order.

4.5 What are the key contractual considerations?

Contractual considerations will include an acknowledgment that parties to the contract will abide by Australian privacy law, including the APPs, and where applicable, do whatever is reasonable to assist the privacy regulator. Contracts will often deal with the obligation of a party to receive appropriate consent to transfer personal information, as well as obligations to de-identify data whenever possible. As noted above, de-identification can be problematic in the healthcare context, particularly where multiple different sources of personal information can be combined to identify an individual. Contracts will also typically create restrictions on disclosure of personal information and cross-border transfer of data. Further, the parties will typically deal with how withdrawal of consent may occur, and specify which party is the preferred party to deal with requests for access, correction and deletion.

Key contractual considerations will invariably depend upon what is being contracted and the context surrounding the procurement.

A common contentious issue is who takes the lead in a data breach situation, where there may be a tension between regulatory requirements and reputational exposure.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Comprehensive rights to personal or sensitive data that is used or collected by digital health organisations will depend entirely on consents by individuals and ongoing compliance with the APPs. It is a requirement under the Privacy Act that an individual reserves the right to withdraw their personal information from an organisation's database. In that sense, it is not possible to secure permanent, ongoing comprehensive rights to Australian personal information.

It is also necessary to ensure that relevant consents are stored for record-keeping purposes, which may be problematic where privacy policies change or are updated. Identification of information which may be health information is also difficult. There may also be obligations imposed on entities which analyse health information, and the consequent obligation to notify individuals of health issues arising from that. This is particularly the case in the context of genetic testing.

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

Other than data inaccuracy, these issues are not really dealt with by Australian law. From a privacy perspective, entities are required to ensure that personal information is up to date; however, this is the limit of obligation. Where an entity receives a request from the relevant individual to correct personal information, the entity must take such steps as are reasonable in the circumstances to correct that information.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

There are a number of issues to consider when sharing personal data. A fundamental issue is whether the individual to which the personal data belongs has provided their consent to its disclosure. This is also subject to the right to disclose for the primary purpose for which the information was collected, as well as secondary purposes directly related to the primary purpose or to which the individual has consented. There is also an obligation on any party which collects personal information to provide a collection statement either before collection or as soon as practical afterwards. In the context of collection from a third party, providing a collection statement can be difficult, and is often overlooked.

There are additional considerations where the personal data is being shared in a cross-border context. It is rare that the jurisdiction the data originates from is the same jurisdiction the data will be housed in. Australian data security laws require that any entity which discloses personal data outside of Australia comply with certain restrictions. These restrictions seek to ensure that the individual is given the opportunity to provide their informed consent, especially with regards to which countries' rules apply.

Further, consideration must be given to whether the data, in the hands of the recipient, identifies an individual. If it does not, it may not be considered personal information, unless it is reasonably possible to re-identify the subject.

5.2 How do such considerations change depending on the nature of the entities involved?

The nature of the entities involved does not really change the issues relating to the sharing of personal information. Where the relevant entity is an organisation and not a public sector entity, it has the right to use and disclose health information for a "permitted health situation", including to undertake research relevant to public health or safety, or to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual in relation to whom data was collected.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The key regulatory requirement applying to data sharing is APP 6 which outlines when an APP entity may use or disclose personal information. APP 6 states that where an APP entity holds personal information that was collected for a particular purpose, it must not use or share the information for a secondary purpose without the individual's consent, or where an exception applies. Disclosure without consent of health information is permitted where the secondary purpose is directly related to the primary purpose.

The information handling requirements imposed by APP 6 do not apply to an organisation if a "permitted health situation" exists. In relation to APP 6, there are three relevant permitted health situations:

- the use or disclosure of health information for certain research and other purposes, consent is impracticable and certain specific guidelines are followed;

- the use or disclosure of a person's genetic information to a genetic relative, in certain strictly limited circumstances; and
- the disclosure of health information to the responsible person for another, where that other cannot provide consent, there is no contrary instruction and certain specified circumstances exist.

Additionally, where the data sharing occurs within a cross-border context, APP 8 applies. Per APP 8, where disclosure of personal information is to a person who is not in Australia, reasonable steps must be taken to ensure that the overseas recipient does not breach the APPs in relation to the information. Generally, where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs.

We note also that, in the context of data collected in the process of clinical research, further restrictions may be imposed by relevant ethical approvals, which may limit or restrict the use of the collected data, even if it is de-identified.

6 Intellectual Property

6.1 What is the scope of patent protection?

The scope of patent protection is determined by the *Patents Act 1990* (Cth) ('Patents Act'). There is no special application process for digital health technologies; the process for applying and obtaining a patent is the same across all technologies. In order to obtain a patent, the invention must be new, useful and inventive. Software and algorithm patents are available, though demonstrating inventiveness for software in particular is problematic. It is noted that recent jurisprudence has confirmed that an AI cannot be an inventor for the purposes of the Patents Act.

Patents give the right to stop others manufacturing, using or selling the invention in Australia without the permission of the patent holder. Patents can be owned by the inventor, a person who has legally obtained rights to the invention from the inventor, or a company or employer of someone who made the invention in the course of their normal duties. A person that holds a patent may also grant a third party a licence to exploit the invention on agreed terms.

The duration of the patent will depend on the type of patent; a standard patent lasts up to 20 years (with extension available for certain pharmaceutical patents) and an innovation patent for up to eight years.

6.2 What is the scope of copyright protection?

In Australia, the scope of copyright protection is determined by the *Copyright Act 1968* (Cth) ('Copyright Act'), which generally reflects the global copyright treaties. Pursuant to the Copyright Act, drawings, art, literature, music, film, broadcasts or computer programs can be protected by copyright. The owner's original expression of ideas is protected, but ideas themselves are not. In Australia, copyright is not required to be registered. Copyright is the most usual form of protection for software and other digital health devices. However, copyright cannot prevent the underlying idea being reproduced.

Copyright protection may be limited by contract, especially in the case of open-source-based software. Similarly, the protection available to data and the outputs of devices is at best limited, and the requirement for a human author persists.

Digital health solutions very commonly use or incorporate open-source components. The scope of various open-source licences can impact the ownership and usage rights of created code, and effectively impact the ability to license new code on other than open-source terms.

6.3 What is the scope of trade secret protection?

Trade secrets are any confidential information, including secret formulas or processes and methods used in production. The protection of a trade secret gives the creator certain rights and privileges depending on the type of protection. Unlike other IP rights, trade secrets are not registered; they are protected by keeping them a secret. The most common way to ensure trade secret protection is by ensuring all involved in the process sign confidentiality and non-disclosure agreements. Additionally, trade secrets are commonly protected by limiting access.

There are some limitations. The scope of protection does not extend to protection from other individuals creating the same product independently and exploiting it commercially. However, it can be very difficult in some contexts to prove independent development, especially where there has been some exposure to the relevant information. There are no exclusive rights and trade secrecy is difficult to maintain over a long period of time or where a number of people know the trade secret.

Australia has a quite advanced confidentiality regime, protected by an extensive body of court-based legal principles. However, Courts are typically unwilling to protect general business information without clear rationale, as it becomes an anti-competitive tool, and hence conflicts with public policy.

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

There are no specific laws or rules applying to academic technology transfers in Australia, but the typical contractual laws apply. Academic institutions will typically have a standard contract that they use for these scenarios, which will include licensing arrangements for the IP and material produced as a result of the agreement.

There have been moves by the Commonwealth Government to produce a harmonised series of documents for use in academic settings. Most academic institutions will aim to retain ownership of IP they develop, and grant exclusive licences, while retaining an ongoing academic licence to use the IP they develop. They particularly like to retain ownership of patents. This can hamper fund-raising and create complexities when it comes to enforcing the patents.

6.5 What is the scope of intellectual property protection for software as a medical device?

SaMDs can be protected via various forms of general IP rights. Novel inventions can obtain patent protection. The underlying software code will typically qualify for copyright protection, though the use of open-source software in the development may infect new code and undermine its commercial worth. Computer-generated works and databases may not be eligible for copyright protection in Australia.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

An AI device cannot be named as an inventor of a patent in Australia. An inventor that is "human" is necessary to apply

for patent protection. This position was confirmed recently by a unanimous decision of the Full Federal Court in *Commissioner of Patents v Thaler*, which determined that an inventor must be a natural person. It is unlikely that the laws in this regard will be changed in the near term.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

There is no broad statutory framework. However, it is becoming increasingly common for rights to be asserted or reserved through contract, particularly to guarantee rights of access on commercial terms. There are no particular rules or laws related to Government-funded inventions in Australia. There is limited funding granted to commercial entities, with most funding being made to universities and research institutes. Some of these agreements may encourage Australian development or exploitation, but have typically not actually intruded into that process. However, we are seeing a trend whereby the Government is being more intrusive in respect of IP developed through activities it funds, in some cases demanding an option over resultant deliverables.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

A critically important consideration applying to collaborative improvements is the ownership structure of IP rights developed through collaboration (e.g. patents, copyrights, technical know-how, research results/data, etc.), and who has the commercialisation lead. Ownership rights are typically governed by the terms of the agreement between the parties. The rights of use of background IP (and improvements to background IP) for commercialisation purposes are also necessary to consider. Such rights may be on a royalty-free or royalty-bearing basis, and exclusive or non-exclusive. Given the limited protection available to data, it is important to consider the protection of data, particularly where publication is a key consideration.

Another important consideration relates to the licensing of existing IP. In collaborative arrangements, licensing is used to manage protected IP that will be shared through the collaborative arrangement.

Additionally, careful consideration should be given to confidentiality obligations applying to the arrangement. Given the nature of collaborative improvements and the risks posed to existing IP, detailed confidentiality regimes are often implemented to protect existing IP rights.

Consideration also needs to be given to the possible application of the competition laws, in particular where the collaboration participants may be actual or potential competitors.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

An important consideration applying to agreements between healthcare and non-healthcare companies is data privacy and compliance. Noting the likelihood of health data being shared, both parties need to ensure they comply with their potentially heightened privacy and data sharing obligations. This is particularly important where the companies are collecting both personal and sensitive health information. Again, de-identification of personal information, and ensuring that appropriate consent has been obtained to transfer, can be critical.

In such agreements, it is particularly important that the healthcare company has properly secured the rights to the healthcare data. If this data has been improperly obtained or secured, the non-healthcare company would be unable to obtain the rights necessary to use such data for its intended purpose. Another important consideration is clarity around ownership of the data shared or produced as a result of this arrangement.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

In Australia, ML is used in a variety of ways and in a variety of clinical settings. ML is commonly used to design and conduct medical research, including clinical trials. The functionality of ML has been used to identify molecular targets and drug-target pairs to assist with drug discovery.

ML is commonly used to expedite computation and data management. Use of ML in this context can reduce costs. ML has been used to analyse molecular structures to correlate them with certain properties, such as the ability to kill bacteria.

ML has been used for direct-for-patient usage through mobile apps. ML has also been used to integrate genomic information into Australia's healthcare systems. There are also potential uses in radiology and pathology to provide assistance in the evaluation of test results. Various companies are seeking to develop algorithms based on data sets, to be used in the context of diagnostic tests.

The arrival of public databases supported by AI which might feed into certain digital pathways has the potential to throw up some complex regulatory and liability issues.

8.2 How is training data licensed?

There are no special rules applying to training data. The licensing of training data depends on the relevant licensee and the terms of each licence agreement. The provenance of such data can be critical to understand, especially if it has been generated in a clinical trial setting. There is clearly a demand for good normal data sets, noting that so many of the data sets around relate to treated persons that are not necessarily representative of the broader community.

However, issues we are seeing emerge are liability/warranty regarding training data, financial return models which seek to lock onto derived data sets and the ownership/entitlement to "insights" that may be garnered from the use or analysis of such data.

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

Following the judgment in *Commissioner of Patents v Thaler* [2022] FCAFC 62, the human inventor of the AI is the *prima facie* owner of IP rights in algorithms. As the Court discussed, there are significant complexities involved in considering to whom a patent should be granted in respect of the AI system's output. The Court considered some potential grantees, which included "the owner of the machine upon which the AI software runs, the developer of the AI software, the owner of the copyright in its source code, the person who puts the data used by the AI to

develop its output, and no doubt others". It should be noted that the ownership may be different as between patents and copyright.

8.4 What commercial considerations apply to licensing data for use in machine learning?

In the context of licensing data for use in ML, the quality of the data is a critical consideration. This has significant consequences for the efficacy of the ML training and validation. It is important to understand the financial model of licensing data, in particular whether it is a "one-off" payment or continues to reach through to secondary uses of the data, for example from the ML outputs (such as an AI model or an algorithm). The treatment of combination data sets from different sources raises complexities when allocating value, similar to the problems with royalty stacking arrangements.

Another important consideration is the applicability of any restrictions to the particular data set, which necessarily fall out of the data set's permitted purpose. Commercially, it is also important to consider who owns the rights to the data produced as a result of the ML.

It is also necessary to ensure sufficient rights to the data to allow combination with other data sets (if necessary) and the requirements, if any, to retain data in perpetuity.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

There are no specific theories of liability applying to adverse outcomes in digital health solutions. Australian tort law will apply where the negligence of a manufacturer or seller causes an adverse outcome.

Australia's consumer law framework also establishes a number of consumer guarantees which provide an additional level of protection. Relevantly, there are consumer guarantees applying to both the sale of goods and provision of services. In relation to goods, suppliers and manufacturers guarantee that goods are of acceptable quality and are reasonably fit for any purpose the consumer or supplier specified. In relation to services, suppliers guarantee that their services are provided with due care and skill and that services will be reasonably fit for any purpose specified by the consumer.

The consumer law framework also incorporates a very broad assurance of the safety of products, which cannot be excluded or limited by contract.

9.2 What cross-border considerations are there?

In circumstances where a product is being sold to Australian consumers, the product, regardless of what it is, must conform to Australian product liability regulatory regimes. In this sense, cross-border considerations do not have an effect on liability. The party that imports the product into Australia is typically deemed as a "manufacturer" for the purposes of the ACL, which requires the importer to comply with the consumer guarantees.

In the context of the TG Act, in order to legally import and supply a medical device in Australia, the device is required to meet the Essential Principles set out in the TG Regulations. The Essential Principles are concerned with ensuring the safe and reliable performance of medical devices. If devices are imported and supplied that do not meet the Essential Principles, civil or criminal penalties may result under the TG Act. As noted above, this may create issues with apps and other SaMDs that are downloaded, creating questions of who has imported the product.

Additionally, overseas manufacturers may be liable under the ACL, which provides a system for manufacturers' liability. Under the ACL, "manufacturer" is defined broadly, to include, amongst others, a person who produces the goods and a person who imports the goods into Australia if at the time of importation, the manufacturer of the goods does not have a place of business in Australia. That system is designed to compensate for loss or damage suffered as a consequence of goods with safety defects.

From a regulatory perspective, overseas manufacturers are unlikely to face regulatory action by the TGA. The regulatory framework is directed towards local sponsors/distributors and not overseas manufacturers. Realistically, the main scope for liability is where there is a class effect, impacting multiple patients.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services typically involve issues such as cyber-security and data protection. Given the sensitive nature of health information, particular care needs to be taken to ensure the data protocols and security mechanisms are effective and appropriate. Where cyber-security issues arise, the providers of Cloud-based services need to have appropriate disaster recovery protocols in place to limit the adverse consequences arising from a breach.

IT service providers who engage with Government health agencies will typically be required to meet certain minimum IT security standards (for example, see the Digital Transformation Agency's Secure Cloud Strategy). Where IT service providers are using Cloud-based services to share health data across borders, compliance with APP 8 is important.

There are also data location rules, for example in the My Health Records Act, as well as State and Territory health records legislation. It is also noted that recent Foreign Investment Review Board guidance suggests that acquisition of an interest in data which may be considered National Security information will be restricted.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Given the highly regulated healthcare market, non-healthcare companies must consider their ability to achieve regulatory compliance within this environment. As part of this, companies must consider the costs involved in obtaining approvals and licences, as well as the costs required to ensure ongoing compliance with the regulatory framework. Companies must also be mindful of the highly regulated marketing environment to ensure their advertising is compliant.

Importantly, non-healthcare companies must consider the heightened data privacy requirements which will apply. These are likely to be more onerous than the requirements such companies are accustomed to.

Non-healthcare companies should also ensure that the pathways to market are clear. This includes determining whether to be considered a consumer-wellness device, or make medical claims and require registration. It is also relevant for the company to contemplate market entry. Given that the Australian regulatory framework is heavily reliant on the EU, Australia often represents a useful follow-up market after European entry. Companies need to ensure a relevant reimbursement pathway, since the

Australian market is heavily dependent on Government subsidy if selling directly to consumers. If targeting providers of healthcare services, it is important to appreciate the different appetites and preferences as between the public and private sector.

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 must ensure that they are aware of the regulatory environment applying to the digital healthcare venture. Firstly, this allows investors to understand the upfront and ongoing costs associated with compliance. This also allows investors to better evaluate the risks of investment, particularly given the move towards increased penalties applying to privacy and data breaches.

In terms of timing, firms should consider the approvals and licensing timeframes as these may delay investment and ultimately any return on investment that materialises. Firms should conduct general investor due diligence, including a thorough review of material IT and IP agreements. It is important that firms understand exactly what it is they are investing in, and the rights or restrictions applying to the venture's ability to commercialise this ownership.

Firms should also consider the company's ownership of, or rights to use, IP and other technology that is fundamental to the business's operations, including the rights to license its products commercially. This includes the title to such assets, issues regarding open-source software, and whether licence terms are sufficiently tailored to allow the proposed commercialisation plan. The steps taken to date in order to commercialise a product should be reviewed to ensure that the steps taken will not need to be repeated in order to comply with the regulatory framework. We tend to see companies either pursuing a US- or EC-centric pathway, and these are not necessarily very compatible. It is also important to consider the success rate of, and timelines for, registration for the therapeutic goods developed by the digital healthcare venture.

Given the heightened cyber-security environment in Australia following recent breaches, investors should take into account what consideration has been given to cyber-security, particularly of personal data. The Australian Government is currently reviewing the Privacy Act and cyber-security standards, and these reforms are expected to increase the privacy protections afforded to individuals and the standards demanded for cyber-security. As part of this, investors should understand the types of data collected and held by the venture.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Currently, there are several barriers impeding the widespread clinical adoption of digital health solutions. Firstly, data privacy, security and the associated consequences of a breach are a significant barrier. Further, as highlighted above, there is an insufficient legislative framework in place to regulate and support the implementation of digital health solutions adequately. The development of bespoke laws relating to digital health technologies may encourage and support more widespread clinical adoption. Further, digital health trends are focusing more on patients rather than clinicians, which can limit take-up.

It is also necessary to note that uptake of emerging technologies can be slow, depending on the capital expenditure necessary, particularly in the public health system. Indeed, given the financial constraints on the overall health system, the offering of additional functionality is hard to sell, unless there is a real, relatively short-term cost-saving dividend to be realised.

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 Australia, the key clinician certification bodies that influence the clinical adoption of digital health solutions are:

- the Australia Health Practitioner Regulatory Agency; and
- the Royal Australia College of General Practitioners.

Additionally, while not being a clinician certification body, the Australian Government has established the Australian Digital Health Agency ('ADHA'), which is a Commonwealth entity which seeks to create a collaborative environment to accelerate adoption and use of innovative digital services and technologies. The ADHA is trying to significantly influence the clinical adoption of digital health solutions by advancing the digital capability of Australia's health workforce. The ADHA is typically taking a guidance role, which results in a need for customers to make their own judgment regarding products.

It is also necessary to consider the role of the Medicare Services Advisory Committee ('MSAC') which appraises new technology and products for public funding. MSAC is responsible for undertaking a health technology assessment to demonstrate quality, safety, efficacy and cost effectiveness of proposed health services. This area is presently under review, and there is considerable uncertainty as to what new model may emerge.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Whether patients who utilise digital health solutions are reimbursed depends upon the particular digital health solution in question. Generally, the Australian Government aims to assist Australians in accessing digital health products and services. This is achieved by subsidising the cost of health-related goods and services, including through the Pharmaceutical Benefits Scheme (subsidies for certain medicines) and the MBS (subsidies for certain health services). The MBS applies to cover the cost of certain medical devices.

In the wake of the COVID-19 pandemic, telehealth services were permanently made available under the MBS. Further, where a patient has appropriate cover, private health insurers are required to pay benefits for products listed on the Prosthesis List which is published by the Australian Government Department of Health and Aged Care. This list includes various digital health products.

However, there is little direct reimbursement for patients for digital health solutions. There are some efforts by private health insurers to encourage wellness activities, and therefore the use of relevant devices. However, this is limited by private health insurance regulations.

10.7 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 following are highlighted as trends or developments which

will affect the adoption and development of various types of digital health solutions:

- Because so much of the health system is funded by Government or private health insurers, the mechanism by which reimbursement levels for these technologies is established is critical, and presently in a state of flux. This is an acute issue where the product or service is patient focused, as opposed to, for example, something more directed to the health ecosystem.
- Australia has, to date, been particularly protective around the sovereignty of its genetic data and health data more generally. There is some specific awareness around data from indigenous persons. It remains to be seen whether this becomes a focus of attention, noting that there is an increasing level of awareness of this issue arising out of various interactions with China.
- The continuing ratcheting up of standards, and penalties for breach of the same, in both the privacy and cybersecurity space. This is being driven by both Federal and State reforms, and also increasingly prescriptive contractual terms.
- The TGA response, if any, to the importer–sponsor issue, and the implications for overseas bodies delivering technology into Australia.
- Companies using digital health tools to get closer to, and more tightly bind themselves to, patients. This trend started with some tools used in the context of clinical trials, to Patient Support Programs with adjunctive digital health support tools, which are becoming increasingly sophisticated and very much part of the patient treatment journey.

Bernard O'Shea is the Head of Norton Rose Fulbright Australia's Life Science sector focus, and has been working in the sector for over 20 years. He has an extensive practice based around the development and commercialisation of products in this sector. His experience encompasses the whole spectrum of regulatory and reimbursement issues the sector confronts. His background in computer science, and many mandates involving privacy and data issues, mean he is adept at assisting clients in the digital health sector. He is recognised by *Chambers Life Sciences Guide* as a Tier one practitioner, and is much sought after for his incisive and strategic advice around emerging issues. Bernard has had the rare privilege of assisting multiple clients bring novel products to market, and is actively involved in assisting multiple digital health companies develop their products, protect their data and satisfy their regulatory obligations.

Norton Rose Fulbright
Level 38, Olderfleet, 477 Collins Street
Melbourne
Australia

Tel: +61 3 8686 6573
Email: bernard.oshea@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

Rohan Sridhar is a commercial, regulatory and intellectual property lawyer based in Melbourne. He practises extensively in the life sciences sector. His experience in the sector covers the full life cycle of pharmaceutical, biotech and med tech products, from discovery to commercialisation. This includes foundational IP licences, research and development collaborations, clinical trials, product registration, pricing and reimbursement, manufacturing, marketing, warehousing, distribution, import/export and recalls. Rohan is also experienced in assisting start-up and spin-out entities with corporate management and fundraising. Rohan has assisted a number of digital health companies to access, develop and commercialise their technologies.

Rohan also advises clients in relation to privacy-related issues, including issues around transfer of data sets and the export of personal information.

Rohan's background in pharmacology enables him to understand the complexity of products existing in this sector and deliver pragmatic and commercial advice to clients.

Norton Rose Fulbright
Level 38, Olderfleet, 477 Collins Street
Melbourne
Australia

Tel: +61 3 8686 6670
Email: rohan.sridhar@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

Austria

Herbst Kinsky Rechtsanwälte GmbH

Dr. Sonja Hebenstreit

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 Austrian law. The Austrian Federal Ministry of Health's definition (see https://www.sozialministerium.at/Themen/Gesundheit/eHealth.html) uses the term "e-health" as the general term, comprising the use of information and communication technologies in health-related products, services (including telemedicine) and processes. The Ministry uses the term "telemedicine" as referring to the provision or support of healthcare services using information and communication technologies, where the patient and the healthcare provider are not present in the same place. This is in line with the definition used by the European Commission who suggested using the term "telehealth" as referring to health-related procedures and "telemedicine" as referring to treating people from a distance (see https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf, page 25).

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

Key emerging technologies are, in particular, artificial intelligence (AI) applications including machine learning, which can contribute, for example, to earlier disease detection and more accurate diagnosis.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health are: compliance with data protection (see sections 4 and 5); the technical requirements (see *GTelG 2012* in question 2.2); and the determination of whether a product qualifies as a medical device (see questions 2.1 and 3.1).

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

There is no reliable data available regarding the digital health market size for Austria, as the available statistics either do not refer to Austria in particular, or only consider specific segments of the total digital health market.

According to a market outlook as published by Statista (see https://de.statista.com/outlook/dmo/digital-health/oesterreich?currency=EUR), the overall revenue for 2022 in Austria in the e-health sector amounts to approximately 420.4 million euros. According to the forecast, a market volume of 607.6 million euros will be reached in 2027, corresponding to an expected annual sales growth of 7.64%. However, this survey does not take into account the public e-health sector in Austria (which is the most relevant sector) as it only includes non-prescription e-health devices and apps.

In another study recently published by Roland Berger (see https://de.statista.com/statistik/daten/studie/1178751/umfrage/umsatz-auf-dem-markt-fuer-digital-health-weltweit/), the volume of the digital health market in 2026 in Germany is estimated to reach 59 billion euros. Consequently, one tenth of this (5.9 billion euros) could be assumed for Austria's digital health market volume in 2026 as a tentative estimate (due to the size ratio between Austria and Germany).

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

As pointed out in question 1.4, there are no reliable figures available on the Austrian digital health market size. Therefore, we cannot provide an overview of the five largest digital health companies by revenue.

Further, please note that a major part of digital health solutions (e.g. Electronic Health Records, known as *Elektronische Gesundheitsakte* (*ELGA*)) applied in Austria are organised by the Austrian state and implemented by the Umbrella Association of Austrian Social Insurance Institutions.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Austrian Physicians Act 1998, Federal Law Gazette I 169/1998, as last amended by the Federal Law Gazette I 65/2022 (*Ärztegesetz* 1998 (*ÄrzteG*)) contains, in principle, regulations on training and admission as a physician, regulations on the exercise of the profession (e.g. group practices), prohibitions of discrimination and regulations on the organisation of the self-administration of physicians (Medical Association). Section 3 of the *ÄrzteG* stipulates that medical advice may only be given by licensed physicians. Section 49 paragraph 2 of the *ÄrzteG* further stipulates that physicians shall practice their profession "personally and directly". This provision is regarded as not generally prohibiting telemedicine, i.e. the individual diagnosis and treatment from a distance, without direct human

contact. The Austrian Medical Association has stated that telemedicine might support the relationship between physician and patient and the treatment process; and that digital monitoring and online contact might be helpful for the diagnosis as well as for the therapy, but has emphasised that a clear legal framework is required for telemedicine services. Currently, no such specific legal framework is in place. In any case, physicians are obliged to comprehensively inform the patient and get the patient's informed consent (likewise), whereas in the case of telemedicine, they need to be in full control of the patient's situation and the telehealth treatment must be for the patient's benefit.

In the context of the referral of patients through online platform operators, the prohibition of commissions according to Section 53 paragraph 2 of the *ÄrzteG* needs to be observed, according to which the physician may not promise, give, take or have promised to himself or another person any remuneration for the referral of patients to him or through him. According to paragraph 3 *leg cit*, activities prohibited under paragraph 2 are also prohibited for group practices (Section 52a) and other physical and legal persons. This means that the collection of commissions from patients is prohibited not only for doctors but also for other third party (natural or legal) persons.

The Austrian Medicinal Products Act, Federal Law Gazette 185/1983, as last amended by Federal Law Gazette I 8/2022, (*Arzneimittelgesetz* (*AMG*)) implements a large number of European Union (EU) directives concerning regulations on medicinal products, in particular Directive 2001/83/EC – Community code relating to medicinal products for human use. The *AMG* contains regulations on the authorisation of medicinal products, regulations regarding marketing, advertising and distribution of medicinal products as well as quality assurance requirements.

The Austrian Medical Devices Act, Federal Law Gazette 657/1996, as last amended by Federal Law Gazette I 192/2021, (*Medizinproduktegesetz* (*MPG*)) as well as the Medical Device Regulation 2017/745 on medical devices (MDR), which entered into force on May 26, 2021, after having been postponed for a year due to the COVID-19 pandemic, constitutes the major regulatory framework for medical devices. The MDR lays down rules concerning the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the EU. The MDR shall also apply to clinical investigations concerning such medical devices and accessories conducted in the EU.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The General Data Protection Regulation, Regulation 2016/679 (GDPR) contains central provisions on data protection. Although the GDPR as a regulation applies uniformly and directly throughout the EU, a large number of opening clauses allow national deviations by Member States. Providers of digital health in particular need to take into account the provisions on the lawfulness of the processing of health data pursuant to Article 9 of the GDPR as well as the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk pursuant to Article 32 of the GDPR.

The Austrian Data Protection Act, Federal Law Gazette I 165/1999, as last amended by Federal Law Gazette I 148/2021, (*Datenschutzgesetz* (*DSG*)) specifies the provisions of the GDPR and, in particular, contains provisions on proceedings before the Austrian data protection authority. For the private sector, the DSG does not provide any provisions for the processing of health data that deviate from the GDPR.

The Austrian Health Telematics Act 2012, Federal Law Gazette I 111/2012 as last amended by Federal Law Gazette I 166/2022, (*Gesundheits-Telematikgesetz* 2012 (*GTelG 2012*)) contains special regulations for the electronic processing of health data and genetic data (please refer to Article 4 Nos 13 and 15 of the GDPR) by healthcare providers. A healthcare provider in the meaning of health telematics is a professional who, as a controller or processor (in the meaning of Article 4 Nos 7 and 8 of the GDPR), regularly processes health data or genetic data in electronic form for the following purposes:

- medical treatment or care;
- nursing care;
- invoicing of health services;
- insurance of health risks; or
- exercise of patient rights.

The *GTelG 2012* also contains detailed regulations on the operation of *ELGA* by ELGA GmbH, which is owned by the Republic of Austria, the Umbrella Association of Austrian Social Insurance Institutions and the federal provinces or their health funds. In the context of *ELGA*, other e-health services have also been introduced, such as the electronic medication prescription (e-medication) or the electronic vaccination pass (e-vaccination pass; see section 24b *et seq. GTelG 2012* as well as eHealth Regulation, Federal Law Gazette II 449/2020, last amended by Federal Law Gazette II 285/2022).

To meet the challenges of the COVID-19 pandemic, (temporary) simplifications to the conditions of transmitting health data via email and fax for healthcare providers have been implemented to the *GTelG* as well.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The *MPG* and, since May 2021, the MDR (see question 2.1) likewise apply to consumer devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In connection with the *GTelG 2012* and Health Telematics Regulation 2013, as last amended by Federal Law Gazette II 506/2013 (*Gesundheitstelematikverordnung (GTelV 2013)*) the Federal Minister for Health is competent for notifications and for the operation of the eHealth directory service according to paragraphs 9 and 10 of the *GTelG 2012*.

In connection with the *ÄrzteG*, the competent authorities are the Austrian Medical Chamber, the respective state governor (*Landeshauptmann*) and the Federal Minister for Health.

The Federal Office for Safety in Health Care (*Bundesamt für Sicherheit im Gesundheitswesen* (*BASG*)) is the central regulatory authority for the medicinal products and medical devices industry. The BASG is responsible, among other things, for the approval of medicinal products, market surveillance and pharmacovigilance, notifications in connection with clinical trials, the control of advertising restrictions and the granting and review of operating licences.

Investigations and assessments are typically carried out by the Austrian Agency for Health and Food Safety (*Österreichische Agentur für Gesundheit und Ernährung* (*AGES*)) on behalf of the BASG.

The Austrian Data Protection Authority (*Datenschutzbehörde* (*DSB*)) is the supervisory authority in Article 4 Section 21 of the GDPR, for the monitoring of data protection law and the assertion of data subjects' rights under the GDPR.

2.5 What are the key areas of enforcement when it comes to digital health?

As far as can be seen, neither the Austrian Medical Chamber nor the *BASG* or the Federal Minister of Health recently took relevant enforcement measures in the regulatory area of digital health and healthcare IT.

In 2018, the *DSB* rendered a major decision regarding the communication between physicians and patients (DSB-D213.692/0001-DSB/2018): according to the *DSB*, patients cannot consent to the (unencrypted) transmission of health data (e.g. medical reports) by physicians. The *DSB* reasoned that the choice of the communication method is a technical/organisational measure according to Article 32 of the GDPR, and that no consent can be provided to insufficient technical/organisational measures.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

According to Recital 19 of the MDR, software qualifies as a medical device when it is specifically intended by the manufacturer to be used for one or more medical purposes, while software for general purposes, even when used in a healthcare setting, or software intended for lifestyle and well-being purposes is not a medical device. The qualification of software, as either a device or an accessory, is independent of the software's location or the type of interconnection between the software and a device. Therefore, as a general rule, software for general purposes, even if used in the healthcare sector, is not a medical device. The manufacturer determines the intended use which is essential for software for general purposes to be differentiated from a medical device.

According to the MDR, manufacturers of medical devices are obliged to carry out a clinical evaluation for all their products – regardless of the risk class – which also includes a post-market clinical follow-up (PMCF). Such clinical evaluation is an essential task of the manufacturer and an integral part of a manufacturer's quality-management system (Article 10 paragraphs 3 and 9f of the MDR). The clinical evaluation is a systematic and planned process for the continuous generation, collection, analysis and evaluation of clinical data for a device. Through the clinical evaluation, the manufacturer verifies the safety and performance of his device, including the clinical benefit.

Furthermore, Regulation No. 207/2012 on electronic instructions for use of medical devices must be observed when providing electronic instructions for use.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

The terms "AI" or "Machine Learning" (ML) are generic and rather technology-neutral terms, as they represent a wide range of different kinds of technologies. To date, there is no definitive legal definition available in the Austrian or European jurisdiction (although the European legislator has increasingly dealt with these topics, as, for example, in its draft for an AI Regulation 2021/0106 (COD), albeit on a rather technology-neutral level). *De lege lata*, the same regulations apply to AI and ML as to all other technologies, for the healthcare sector, in particular, the MDR as well as the GDPR.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Furthermore, the physician needs to decide in each individual case of such telehealth consultation if he can sufficiently control possible dangers despite the lack of physical contact with the patient and whether he has a sufficient information basis for his decisions. In case the physician fears that he does not have a sufficient basis for his medical decision due to lack of physical patient contact, he must advise the patient to physically see a physician.
  Austrian law does not contain rules for the provision of telemedicine or virtual care services in general, but a specific regulation has been issued regarding the provision of teleradiology services: the Medical Radiation Protection Regulation, Federal Law Gazette II 375/2017, last amended by Federal Law Gazette II 353/2020 (*Medizinische Strahlenschutzverordnung*) provides that teleradiology is permitted within the framework of basic and special trauma care as well as in dispersed outpatient primary care facilities of acute hospitals and otherwise only in order to maintain night, weekend and holiday operations for urgent cases.
  According to paragraphs 3 and 4 of the *GTelG 2012*, health service providers may transfer health data and genetic data only if:
  - the transmission is permitted under Article 9 of the GDPR;
  - the identity of those persons whose health data or genetic data is to be transmitted is proven;
  - the identity of the healthcare providers involved in the transmission is proven;
  - the roles of the healthcare providers involved in the transmission are demonstrated;
  - the confidentiality of the transmitted health data and genetic data is guaranteed; and
  - the integrity of the transmitted health data and genetic data is guaranteed.

  In addition, the *GTelG 2012* and *GTelV 2013*, issued by the Federal Minister of Health on the basis of the *GTelG 2012*, contain detailed regulations on encryption and technical implementation of communication.
  The COVID-19 pandemic has led to a massive increase regarding the use and offer of telemedicine services.
  As outlined above in question 2.2, due to the COVID-19 pandemic, (temporary) simplifications to the conditions of transmitting health data (via email and fax) for healthcare providers have been implemented to the *GTelG*.
- **Robotics**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Furthermore, robotics may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes (e.g. robotics for surgical purposes).
- **Wearables**
  Wearables may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes.

- **Virtual Assistants (e.g. Alexa)**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Virtual Assistants in general would not qualify as a medical device. However, natural language processing may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes.
- **Mobile Apps**
  See question 2.6 (Software as a Medical Device).
- **Software as a Medical Device**
  See question 2.6.
- **Clinical Decision Support Software**
  See question 2.6. Further, the GDPR, in particular its provisions on automated individual decision-making (Article 22 of the GDPR), needs to be considered in case personal data is processed.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  See question 2.6 (Software as a Medical Device) and section 8 (AI and Machine Learning).
- **IoT (Internet of Things) and Connected Devices**
  IoT and connected devices may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes (e.g. blood pressure measurement using cloud recording); furthermore, the GDPR needs to be considered in case personal data is processed.
- **3D Printing/Bioprinting**
  Bioprinting raises a wide range of legal and ethical questions. Currently, no *sui generis* regulatory regime governing the entire bioprinting process is in place in Austria. According to the European Commission and the European Medicines Agency, tissue-engineered products might fall under the definition of advanced therapy medicinal products (ATMPs). Additionally, IP and, in particular, patent rights questions might arise.
- **Digital Therapeutics**
  Digital therapeutics is a rather broad term used for device-controlled therapy measures. In particular, digital therapeutics may be subject to the MDR as well as provisions of the GDPR. In view of its high-risk potential, digital therapeutic software shall, according to Annex VIII; Rule 11 of the MDR, be classified as a medical device of at least risk class IIa.
- **Natural Language Processing**
  Natural language processing generally does not qualify as a medical product (e.g. speech recognition in dictation software). However, natural language processing may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes; furthermore, the GDPR needs to be observed.

3.2 What are the key issues for digital platform providers?

One of the main restrictions on digital platforms for individual healthcare is that medical advice may only be given by licensed physicians (Section 3 of the *ÄrzteG*; see question 2.1).

Furthermore, online platform operators should keep in mind the prohibition of commissions in Section 53 paragraph 2 of the *ÄrzteG*, according to which the physician may not promise, give, take or have promised to himself or another person any remuneration for the referral of patients to him or through him. Moreover, these activities are also prohibited for group practices (Section 52a) and other physical and legal persons. This means that the collection of commissions from patients is prohibited not only for doctors, but also for other third party (natural or legal) persons.

Digital platforms must take appropriately (high) technical/organisational measures for data security when processing health data (Article 32 of the GDPR) and the *GTelG 2012* needs to be considered in case personal health data is processed.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The processing of personal data must comply with the GDPR. When processing health data, Article 9 of the GDPR applies; according to that provision, the processing of health data in connection with healthcare providers is lawful only if (only the most relevant legal grounds have been included in the following):

- the data subject has given explicit consent to the processing of their personal data for one or more specified purposes (Article 9 Section 2 letter a of the GDPR);
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (Article 9 Section 2 letter c of the GDPR);
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health, social care, treatment or the management of health or social care systems (Article 9 Section 2 letter h of the GDPR);
- pursuant to a contract with a health professional, when the personal data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy (Article 9 Section 2 letter h in connection with Section 3 of the GDPR); and
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices (Article 9 Section 2 letter i of the GDPR).

4.2 How do such considerations change depending on the nature of the entities involved?

In principle, the provisions of the GDPR apply equally to all entities. However, the legal grounds in Article 9 Section 2 letter h only apply to data processing, when the personal data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy. Therefore, entities not subject to professional secrecy cannot rely on this legal ground.

4.3 Which key regulatory requirements apply?

The general regulatory provisions of the GDPR apply, namely the principles of transparency, lawfulness, purpose limitation, data minimisation, proportionality, accuracy, data security and accountability. As in the context of digital health services, large-scale processing of sensitive personal data will be involved, the entity providing such services is required to designate a Data Protection Officer in accordance with Article 37 para 1 lit c of the GDPR. Furthermore, a data protection impact assessment (DPIA) might be required (e.g. according to Article 35 para 3 lit b of the GDPR) before processing is started.

4.4 Do the regulations define the scope of data use?

Yes, please refer to question 4.1. Some legal grounds of Article 9 impose limitations on the purpose of the processing (e.g. preventive or occupational medicine; see question 4.1). Neither the GDPR nor the DSG contain regulations defining the scope of data use in the context of digital health.

4.5 What are the key contractual considerations?

If the processing is based on explicit consent of the data subject, such valid and fully informed consent needs to be given by the patient/data subject. Furthermore, according to Article 28 of the GDPR, any data controller must conclude a written data processing agreement with processors, which must contain the minimum contents specified therein. In the event where more than one controller jointly decides on the respective processing, an agreement on joint controllership needs to be concluded between these controllers.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The key legal issues and therefore greatest challenge with regard to securing comprehensive rights to personal data is that the personal data must be collected in accordance with the principles pursuant to Article 5 of the GDPR and that a corresponding legal basis must be guaranteed for each processing at all times. Successfully facing those legal issues is not only important because of the severe penalties for the unlawful processing of personal data provided for in the GDPR (Article 83 of the GDPR); it is also vital for any digital (health) application using personal data to safeguard that such use is lawful as otherwise the application risks being shut down by the data protection authority at any time.

However, the GDPR is only applicable to personal data. Therefore, if no personal data according to Article 6 or Article 9 of the GDPR is processed, a specific right to process the data is not necessary from a data protection point of view.

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

A data subject may request the respective data controller to correct any inaccurate or incomplete personal data. If the data is not corrected by the processor or if the data subject is of the opinion that the processing of the personal data violates the GDPR, the data subject may file a complaint with the data protection authority and/or a (civil) lawsuit against the controller requiring the correction of the inaccuracy.

The Federal Act on Equal Treatment, Federal Law Gazette I 66/2004, as last amended by Federal Law Gazette I 16/2020 (*Gleichbehandlungsgesetz* (*GlBG*)) focuses on equal treatment in the world of work and in other areas. No one shall be discriminated because of his gender, age, ethnical affinity, religion or belief or sexual orientation. A person who is subject to discrimination can claim the establishment of the non-discriminatory condition and compensation for the pecuniary loss and for the personal impairment suffered.

The Federal Act on the Equality of Persons with Disabilities, Federal Law Gazette I 82/2005, as last amended by Federal Law Gazette I 32/2018 (*Bundes-Behindertengleichstellungsgesetz* (*BGStG*)) aims to eliminate or prevent discrimination against persons with disabilities. This is to ensure equal participation of persons with disabilities in society and to enable them to lead a self-determined life.

No one may be discriminated against on the basis of a disability. In the event of a violation of this prohibition, the person concerned is in any case entitled to compensation for the pecuniary loss and for the personal impairment suffered.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Sharing health data between healthcare professionals is subject to the *GTelG 2012* (see question 3.1 for the conditions of sharing under the *GTelG 2012*), sharing of data between individuals other than healthcare professionals is solely subject to the GDPR; see question 4.1 for sharing within the EU. For sharing with an individual located outside the EU/EEA, the GDPR provisions on the transfers of personal data to third countries or international organisations apply.

5.2 How do such considerations change depending on the nature of the entities involved?

Sharing of data between individuals other than healthcare professionals is solely subject to the GDPR (see question 4.1). In this case, the *GTelG 2012* does not apply.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please refer to questions 4.3 and 5.1.

6 Intellectual Property

6.1 What is the scope of patent protection?

Technical inventions that are novel, that, considering the state of the art, are not obvious to a person skilled in the art, and that can be applied in the industry, can be subject to patent protection under the Austrian Patent Act 1970, Federal Law Gazette I 259/1970, as last amended by Federal Law Gazette I 61/2022 (*Patentgesetz 1970* (*PatG 1970*)). Only a natural person can qualify as an inventor.

The inventor can either file a patent himself or transfer his right to a third party. The patent owner has the exclusive right to manufacture, put into circulation, offer for sale and use the patented invention for the duration of the patent, namely up to 20 years. A "prolongation" of the patent protection can only be achieved by virtue of a Supplementary Protection Certificate, a *sui generis* intellectual property right available for specific medicines and plant protection products.

Software programs as such cannot be subject to patent protection.

6.2 What is the scope of copyright protection?

Under Austrian law (the Austrian Federal Law on Copyright in Works of Literature and Art and on Neighbouring Rights, Federal

Law Gazette I 111/1936, as last amended by Federal Law Gazette I 244/2021 (*Urheberrechtsgesetz* (*UrhG*)), a work is defined as an "original intellectual creation" (Section 1 paragraph 1 of the UrhG). The author has the exclusive right to use his work in the way defined by the law (in particular: reproduction right; distribution right; rental and lending right; broadcasting right; right of public performance; and of communication to the public of a performance, making available right). Protection starts in the very moment of creation, which means that no registration with any authority is required for protection under the Copyright Act. According to Section 1 paragraph 1 of the UrhG, works can be original intellectual creations in the area of literature (including computer programs), musical arts, visual arts and cinematography. In principle, only creations of human beings are regarded as works and protected by copyright; and the legislator has so far not provided for specific rules for "computer-generated works". According to current doctrine, computer-generated works might still be subject to copyright protection and the programmer as the author in case the programmer, although not directly involved in the creation of the work, has created the creative framework for it by programming the appropriate autonomy.

The Copyright Act further grants exclusive rights to performers (such as singers, dancers and actors) as well as phonogram producers, photographers, broadcasters and the producers of a database (*sui generis* right).

6.3 What is the scope of trade secret protection?

The Unfair Competition Act, Federal Law Gazette I 448/1984, as last amended by Federal Law Gazette I 110/2022 (*Bundesgesetz gegen unlauteren Wettbewerb,* (*UWG*)) contains in its Sections 26a *et seq.* civil law and civil procedural law rules for the protection of trade secrets. According to the legal definition in Section 26b of the UWG, information that is:

- secret, namely not known or readily accessible by persons that normally deal with the respective information;
- of commercial value because of its secrecy; and
- subject to reasonable measures to be kept secret,

qualifies as a trade secret.

It must be proven that reasonable measures have been taken; these may include specific IT security measures and the restricted accessibility of secret information (e.g. only accessible to particularly trustworthy employees).

A variety of information may be regarded as a trade secret, for example, inventions and designs (if not protected as a patent or design) as well as not otherwise protected information such as production processes, customer information, business models or the like.

The owner of a trade secret is particularly entitled to claims of forbearance, removal and damages against anyone who unlawfully acquires, uses or discloses his trade secrets.

Section 26h of the UWG contains specific rules to ensure the protection of trade secrets in civil proceedings.

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

Universities may claim any service invention made by one of its employees within three months of notification of the invention (see Section 106 paragraph 2 of the University Act 2002, Federal Law Gazette I 120/2002, as last amended by Federal Law Gazette I 177/2021, (*Universitätsgesetz 2002* (*UG 2002*)) in connection with the Patent Act's rules on service inventions); the employee is generally entitled to a special remuneration if the university makes use of that right. If the university does not claim the invention, the general rule applies, namely, the inventor is entitled to the invention. Regarding the commercialisation of technology developed by its researchers, Austrian universities pursue different strategies – from outlicensing to transferring IP and increasingly, additionally acquiring shares in its spin-out companies.

6.5 What is the scope of intellectual property protection for software as a medical device?

There are no specific rules for Software as a Medical Device from an intellectual property protection point of view, i.e. the software as such will be protected by copyright law; whether patent protection can be sought needs to be assessed individually.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

Exclusively natural persons can be named and registered as an inventor for patents, as the legal institution of an "e-person" is not recognised in Austrian law. If an AI device should "invent" a patentable product, this goes back to the actual inventor (natural person) of the AI device.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

In principle, the rules of the Patent Act regarding service inventions (section 7 *et seq.* Patent Act) apply to inventions made within academic (see question 6.4), or other public-funded institutions (see e.g. the Federal Act on General Matters Pursuant to Article 89 of the GDPR and the Research Organization (*Forschungsorganisationsgesetz,* (*FOG*)), Federal Law Gazette I 341/1981, as amended by Federal Law Gazette I 116/2022, and Federal Act on the Institute of Science and Technology Austria (*IST-Austria-Gesetz* (*ISTAG*)), Federal Law Gazette I 69/2006, as amended by Federal Law Gazette I 75/2020).

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

If not otherwise regulated, collaborative improvements belong to the respective inventors of such improvement, whereas the ownership of the basis technology will not change following such improvements. The ownership, and eventually licences regarding the use of such collaborative improvements, is therefore usually regulated precisely and meticulously in the respective agreements containing the regularities for the collaboration.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

Besides regulatory considerations (see question 2.1), the general principles apply, namely Austrian law's (federal) rules on commercial contracts, providing regulations on the general principles and specific contract types.

The general principles of contracts as well as a large number of specific contracts are regulated in the Civil Code (*Allgemeines Bürgerliches Gesetzbuch*) and in the Commercial Code (*Unternehmensgesetzbuch*).

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Many digital health devices use machine learning (such as, e.g. in the field of radiology, and generally in diagnosing). Machine learning is substantial for developing smart digital health solutions and is said to have the potential to substantially transform healthcare both for patients and medical professionals.

8.2 How is training data licensed?

The protection and licensing of training data does not differ from any other protection of information, creations and data. If the training data were created in a specific way by a human being (e.g. texts for speech recognition) they may be subject to copyright protection (see question 6.2). In addition, training data may also be subject to trade secrecy protection (see question 6.3). For using such data, a licence agreement needs to be concluded with the respective right holder.

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

Software may, in principle, be protected by copyright (see question 6.2). However, copyright protection requires an "intellectual creation" which, according to Austrian law, can only originate from the thoughts of a human being. Assuming that the improvement could have only been achieved because the programmer has "instructed" the algorithms correspondingly, it could be argued that the programmer is the author of the work (the improvement, which is furthermore depending on the basis work). In case the improvement was indeed created without active human involvement it does not qualify for copyright protection.

8.4 What commercial considerations apply to licensing data for use in machine learning?

For the provision of data for use in machine learning, the licensor is often commercially interested not only in remuneration but will often have an interest in technical cooperation, under which the licensor acquires rights to the results of the machine learning. Therefore, the provision of data for use in machine learning is often based on a broad cooperation.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

No specific liability schemes for adverse outcomes in digital health solutions exist under Austrian law. Austrian tort law generally stipulates that the tortfeasor is obliged to compensate for those damages which he has culpably and unlawfully caused. In addition to material damages, the injured party is also entitled to receive compensation for pain and suffering in case of injuries to the body and/or health. Punitive damages are not paid in Austria. Unlawfulness in the context of the provision of health services typically results from the violation of contractual obligations (e.g. duties of care, non-valid consent to the treatment because of incorrect or insufficient information). The liability for personal injury cannot be excluded and/or limited by contract.

The Austrian Product Liability Act, Federal Law Gazette 99/1988, last amended by Federal Law Gazette I 98/2001, (*Produkthaftungsgesetz* (*PHG*)) transposes in particular Directive 1999/34/EC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. If a defect in a product kills a person, causes bodily injury or damage to health, or damages a physical object other than the product, the manufacturer, distributor and the importer shall be liable for damages under Section 1 of the PHG. Liability is subject to the product being defective and therefore not offering the safety that can be expected under consideration of all circumstances (Section 5 paragraph 1 of the PHG). However, liability shall be excluded if the manufacturer, distributor or importer proves that: (i) the defect is due to a legal provision or official order with which the product had to comply; (ii) the characteristics of the product are in accordance with the state of the art in science and technology at the time when the person making the claim put it into circulation; or (iii) where the person making the claim has manufactured only one basic material or part of a product, the defect was caused by the design of the product into which the basic material or part has been incorporated or by the instructions of the manufacturer of that product.

9.2 What cross-border considerations are there?

In case of any cross-border provision of digital health services, the respectively applicable law and the applicability of regulatory requirements have to be determined.

In case it is intended that foreign doctors provide telemedical treatment to Austrian patients, these require an Austrian professional licence if their activity does not fall under Section 37 of the *ÄrzteG* (freedom to provide services). According to Section 37 of the *ÄrzteG*, nationals of EU/EEA Member States or Switzerland who lawfully exercise the medical profession in another EU/EEA Member State or Switzerland may, from their foreign professional domicile or place of employment, practice medicine in Austria only if the medical activity is temporary and occasional, which must be assessed on a case-by-case basis, in particular on the basis of the duration, frequency, regular return and continuity of the activity.

Further considerations refer to the law applicable in a cross-border scenario: the provision of health services is typically based on a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the patient) with another person acting in the exercise of his trade or profession (the medical professional). According to Article 6 Regulation 593/2008 on the law applicable to contractual obligations (Rome I) the contract as well as the contractual liability derived therefrom shall therefore be governed by the law of the country where the consumer has his habitual residence, provided that the professional: (i) pursues his commercial or professional activities in the country where the consumer has his habitual residence; or (ii) by any means, directs such activities to that country or to several countries including that country. Cross-border healthcare providers therefore typically have to comply with the laws of a large number of countries in which they offer their services.

For claims arising from product liability under the PHG, pursuant to Article 5 Regulation 864/2007 on the law applicable

to non-contractual obligations (Rome II), the law applicable shall be: (i) the law of the country in which the person sustaining the damage had his habitual residence when the damage occurred, if the product was marketed in that country; or, failing that; (ii) the law of the country in which the product was acquired, if the product was marketed in that country; or, failing that (iii) the law of the country in which the damage occurred, if the product was marketed in that country. As a result, providers of medical devices must therefore also comply with a large number of legal systems in the area of product liability.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Like for healthcare IT in general (see question 1.3) the main legal issues for Cloud-based services for digital health are the compliance with data protection (see sections 4 and 5), the technical requirements for telehealth (see *GTelG 2012* in question 2.1) as well as determining whether a product qualifies as a medical device (see questions 2.1 and 3.1).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The intended business model and the actual product or service that shall be offered needs to be carefully examined from a legal perspective, in particular from a regulatory (e.g. the Physicians Act and limitations of telemedicine, MDR) and from a data protection point of view; in addition, the applicability and requirements of the *GTelG 2012* need to be considered. Furthermore, if such is relevant, depending on the business model, it should be assessed whether reimbursement of the services in question by the state sick funds is at all possible.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

A comprehensive regulatory (including data protection) due diligence is advisable in order to safeguard that the business the digital healthcare venture intends to undertake or already undertakes complies with all applicable legal requirements.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

One key barrier is Section 3 of the ÄrzteG, according to which medical advice may only be given by licensed physicians. Furthermore, the funding and/or (non-)reimbursement of digital health solutions by the state sick funds is a major issue; non-reimbursement would be a barrier to the widespread use of digital health solutions. Since the COVID-19 pandemic, the sick funds have expanded reimbursement of telemedicine treatment.

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?

From a formal/legal point of view, under Austrian law, clinician certification bodies might not be of specific relevance, even though acceptance or endorsement of a specific digital health solution by such body might prove compliance with specific quality standards or recommendations issued by such body. However, within a possible legislative process, these bodies might typically be consulted. The introduction of digital health solutions is in principle exclusively governed by law.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

The Austrian state provides for a central digital health solution, namely *ELGA* (see question 2.2), which is owned by the Republic of Austria, the Umbrella Association of Austrian Social Insurance Institutions as well as the federal provinces or their health funds. The services that are provided within *ELGA* (e.g. e-medication) do not have to be paid separately by patients and are covered by the general health insurance. The legal requirements of *ELGA* are set forth in the *GTelG 2012*.

Any other digital health solution an individual might want to use would need to be prescribed by a physician and be appropriate in order to be reimbursable by the Umbrella Association of Austrian Social Insurance Institutions.

10.7 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 COVID-19 pandemic has led to a massive increase regarding the use and offer of telemedicine services in Austria, including non-contact medication prescriptions and the COVID-specific symptom check and triaging via app. With the help of these telemedicine applications, it was possible to find rapid solutions for patient care during the pandemic.

In addition, reimbursement by sick funds for telemedicine treatments was expanded and the use of video consultations mostly for initial consultations, therapeutic discussions and review of findings increased.

These developments have proven useful and will therefore be kept and be further expanded in fields where telemedicine can be reasonably used, as telemedicine offers enormous potential for the high-quality and cost-effective provision and support of healthcare services and ensures access to high-quality healthcare, not only in centres but also on the periphery. Consequently, it is probable that the Austrian healthcare system will further expand access to telemedicine and e-health solutions.

Dr. Sonja Hebenstreit is a Partner at Herbst Kinsky Rechtsanwälte GmbH, which she joined in 2005. She specialises in the fields of intellectual and industrial property law, unfair competition, life sciences and data protection. Sonja Hebenstreit represents Austrian and international clients, including biotech start-ups as well as numerous pharmaceutical and medical devices companies, in a variety of regulatory issues, licensing and other contractual matters as well as in data protection, unfair competition and reimbursement matters.

Herbst Kinsky Rechtsanwälte GmbH
Dr. Karl Lueger-Platz 5
A-1010 Vienna
Austria

Tel: +43 1 904 2180
Email: sonja.hebenstreit@herbstkinsky.at
URL: www.herbstkinsky.at

The Firm

Since its establishment in 2005, Herbst Kinsky has become one of Austria's leading commercial law firms. Its specialised and highly committed lawyers combine many years of experience gained abroad and in reputable Austrian law firms. The Firm's practice covers a full range of services in all areas of commercial, corporate, civil and public law, including banking, insurance and capital markets, corporate and M&A, IP, IT and life sciences, merger control, antitrust and competition, data protection, real estate, dispute resolution and arbitration. The Firm has established a particularly strong presence in the field of life sciences and healthcare.

Our Clients

The Firm's clients range from large international privately held and publicly listed companies, banks, insurance companies and private equity investors to small and mid-size business entities, as well as start-ups. Clients cut across many different industries, including life sciences, energy, information technology, financial institutions and insurance.

www.herbstkinsky.at

Belarus

Sorainen


Kirill Laptev


Marina Golovnitskaya

1 Digital Health

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

Under Belarus law, digital health is a set of information systems and resources, and information and communication technologies, functioning in the healthcare sector on the basis of common principles and rules, providing information interaction between organisations and citizens, as well as serving their information needs. This definition is included in the Concept for the Development of Digital Health in the Republic of Belarus for the period up to 2022 (**Concept**), approved by the order of the Ministry of Healthcare. The Concept sets key goals, objectives and principles of digital health development as well as expected results.

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

One of the main directions of digital health in Belarus is the creation and use of the Centralised Healthcare Information System (**CHIS**), which is an integrated information system that provides centralised storage and processing of medical information, as well as users' access to it in accordance with the established procedure. The main roles of the CHIS include:

- e-health development;
- collection, accumulation and storage of information regarding the state of patients' health;
- protection of information;
- transfer of medical services to electronic form;
- creation of a unified electronic archive of medical information about patients based on the patient's electronic medical record; and
- provision of patient access to healthcare services using the patient's personal electronic account, etc.

The CHIS includes information:

- contained in the patient's electronic medical record and other electronic medical documents;
- regarding healthcare organisations;
- regarding people who receive medical care;
- regarding statistical observations in the field of healthcare; and
- regarding high-tech medical care organisations, etc.

Receiving, transferring, collecting, processing, accumulating, storing and providing medical information contained in the CHIS is performed by healthcare specialists without consent of patients or their representatives, unless they have refused to enter information constituting medical secrecy into the CHIS.

The system of electronic prescriptions is also worthy of note. Its principle is that doctors issue e-signed prescriptions in electronic form through a special system where healthcare organisations and pharmacies are registered. Patients can obtain prescribed pharmaceuticals upon presentation in pharmacies of special personal cards issued by healthcare institutions where their electronic prescriptions are reflected. To obtain the special personal card of medical care the patient should verify their passport data. The list of pharmacy chains where patients can purchase pharmaceuticals with electronic prescriptions is limited but becomes broader each year. It is worth mentioning that an electronic prescription is issued only if there is written consent from the patient with regard to processing personal data and information constituting medical secrecy. This written consent is drawn up in the form of a paper document signed by the patient.

Moreover, telemedicine technologies are currently the most developed part of the digital health sector in Belarus, enabling the provision of medical assistance to patients remotely, conducting medical monitoring and medical examinations, as well as consultations between medical specialists. Please see question 3.1 for details.

1.3 What are the core legal issues in digital health for your jurisdiction?

Although the development of digital health in Belarus was planned in the Concept to take place in 2022, at the time of writing (January 2023) the CHIS is still not functioning and the use of telemedicine technologies is working in a fragmented way. In this regard, the core legal issue and the main vector for Belarus is the further development and improvement of a legal base with specific standards and regulations for the performance of healthcare activities using information technologies.

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

There is no publicly available information on the digital health market size in Belarus.

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

The CHIS is a state information system, the general coordination of which is carried out by the Ministry of Healthcare. The Republican Scientific and Practical Centre for Medical

Technologies, Informatisation, Management and Economics of Health is responsible for the informatisation in the healthcare sector. Consequently, the main players currently in digital health in Belarus are the state, state authorities and organisations, so it is not possible to highlight the five largest companies in the digital health sector.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Regulation of digital health in Belarus is covered by the Law of the Republic of Belarus "On Healthcare". It establishes the specifics of the regulation of health information support.

There are also acts of the government and sectoral authorities that regulate digital health: the Resolution of the Council of Ministers "On the Functioning and Use of the Centralised Healthcare Information System"; 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.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The general rules for the regulation of information protection, including personal data, creation and use of information resources, information systems and information networks are contained in the Law of the Republic of Belarus "On Personal Data Protection" (**Law on PDP**) and the Law of the Republic of Belarus "On Information, Informatisation and Data Protection".

The particularities of the legal regulation of information relationships concerning state secrets and medical secrets, as well as specifics in terms of personal data protection, are regulated by the Law of the Republic of Belarus "On State Secrets" and the Law of the Republic of Belarus "On Healthcare".

Regulation of the anti-kickback issues is stipulated in the Law of the Republic of Belarus "On Measures to Prevent Legitimisation of Money Obtained by Criminal Actions, Financing of Terrorist Activities and Financing Weapons of Mass Destruction Proliferation".

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Belarus legislation does not contain legal regulation of consumer healthcare devices or software in particular.

In Belarus, medical devices means 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. This definition, as well as general questions of regulation of the circulation of medical products, is contained in the Law of the Republic of Belarus No. 2435-XII dated 18 June 1993 "On Healthcare".

Being essentially a software, consumer healthcare devices should not be subject to medical device regulations, unless they have suitable features. For example, if relevant consumer healthcare devices are accompanied with certain hardware, they may be subject to medical device regulations. As a general rule, medical devices are permitted for production, sale and medical use in Belarus after their state registration or registration within the Eurasian Economic Union.

The procedure for state registration of medical devices is set out in the Regulation on state registration (re-registration) of medical devices and medical equipment, approved by the Resolution of the Council of Ministers of the Republic of Belarus No. 1269 dated 2 September 2008.

The Law of the Republic of Belarus "On the Protection of Consumer Rights" deals with relations in the field of consumer rights protection, including rights of the consumers of medical devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The regulatory authority for digital health is the Ministry of Healthcare of the Republic of Belarus. The Ministry of Healthcare has the role of organising the provision of healthcare to the population, providing pharmaceuticals and medical devices, conducting scientific research and training scientists, and providing information support in the field of healthcare. There are state organisations under the supervision of the Ministry of Healthcare which assist it in carrying out its functions and duties.

2.5 What are the key areas of enforcement when it comes to digital health?

The key areas of enforcement relating to digital health are confidentiality, data security, data protection obligations, legal qualification as a medical device, medical secrecy regime, liability in case of damage, safety and intellectual property specifics.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Please see our response to question 2.3. Under Belarus law, software should not be identified as a medical device, but may be an accessory necessary for the use of a medical device, unless they have suitable features (e.g. accompanying hardware).

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Belarus legislation does not contain legal regulation of artificial intelligence/machine learning powered digital health devices or software solutions. Being essentially a software, they should not be subject to medical device regulations, unless they have suitable features (please see question 2.3). For example, if relevant software is accompanied with certain hardware, it may be subject to medical device regulations. As a general rule, medical devices are allowed for production, sale and medical use in Belarus after their state registration or registration within the Eurasian Economic Union.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Telemedicine technologies are one of the most innovative IT manifestations in healthcare in Belarus.
  Personal data protection in the framework of medical secrecy regime seems to be the core issue in telemedicine regulation. The introduction of an intelligent system for remote monitoring of health (telemedicine, robotics in high-tech operations) is provided for in the program of social and economic development of the Republic of Belarus for 2021–2025.
  Telemedicine technologies are defined as information technologies which provide for remote interaction of healthcare specialists between each other and with patients for the purposes of:
  - conducting medical consultations;
  - providing an additional medical opinion on the assessment of a patient's health status, clarifying the diagnosis, determining the prognosis and methods of medical care;
  - healthcare specialists remotely carrying out medical monitoring of a patient's health after an in-person appointment (examination, consultation); and
  - conducting medical examinations.

  Thus, taking into account the purposes of using telemedicine technologies, two main types of use of such technologies can be distinguished in Belarus: telemedicine counselling; and medical care with the use of telemedicine technologies.
  Telemedicine counselling does not provide for direct involvement with a patient – it is instead a tool for:
  - elimination of the negative consequences of staffing issues (when a healthcare organisation does not have the necessary kind of specialised physician); and
  - interactions between doctors of the same profile who have different skill levels, making it possible to make better decisions regarding the diagnosis and treatment of patients (a kind of "online consultation").

  The provision of medical care using telemedicine technologies involves interaction between a doctor and a patient and, in fact, can replace a regular face-to-face visit to a healthcare organisation.
- **Robotics**
  There are no specific robotics regulations in Belarus healthcare.
  The introduction of an intelligent system for remote monitoring of health (telemedicine, robotics in high-tech operations) is provided for in the program of social and economic development of the Republic of Belarus for 2021–2025.
  Legal qualification as a medical device, personal data protection in the framework of medical secrecy regime and liability in case of damage seem to be the core issues in case special regulation is introduced with regard to robotics in healthcare.
- **Wearables**
  There are no specific wearables regulations in Belarus healthcare.
  Legal qualification as a medical device, considering wearables may have functions different to a medical nature, processing personal data considering medical secrecy regime and safety seem to be the core issues in case special regulation is introduced with regard to wearables in healthcare.
- **Virtual Assistants (e.g. Alexa)**
  There are no specific virtual assistants regulations in Belarus healthcare.
  To the best of our knowledge, virtual assistants (such as Alexa or Siri) do not have special medical functions. They potentially can be used for collecting medical information from patients. In this case, legal qualification as a medical device and processing personal data considering medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to virtual assistants in healthcare.
- **Mobile Apps**
  There are no specific mobile app regulations in Belarus healthcare.
  To the best of our knowledge, the Eurasian Development Bank, an international financial institution whose members are Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan, launched the mobile app "Travelling without COVID-19" during the relevant pandemic. This app serves the purposes of collecting results of COVID-19 tests and demonstrating them when crossing borders.
  The implementation of mobile applications in healthcare is included in the priorities of the Commonwealth of Independent States, of which Belarus is a member.
  Legal qualification as a medical device and processing personal data considering medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to mobile apps in healthcare.
- **Software as a Medical Device**
  There are no specific healthcare regulations in Belarus with regard to software considered as a medical device.
  Legal qualification as a medical device considering such software has other components and may have functions different to a medical nature and processing personal data considering medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to software considered as a medical device.
  Please also see the comments regarding legal protection of such software from an intellectual property perspective in question 6.5.
- **Clinical Decision Support Software**
  There are no specific healthcare regulations in Belarus with regard to Clinical Decision Support Software.
  Legal qualification as a medical device, processing personal data considering medical secrecy regime and medical ethics seem to be the core issues in case special regulation is introduced with regard to Clinical Decision Support Software.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  There are no specific artificial intelligence/machine learning regulations in Belarus healthcare.
  Processing personal data considering medical secrecy regime, liability in case of damage and interaction with healthcare specialists seem to be the core issues in case special regulation is introduced with regard to artificial intelligence/machine learning in healthcare.
  Please also see the more detailed comments in questions 8.1–8.4.
- **IoT (Internet of Things) and Connected Devices**
  There are no specific IoT regulations in Belarus healthcare. IoT-connected devices can be used to provide remote health monitoring and emergency alert systems.

Legal qualification as a medical device and processing personal data considering medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to IoT and connected devices in healthcare.

- **3D Printing/Bioprinting**
  There are no specific bioprinting regulations in Belarus healthcare.
  The development of new methods of treatment based on bioprinting is provided for in the program of social and economic development of the Republic of Belarus for 2021–2025.
  Licensing such type of activity, legal qualification from civil law and intellectual property perspective, medical ethics and liability seem to be the core issues in case special regulation is introduced with regard to bioprinting.
- **Digital Therapeutics**
  There are no specific healthcare regulations in Belarus with regard to digital therapeutics.
  Licensing such type of activity, legal qualification as a medical device, processing personal data considering medical secrecy regime, liability in case of damage and interaction with healthcare specialists seem to be the core issues in case special regulation is introduced with regard to digital therapeutics.
- **Natural Language Processing**
  There are no specific healthcare regulations in Belarus with regard to natural language processing.
  Legal qualification as a medical device and processing personal data considering medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to natural language processing in healthcare.

3.2 What are the key issues for digital platform providers?

Digital platform/solution providers face issues derived either from lack of specific regulation in relevant regulation or continuous development of the legal framework in the sphere.

Providers of those digital platforms that are being developed and operated as a part of state digital healthcare mostly focus their efforts on the creation and implementation of platforms in line with scope, time and budgets agreed for their development.

All the issues referred to in answer to question 3.1 above are relevant for digital platform providers, as well as specific obligations related to platform operation that may be prescribed in the legal acts regulating particular digital solutions/platforms (e.g. those developed for the use of telemedicine in Belarus).

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The key issue to consider for use of personal data is the correlation between general requirements for personal data protection and specific rules established in the healthcare sphere. Personal data operated in healthcare may also be subject to medical secrecy regime, which triggers protection of the same information both from personal data and medical secrecy perspectives. Under medical secrecy, the following information should be protected:

- information about a patient's request for medical assistance and his/her health status;
- data about diseases;
- diagnosis;
- possible methods of medical assistance;
- risks related to medical intervention as well as alternatives to it; and
- other data, including personal data, obtained when providing medical assistance, and results of postmortem examinations.

4.2 How do such considerations change depending on the nature of the entities involved?

A service provider shall take into account territorial scope of the Law on PDP, which does not specify whether it has an extraterritorial effect.

The definition of the operator (analogue to the controller under the GDPR) comprises "other organisations" without clarification whether foreign organisations processing personal data of Belarusians are concerned. However, the Belarusian Data Protection Authority (**DPA**) currently maintains the position that the scope of the Law on PDP is limited to the territory of Belarus and does not apply to foreign organisations having no local presence. Therefore, providing services and performing processing of personal data from abroad by a non-Belarusian legal entity without local presence should not fall in the direct scope of the Law on PDP application.

Application of the Law on PDP does not differ depending on the state/private type of company ownership. Laws may establish specific requirements/obligations for personal data processing, which can be used as a valid legal basis therefore.

4.3 Which key regulatory requirements apply?

The Law on PDP provides for a specific list of legal bases for the processing of personal data. Generally, the processing of personal data is carried out on the basis of the data subject's consent. Exceptions to that rule are stipulated by the Law on PDP and other legislative acts. The list of legal bases vary depending on the type of personal data: special (sensitive); or other types.

The laws in the sphere of healthcare also provide for certain deviations for the general requirements in certain aspects. For instance, healthcare regulations establish specific procedure for giving consent to process personal data and information that constitutes medical secrecy in the central informational healthcare system. Moreover, information constituting medical secrecy could be disclosed without the patient's (his/her legal representative's, guardian's, spouse's or close relative's) consent in certain cases as defined in legislation (e.g. upon written request of bodies of criminal prosecution and courts in relation to conducting an investigation or court proceedings).

With regard to clinical trials, participation of patients in clinical trials is voluntary and subject to written, informed consent. The investigator must fully inform a potential patient or their legal representative about all significant aspects of a trial, *inter alia*, providing information about the trial in writing.

Operators should also note other key requirements, such as rules for cross-border transfer, requirements for the contracts with authorised persons (analogue to the processor under the GDPR), respect for the rights of data subjects, developing data processing policies, etc.

4.4 Do the regulations define the scope of data use?

The Law on PDP covers the protection of personal data while processing of such data is accomplished with the use of:

- automated means (tools); or
- non-automated means (tools), if such means (tools) provide the possibility to search for personal data and (or) access personal data with the help of certain criteria (card-indexes, lists, databases, logs, etc.).

Processing means any type of actions taken in relation to personal data, including the collection, systematisation, storage, modification, use, depersonalisation, blocking, distribution, provision and erasure of personal data.

The Law on PDP will not apply to the processing of personal data that is:

- accomplished for personal use, not relating to professional and entrepreneurial activity; or
- related to state secrets.

As for the scope of data use, it may be established either by the operator itself (e.g. describing the purpose and scope of processing in a privacy policy, when the processing performed is based on consent) or established in the legislation (e.g. a particular number of data that should be reflected in the patient file).

4.5 What are the key contractual considerations?

An operator may authorise another person or entity for the processing of personal data based on the agreement. The agreement between the operator and the authorised person shall contain the following provisions:

- a list of actions in regard to personal data that could be performed by the authorised person;
- the purposes of the above actions;
- confidentiality obligations with respect to personal data; and
- measures to ensure the protection of personal data in accordance with the Law on PDP.

Mandatory measures to ensure the protection of personal data are:

- legal measures, such as publication of documents defining the policy of the operator (authorised person) regarding the processing of personal data;
- organisational measures, such as appointment of a structural unit or a person responsible for the control over the processing of personal data (**DPO**); familiarisation of employees and other persons directly engaged in the processing of personal data with the provisions of the legislation on personal data, including the requirements for the personal data documents of the operator (authorised person) as well as training of these employees and other persons; establishing the procedure for accessing personal data; and
- technical measures, such as implementation of technical and cryptographic protection of personal data.

Notwithstanding the terms of the agreement, the operator remains the party responsible for the proper processing of personal data (but not the authorised person).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Generally, operators and their authorised persons are not required to notify the DPA of the processing of personal data. Nevertheless, the DPA is entitled to request and receive any information concerning the operators' and their authorised persons' compliance with data protection rules.

Right to be informed: The operator involved in the processing of personal data shall give clarifications to the data subject regarding their rights related to the processing of their personal data prior to consent collection. Prior to obtaining consent, the operator is obliged to provide the data subject with information concerning the processing of personal data, which includes, *inter alia*:

- the operator's name;
- the purposes of processing;
- a list of personal data;
- the period of consent; and
- a list of actions in regard to personal data.

Furthermore, the operator is obliged to clarify to the data subject, in plain and simple language, his/her rights and the consequences of giving consent or refusing to give it.

Right to access: The operator shall also provide certain information following the data subject's request. Data subjects are entitled to receive information on the processing of their personal data, as well as information on the transfer of the data to third parties, including:

- the name of the operator;
- confirmation of the fact of data processing;
- a description of the personal data and the sources of data;
- legal grounds and the purposes for the data processing;
- the period of the data subject's consent; and
- information on the authorised person.

Information on the transfer of personal data to third parties can be obtained from the operator by the data subject free of charge once a year.

Right to rectification: Under the Law on PDP, an operator involved in the processing of personal data shall fulfil the request of data subjects to amend (update) their personal data, if such data are incomplete, obsolete or inaccurate.

Right to erasure: A data subject has the right to erasure of such data at any time without giving reasons in case of absence of lawful grounds (including the data subject's consent) for the processing of personal data.

Right to object/opt-out: Under the Law on PDP, a data subject may:

- withdraw his/her consent for the processing of personal data; and
- require the termination of the processing of personal data at any time without giving reasons, if there are no legal grounds for the processing.

In that case, the operator is obliged to erase or, if erasure is not possible, to block the personal data as well as to ensure that the data is no longer processed by the authorised person.

Other rights: The Law on PDP provides for the right of the data subject to claim compensation for damage, including moral damage, caused by the violation of his/her rights, stipulated thereby. Compensation for moral damage is not dependent on real damage and losses faced (or not) by the data subject.

The data subject can also appeal against the actions (including omissions) and decisions of the operator or the authorised party to the DPA.

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

The Law on PDP introduces a number of principles, including accuracy of the personal data processed by the operator and, if

necessary, their rectification. Current legislation does not establish the right not to be subject to automated decision-making in terms of personal data processing.

There is no specific regulation of data bias and/or discrimination in the healthcare sphere in Belarus.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

When sharing personal data, one should generally consider (i) the availability of proper legal basis for sharing data, e.g. consent of the data subject, and (ii) whether the sharing party complies with cross-border data transfer requirements (if applicable).

Personal data may also be subject to medical secrecy regime, which triggers protection of the same information as medical secrets. This, among others, affects the scope of the parties who may claim for sharing information that constitutes a patient's medical secrets.

In particular, the patient has the right to decide to whom information about his/her health condition can be disclosed, or to forbid disclosure to certain persons. Medical secrecy concerning a patient who is a minor is provided to the patient's legal representatives: parents; adoptive parents; guardians; custodians; etc. If the patient is not able to make a conscious decision due to health reasons, information constituting medical secrecy may be shared with the patient's spouse or one of their close relatives (parents, adult children, siblings, grandchildren, grandparents). The persons mentioned above have the right to receive extracts from medical documents, medical certificates on the state of health and other documents containing information on the patient's health, in accordance with the procedure established by Belarus legislation. Legislation also stipulates cases in which medical secrecy may be provided to certain public authorities and organisations without the consent of the patient or persons mentioned above.

5.2 How do such considerations change depending on the nature of the entities involved?

Regarding the personal data requirements, please see the answer to question 4.2.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please see the answers to questions 4.3 and 4.5 regarding (i) proper legal basis, and (ii) necessary contractual arrangements between an operator and an authorised party.

According to the general rule provided by the Law on PDP, the cross-border transfer of personal data to countries not ensuring sufficient measures of personal data protection is prohibited. The list of "adequate" jurisdictions refers to states that are (i) parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981, or (ii) members of the Eurasian Economic Union.

The PDP Law provides for the exceptions where transfers are allowed to the jurisdictions that are not in the list defined by the DPA. For example, such cases include the consent of the data subject with due notification on the relevant risks or a permit for cross-border transfer issued by the DPA.

6 Intellectual Property

6.1 What is the scope of patent protection?

The main Belarus legal act describing patent protection is the Law of the Republic of Belarus "On Patents for Inventions, Utility Models, Industrial Designs".

The exclusive right to an invention is protected and is certified by a patent which is issued upon application. The scope of patent protection related to an invention is determined by the invention claims.

Legal protection is granted to an invention in any field of technology (e.g. medical devices and equipment), if it relates to a product or a method, appears as novel, involves an inventive step and is industrially applicable. Product implies an object of human labour. Method denotes a process, technique or method of performing interrelated actions on a material object with the help of material means.

Computer programs and mathematical methods are not patentable *per se*. However, if the invention (1) meets the above criteria, and (2) is created with the help of computer programs or artificial intelligence, it may be patentable.

According to Belarus law, only an individual can be the invention creator; the status of artificial intelligence activities is debatable.

The exclusive right to use an invention includes the right to use the invention at one's own discretion, assuming this does not violate the rights of others, and the right to prohibit others from using the invention.

The patent term related to an invention is 20 years from the application filing date (in some cases this term may be extended, but by no more than five years).

6.2 What is the scope of copyright protection?

The main Belarus legal act describing copyright protection is the Law of the Republic of Belarus "On Copyright and Related Rights".

Copyright protection arises by virtue of the fact of its creation. Acquisition and exercise of copyright do not require any formalities (e.g. receiving protection documents).

Copyright protection extends to works of science, literature and art that are the result of creative activity, regardless of the purpose and dignity of the works, as well as the way they are expressed.

Copyright is protected with regard to both published and unpublished works which exist in some objective form, for example: in sound or video recordings (mechanical, magnetic, digital, optical, etc.); or in electronic form, including in digital form.

Computer programs (including software, source code, designs) are eligible for copyright protection.

Copyright does not extend to ideas, methods, processes, systems, concepts, principles, discoveries or facts, even if they are expressed, displayed, explained or embodied in a work.

As mentioned in question 6.1 above, according to Belarus law, only an individual can be the author of a particular work and the status of artificial intelligence activities is debatable.

There are two types of rights under copyright: economic rights, which allow the owner of the rights to derive financial reward from the use of the works by others; and moral rights, which allow the author to take certain actions to preserve the personal link between himself/herself and the work. Economic rights are valid, as a general rule, during the life of the author and 50 years after his/her death. Moral rights are protected indefinitely.

6.3 What is the scope of trade secret protection?

The main Belarus legal acts describing trade secret protection are the Civil Code of the Republic of Belarus and the Law of the Republic of Belarus "On Commercial Secrecy".

Information constituting a trade secret is protected under the regime of commercial secrecy, if all of the following criteria are met:

- it is not generally known or available to third parties that usually deal with this kind of information;
- it has commercial value for its owner due to being unknown to third parties;
- it is not an object of exclusive rights to the results of intellectual activity; and
- it is not a state secret.

The commercial secrecy regime is considered to be established after (1) determining the list of information subject to protection, and (2) taking a set of measures necessary to ensure confidentiality by the information owner.

The legislation also defines the list of information which cannot fall under the commercial secrecy regime, for example: medical; attorney; banking; tax; or other secrets protected by law or information about the state of the environment.

The trade secret owner has the right to protect the trade secret from being used by others without permission. Trade secrets are protected without any procedural formalities (registration, acquisition of a certificate, etc.). They are not formally limited by any term and are valid while the above-mentioned criteria are met.

Unpatented digital technologies or medical devices, etc. can be protected as a trade secret, i.e.:

- trade secret protection can appear as an alternative to patenting; and
- if the rightsholder can obtain patent protection with regard to a significant solution; the information needed for its realisation may be protected as a trade secret.

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

Academic technology transfers are not regulated in detail in Belarus. Overall, in such cases general rules related to works and inventions for hire should apply.

A work for hire is a work created in the course of performing an official assignment or official duties by an employee. The moral rights belong to its author; the economic rights belong to the author's employer.

An invention for hire is the invention which relates to the field of the employer's activity, and the activity which led to its creation relates to the official duties of the employee. Alternatively, the invention for hire may be created in the course of completing a specific task received from the employer, or the employee used the employer's experience or funds. The moral rights belong to the creator of the invention for hire; the right to obtain a patent and the economic rights belong to the creator's employer, unless otherwise provided by the agreement between them. By acquiring the economic rights, the employer also acquires the obligation to pay appropriate remuneration to the employee, of which the minimum amount is established by law.

Furthermore, Belarus law establishes obligatory commercialisation of the results of scientific activities at the expense of public funds. Intellectual property and documented scientific and technical information created in the course of scientific activity at the expense of public funds, in accordance with agreements for performing research, development and technological work, are considered as the results of scientific activity. Please see question 6.7 for more details.

6.5 What is the scope of intellectual property protection for software as a medical device?

Belarus law does not specifically describe protection for software as a medical device.

Software being interpreted as a computer program is not patentable in Belarus. As mentioned in question 6.2, software is eligible for copyright protection.

If software is a component of a medical device consisting of some other components (e.g. hardware), such medical device may still be patentable.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

No, an artificial intelligence device cannot be named as an inventor of a patent in Belarus. According to Belarus law, only an individual can be the invention creator. Therefore, we believe that the results of artificial intelligence activities (e.g. devices) cannot be granted legal protection as inventions.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The main Belarus legal act describing the rules applicable to government-funded inventions is the Edict of the President of the Republic of Belarus "On Commercialisation of the Results of Scientific and Scientific-Technical Activities Created at the Expense of Public Funds".

According to this Edict, Belarus law establishes obligatory commercialisation of the results of scientific activities at the expense of public funds. Intellectual property and documented scientific and technical information created in the course of scientific activity at the expense of public funds, in accordance with agreements for performing research, development and technological work, are considered as the results of scientific activity. Commercialisation implies the following options (the list is not exhaustive):

- sale of goods created with the use of the results of scientific activity, or use of these results for other needs;
- fee-based or gratuitous license of the right to use the results of scientific activity;
- fee-based or gratuitous assignment of property rights to the results of scientific activity;
- fee-based or gratuitous transfer of information constituting trade secrets; and
- fee-based or gratuitous transfer of documented scientific and technical information.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

In addition to determining: collaboration purposes; participants' rights and obligations; applicable regulations and liability allocation; and collaboration termination, it is also important to determine a specific intellectual property regime which should be applicable to the specific collaboration improvements.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

Firstly, such agreements must comply with the general principles and rules of Belarus civil law on agreements, as well as competition legislation. In addition, prices and tariffs in the healthcare sector are regulated by the state, therefore pricing requirements must also be complied with. Finally, with regard to agreements between Belarus residents and non-residents, it is important to comply with local foreign trade rules.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning in digital health and, overall, in healthcare is not regulated in Belarus. Implementing machine learning in digital health will contribute to improving the quality of medical care and active early detection of diseases in the human body. Machine learning possibilities may also be effective in the development of pharmaceuticals, storage of medical records and other methods of assistance to healthcare professionals with research and practice.

8.2 How is training data licensed?

There are no regulations covering training data licences in Belarus. Instead, general regulations should apply: (1) if training data relates to using personal data and information constituting medical secrecy, rules of sharing such data should apply – please see question 5.3; and (2) if training data relates to using intellectual property, rules of copyright licensing should apply.

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

This matter is not regulated in Belarus.

According to Belarus law, only an individual can be the author of a particular work (e.g. a computer program) – please see question 6.2. Moreover, algorithms should not be protected as copyright because copyright does not extend to methods, processes or systems, even if they are expressed, displayed, explained or embodied in a work (e.g. a computer program).

8.4 What commercial considerations apply to licensing data for use in machine learning?

Confidentiality of personal data, permissions to use relevant data, the scope of rights to be licensed and regulatory restrictions may be key commercial considerations that apply to licensing data for use in machine learning.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Belarus legislation does not contain specific rules and theories on liability for violations in the field of digital health; therefore, general principles on civil, administrative and criminal liability apply.

In particular, liability for breach of medical secrecy may include:

- disciplinary liability (reprimand, admonition, dismissal, in accordance with labour legislation);
- administrative fine, if disclosure does not contain elements of crime;
- civil liability (e.g. compensation of damages and (or) moral harm); or
- criminal liability.

In relation to the illegal processing of personal data, non-compliance with requirements on data protection measures may lead to administrative fines. Some violations in the sphere of the protection of personal data may cause criminal liability; in particular:

- the unlawful collection or distribution of information relating to the private life, personal or family secrecy of another person without his/her consent; or
- the failure to comply with measures to ensure the protection of personal data by a person who processes personal data, which has inadvertently resulted in their dissemination and caused serious consequences.

9.2 What cross-border considerations are there?

There are some legal provisions that are subject to extraterritoriality in certain cases (e.g. personal data or antitrust regulation). In practice, however, the question of enforcement in such cases is open.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Information security and data protection are the key issues in Cloud-based services for digital health. Please see our responses to sections 4 and 5.

Distrust of service providers and the lack of standards that regulate this area are also worthy of mention. In particular, the lack of unified industry standards that require international standards HL7 FH1R, CDA, IHE, STB ISO/IEC 27001-2011 and reference books LOINC, SNOMED ST, which define the requirements for organising the storage, processing and transmission of information, ensuring the protection of personal data, identification of the system participants' healthcare and information interaction between the participants of a single medical information space.

Local parties involved in data processing may be affected by certain localisation requirements. According to the Presidential Edict No. 60 dated 1 February 2010, an activity involving selling goods, performing works or rendering services in the territory of Belarus through information networks, systems and resources, having connection to the Internet, is carried out by legal entities, their branches and representative offices, incorporated under the Belarus law with the seat in Belarus, as well as individual entrepreneurs, registered in Belarus, by using information networks, systems and resources located in Belarus and duly registered. In our opinion, this provision should be interpreted narrowly, and consequently applies only to Belarusian residents (e.g. when using Cloud-based solutions, located outside Belarus, to render services in Belarus) and shall not affect foreign Cloud-based providers directly.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Comprehensive regulatory due diligence, including data protection and investment issues, should be considered. Moreover, due to significant state-involvement in healthcare, it is important to consider local licensing and regulatory peculiarities. For example, clinical trials are conducted in state healthcare organisations defined and authorised by the Ministry of Healthcare. An agreement on conducting clinical trials is concluded between the sponsor and healthcare organisation; direct agreement with the investigator is not allowed.

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, regulatory due diligence is recommended. As well as analysing the state of the field of venture capital and (or) direct financing, investors should identify negative trends on the Belarus market that affect its development.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Based on the Concept, one of the main problems is the lack of necessary standards for the exchange of medical information in the healthcare system in accordance with the requirements of the legislation. Additionally, there is a lack of formed databases and data banks, as well as a lack of technical equipment.

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 clinician certification bodies in Belarus; and we are not aware of any other bodies that have a power to influence the clinical adoption of digital health solutions. The relevant decisions are made in cooperation, mainly, between the Belarus government and the Ministry of Healthcare.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

There are no special regulations related to utilising digital health solutions and corresponding reimbursement. Instead, general reimbursement principles related to causing harm to patients' health should apply.

10.7 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.

Currently, Belarus is testing the central software platform of the CHIS. In case of successful completion of the tests, the intent is to introduce the platform. Preparations are also underway to switch to the new International Statistical Classification of Diseases and Related Health Problems, Revision 11 (ICD-11).

The plan for this platform is to provide access for each patient to their personal account and access to their medical data. The patient will be able to make an appointment through a personal account, receive test results and conclusions issued after consultations by specialists.

Kirill Laptev is a partner with Sorainen Law Firm in Belarus. He heads the TMT Sector Group and leads the Data Protection practice at Sorainen Belarus. Kirill is one of the shortlisted specialists for data protection and privacy matters, both on a national level and from an EU perspective, with a deep understanding of GDPR specifics. His key areas of expertise also include commercial contracts and regulatory matters. Kirill has broad experience in high-profile international commercial and investment arbitration, including in the sphere of IT/IP uniquely for the local market.

Sorainen
ul Internatsionalnaya 36-1
220030 Minsk
Belarus

Tel: +375 29 339 4590
Email: kirill.laptev@sorainen.com
URL: www.sorainen.com

Marina Golovnitskaya is a counsel with Sorainen Law Firm in Belarus and an international head of the Sorainen Life Sciences and Healthcare Sector Group. She manages Sorainen's regional team and leads the life sciences-related projects in Belarus. For years, she has worked with companies in the pharmaceuticals sector, learning the industry from within. Marina serves as a day-to-day advisor for both Big Pharma and boutique healthcare companies in a range of matters; for example: clinical trials; marketing of pharmaceuticals; patients' data protection; regulatory issues; compliance; anti-corruption and antibribery regulations; and white-collar crimes. Marina is also a Co-head of the Intellectual Property Practice Group and is recommended by *The Legal 500* for Intellectual Property.

Sorainen
ul Internatsionalnaya 36-1
220030 Minsk
Belarus

Tel: +375 29 188 4328
Email: marina.golovnitskaya@sorainen.com
URL: www.sorainen.com

Sorainen is a fully integrated international business law firm, advising organisations on all business law and tax issues involving the Baltic States and Belarus.

With uniquely integrated offices in Estonia, Latvia, Lithuania and Belarus, we operate as a single connected legal ecosystem. Our regional teams combine their legal expertise to cover all sectors and practice areas, our offices share a unified practice and quality management system, while our know-how is exchanged amongst our team of more than 250 lawyers and tax specialists.

We have closely partnered with businesses – local, regional and international – to increase prosperity in the Baltic States and Belarus by helping our clients succeed in business. Our approach, regardless of a client's size and scope, is to help a business succeed by providing exact solutions to carefully evaluated legal issues.

www.sorainen.com

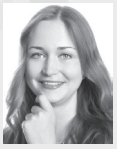
SORAINEN

Belgium


Olivier Van Obberghen


Pieter Wyckmans


Amber Cockx


Hannah Carlota Osaer

Quinz

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 technologies in your jurisdiction?

In recent years, Belgium has seen a rise in the development and implementation of a number of health technologies such as apps, wearables, platform technology and AI-based software across the life sciences value chain and into the patient journey with a focus on remote, personalised, precision and preventative care.

1.3 What are the core legal issues in digital health for your jurisdiction?

The emergence of new health technologies results in changing roles for healthcare actors and challenges the boundaries of the current legal framework. With an increasingly consumer-centric approach to healthcare, patients are empowered to take an active role in the co-maintenance of their own health. In response, the role of the hospital is gradually shifting from a focus on inpatient to outpatient treatment, while the medical (tech) industry more often comes into direct contact with patients, leading to data protection and compliance concerns. The reality of an ever-increasing digitalisation of healthcare is often at odds with existing laws and regulations (concerning, for example, intellectual property protection, data protection, liability, and compliance) and will continue to require swift and agile action by the legislator.

1.4 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. Some unofficial estimations project that the digital health market in Belgium could reach up to 650 million euros in 2023.

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

In line with question 1.4, 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.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

- 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; *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; and
- A number of legislative initiatives and already adopted instruments in light of the EU's digital strategy, such as the Digital Services Act (EU Regulation 2022/2065) and the EU proposal for an artificial intelligence (AI) act.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The legislation on product safety, personal data protection and e-commerce apply to digital health and healthcare IT. In addition, general regulations on competition, consumer law and unfair commercial practices must be kept in mind. Certain specific rules might also be relevant (e.g. the Act of 21 August 2008 establishing and organising the eHealth platform or the EU framework on cross-border healthcare). Lastly, a number of substantial legislative proposals in light of the EU's digital

strategy (i.e. regarding digital services, markets, content, AI, cybersecurity, etc.) will significantly impact the offering of digital health goods and services in the future.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The legislation on medical devices (see question 2.6), product liability (see question 9.1), e-commerce and the consumer protections set forth in the Code of Economic Law (CEL), Book VI (as recently amended) are relevant to consumer healthcare devices. Intellectual property rights of software are protected by Book XI, Title 6 of the CEL.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

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) supervises the quality, safety and efficacy of medicines and health products. 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. Lastly, the Belgian Data Protection Authority (DPA) enforces compliance with data protection and a Health Data Protection Authority (yet to be established) should oversee the sharing and use of healthcare data.

2.5 What are the key areas of enforcement when it comes to digital health?

The DPA and the Market Court in Brussels ensure enforcement of 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 offenses that are criminally curbed.

2.6 What regulations 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 (note that, recently, the Belgian national regulatory framework was brought in line with the IVDMDR by 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. In addition, medical devices need to be traceable throughout the supply chain up until the end user. Finally, the FAHMP is responsible for post-market surveillance of (software as a) medical device.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Software that is powered by AI/Machine Learning (ML) is currently governed by the same regime as other software (see questions 2.3 and 2.6). 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. It can, however, be expected that AI/ML powered devices or software will in the future be regulated by specific instruments. In this regard, the European Commission has proposed a new draft regulation on AI (the AIA). The AIA recognises that, if AI/ML powered digital health devices or software solutions constitute medical devices, they may be identified as high-risk, and both the requirements of the MDR/IVMDR and the AIA will have to be complied with.

3 Digital Health Technologies

3.1 What are the core 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). 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. In addition to that, certain remote consultations by doctors are being reimbursed by the NIHDI.
- **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 aging 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 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 General Data Protection Regulation (GDPR) and the requirements of art. 5(3) of the Directive 2002/58/EC on privacy and electronic communications (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 recent introduction of the Digital Services Package by the European Commission might also have a significant impact on the marketing and use of VVAs as companies offering core platform services, which includes, amongst others, virtual assistant services, could be considered a 'gatekeeper' if they meet other requirements indicating that such companies have a position of power in the market.
- **Mobile Apps**
  Since January 2021, mobile apps can be reimbursed if they fulfil all criteria of the mHealth Belgium validation pyramid. 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, only one mobile app has received a temporary reimbursement decision (however, 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. Again, 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 medical devices' framework, while other apps may be considered a wellness or lifestyle device.
- **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. 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. According to art. 22 of the GDPR, a data subject is entitled not to be subject to a decision based solely on automatic means that significantly affects them. While there are exceptions to this principle (e.g. explicit consent and suitable safeguards), a data subject has the right to receive meaningful information about the logic involved in the automatic decision-making and to obtain human intervention and contest a decision made by automated means. This is particularly difficult when the processing has been done by artificial neural networks, as it may be impossible to determine how the AI decided on a particular outcome. Exercising other rights, such as the right to access and erase personal data might (technically) also be notably difficult. Besides data protection, the interplay of the proposed AIA and the MDR suggests that AI-powered medical devices will in the future be regulated by stringent requirements in both instruments. 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 II 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**
  Again, while IoT and connected devices offer great advantages for patients (e.g. assisted living), for physicians (e.g. telemonitoring) and for hospitals (e.g. stock management and patient identification), privacy, data protection and security issues have been raised.

- **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**
  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.
- **Natural Language Processing**
  This technology is similarly impacted by data protection concerns as virtual assistants are (see above). Healthcare professionals wishing to use this technology in the management of electronic health records may also encounter interoperability issues. Additionally, natural language processing technology raises issues concerning discrimination on language grounds and a range of other ethical and legal issues such as transparency, fairness, accountability, etc. As natural language processing technology is AI driven, the expected rules on AI will also need to be considered.

3.2 What are the key issues for digital platform providers?

Under the current regime, liability of digital platform providers for copyright breaches and other infringements has been limited (Book XII of the Code of Economic Law). Hosting providers cannot be held liable for infringements committed through their services insofar as the service provided merely consists of the storage of information provided by a recipient of the service. In addition, the platform provider may not have (had) knowledge of the illegal activity or information. Once the provider has actual knowledge of the infringement, it needs to act expeditiously to remove or to disable access to the information concerned and it needs to inform the public prosecutor of such infringement. While the 'notice and take down'-principle is upheld under the new EU Digital Services Act, more stringent obligations are imposed on intermediary service providers, including extensive transparency obligations. 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).

4 Data Use

4.1 What are the key issues to consider for use of personal data?

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 healthcare providers. 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.

4.2 How do such considerations change depending on the nature of the entities involved?

As a consequence of the introduction of e-health, the personal data of patients are no longer solely processed by physicians and other healthcare providers, 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)).

4.3 Which key regulatory requirements apply?

In the physician–patient relationship, patients have the right to consult their medical record, which should be updated and stored carefully (art. 10 of the Act on Patients' Rights, arts 22–24 of the Code of Medical Ethics of the NCOP, arts 33–40 of the Health Care Quality of Practice Act of 22 April 2019). Since 2008, a national e-Health platform has been established, where healthcare providers upload electronic health records of a patient after having obtained the patient's consent (art. 5.4(b) of the Law Establishing and Organising the eHealth Platform). Only healthcare providers having a therapeutic relation with

the patient may access the electronic health records of a patient, excluding, for example, medical advisors from insurance companies. In the broader context of (e-)health services, one must take account of the GDPR and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data.

4.4 Do the regulations define the scope of 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.)

4.5 What are the key contractual considerations?

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).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The GDPR maintains 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.

4.7 How are issues with 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. As discussed under question 2.1, 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.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 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 in the European Commission's proposal of a European Health Data Space, intended to facilitate the use and sharing of European health records both for the purpose of providing healthcare services and for 'secondary purposes' such as research.

5.2 How do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The sharing of data is considered to be another aspect of the processing of data under Belgian law. Correspondingly, the same regulatory requirements apply (see question 4.3). Notably, a data subject must be informed about the third parties with whom its personal data will be shared. Further, if the third party is situated outside the scope of the GDPR, adequate safeguards must be taken to protect the personal data when transferred.

6 Intellectual Property

6.1 What is the scope of patent protection?

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 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 methods as such. One can apply for patent protection for "mixed inventions", for instance for a new product of a technical nature which incorporates a software program. The European Patent Office (EPO) classifies AI- and ML-related applications as mathematical methods in its guidance. Patents are valid for 20 years.

6.2 What is the scope of copyright protection?

Copyright protects literary or artistic works in a broad sense (Title 5 of Book XI of the Code of Economic Law). A work is eligible for copyright protection provided that it represents the author's own intellectual creation. 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. The expression of software is also protected by copyright, as well as databases which meet the requirement of originality.

6.3 What is the scope of trade secret protection?

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 Code of Economic Law). Trade secrets are not protected by an intellectual property 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. In addition, the malicious or deceptive disclosure of secrets of the factory in which someone has worked is criminally sanctionable (art. 309 of the Code of Criminal Law). Employees are also obliged to safeguard the trade secrets of their employers and any act of unfair competition is sanctionable (art. 17 of the Law concerning Employment Contracts of 3 July 1978 and art. VI.104 of the Code of Economic Law).

6.4 What are the rules or laws that apply to 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 license or other types of collaboration agreements or participation in spin offs.

6.5 What is 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 Code of Economic Law).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

The EPO has confirmed on multiple occasions that AI (devices) cannot be named as inventors on patent applications.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The core rules and laws applicable to government-funded inventions in Belgium are noted down in the Belgian Code of Economic Law, Book XI, Title 1, Chapter 2. Irrespective of any governmental funding, the inventor is considered the person who developed the invention.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The allocation of intellectual property 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 considerations apply in 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.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

ML is valuable for a broad array of applications in digital health which can lead to more holistic care strategies that could improve patient outcomes. In this context, ML can help healthcare organisations meet growing medical demands, improve operations and lower costs, which is especially valuable for a sector characterised by limited resources. Besides, ML can help practitioners detect and treat diseases efficiently, with more precision and personalised care.

8.2 How is training data licensed?

The Database Directive laid some of the groundwork in facilitating the license of vast amounts of data. Databases may be protected either through copyright protection, if the structure of the database is sufficiently original, or through the *Sui Generis* Database Right (SGDR) for the substantial investment in obtaining, verifying or presenting the content of the database (or through both) (Title 7 of Book XI of the Code of Economic Law). Under the SGDR, the extraction and reuse of substantial parts of a database can be commercialised for a period of 15 years from the creation date of the database or from the moment the database first became publicly available. The right of a producer of a database can either be transferred or licensed (exclusive or not).

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 ML, cannot be protected by copyright if it is created without creative human involvement and does not meet the requirement of originality. As with regard to patents, according to the EPO and Article XIV §1, 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 considerations apply to licensing data for use in machine learning?

The quality of the data used in ML is essential for the quality of the results it presents. Therefore, companies developing AI technology will become increasingly interested in (exclusive) licences on quality datasets with the least restrictions possible. On the other hand, Belgian data protection regulation principally prohibits the processing of health-related data, unless an exception, such as consent of the data subject, applies. Moreover, the principle of data minimisation and the restrictions on data processing for a purpose other than for which it was initially collected, may directly clash with the commercial interests of tech companies.

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 proposals for an updated product liability directive and an AI liability directive, for example, with the aim of more equally sharing the burden of proof for complex digital solutions between the claimant and manufacturer.

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. 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.

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, 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 recently adopted Directive (EU) 2022/2555 (NIS 2 Directive), which aims to ensure a high level of security for essential service providers, requires implementation in Belgian law. 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?

To assess the growth potential and the relative strength of a digital healthcare venture amongst its competitors, one needs to take account of certain elements. 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 not currently reimbursed.

10.7 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 economic turbulence, inflation and supply chain disruptions 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. Lastly, shortages in, for example, the chip industry have important consequences for the costs and availability of medical devices.

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
1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: olivier.vanobberghen@quinz.be
URL: www.quinz.be

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
1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: pieter.wyckmans@quinz.be
URL: www.quinz.be

Amber Cockx is a Life Sciences lawyer with a main focus on 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, marketing authorisations, advertising and promotion, pricing and reimbursement, and interactions with healthcare professionals and healthcare organisations.

Quinz
Medialaan 28B
1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: amber.cockx@quinz.be
URL: www.quinz.be

Hannah Carlota Osaer is a corporate lawyer with a main focus on the Life Sciences industry, including digital health. She has a background in international commercial arbitration and data protection law. Hannah Carlota provides transactional and regulatory support to clients active in the pharmaceutical sector. Her main areas of expertise comprise of negotiating and drafting contracts, transactional and regulatory assistance throughout the entire product life cycle, clinical trials, distribution, advertising and promotion, as well as all aspects of data protection and privacy laws.

Quinz
Medialaan 28B
1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: hannahcarlota.osaer@quinz.be
URL: www.quinz.be

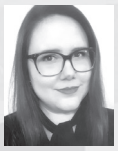
Quinz is a Brussels-based law firm with a strong focus on Life Sciences. Quinz assists the global, regional (EMEA, LATAM, APAC) and local (Belgium, Luxembourg and the Netherlands) legal departments of pharmaceutical companies on a broad array of (strategic, operational, licensing and M&A) transactions 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

Brazil


Ricardo Barretto Ferreira da Silva


Juliana Gebara Sene Santos Ikeda


Lorena Pretti Serraglio

Azevedo Sette Advogados

1 Digital Health

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

The Brazilian Ministry of Health defines "digital health" as the use of Information and Communication Technology (ICT) resources in healthcare, producing and delivering reliable health status information to citizens, health professionals and public managers, in order to solve issues in the public and private healthcare systems. It also includes innovative ICT resources in healthcare, e.g., social networking applications, Internet of Things (IoT), Artificial Intelligence (AI), use of personal devices and emerging technologies.

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

The key emerging technologies implemented by the Brazilian National Digital Health Strategy 2020–2028 (BNDHS 2020–2028) include: telemedicine and telehealth; AI/IoT; wearables and automation; big data; and mobile health applications.

Telemedicine and telehealth intend to provide safe integrated care and monitoring for patients in a remote manner, through the use of ICT resources. Artificial Intelligence of Things (AIoT) includes the use of AI algorithms to manage the operation of machines by integrating the systems to the internet. Wearables and mobile health applications are used to record, analyse, regulate, and even treat diseases to maintain the health of the user, by monitoring their clinical information through electronic mobile devices.

1.3 What are the core legal issues in digital health for your jurisdiction?

The main legal issues faced by digital health in Brazil include: (i) the lack of specific and unified regulation that ensures the safety and transparency in the collaboration of stakeholders, in addition to the legal uncertainty regarding essential rights and the different authorities that rule these matters; (ii) the risks involving data protection and security of sensitive data; and (iii) the lack of computer integration of the Brazilian public health system in different jurisdictions and private and public sectors.

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

According to the study published by PwC Brasil (https://www.pwc.com.br/pt/sala-de-imprensa/release/Estudo-da-liga-ventures-e-pwc-brasil-aponta-aumento-no-numero-de-healthtechs-entre-2019-e-2022.html), the number of healthtechs in Brazil has increased by more than 16% between 2019–2022. Such growth is directly associated with the COVID-19 pandemic, and the implementation of governmental programs in the Brazilian Unified Health System (SUS), especially the program ConecteSUS. According to the same research, Mergers & Acquisitions (M&A) transactions and investments in the Brazilian digital healthcare market actually involved BRL 1.79 billion in such period (2019–2022).

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

The five largest digital health service companies in Brazil, based on the values of rounds collected by healthtechs in 2022, are Alice, Bionexo, Memed, Conexa Saúde and 3778 based on the recent Healthtech Report 2022 (https://7735036.fs1.hubspotusercontent-na1.net/hubfs/7735036/MINING-HEALTHTECH-2022-20220909-3.pdf?utm_campaign=techtrends_healthtech&utm_medium=email&_hsmi=224604938&_hsenc=p2ANqtz-8kzlwp8j5PQIN5YEHFA-eigzcO_pCx4jyxk0bW7i9B164WJBCa0T20thiATJ45lJB8giDKAkkqo4Nf2lW8-LXmVNw2YSDK-RC-NVWSFT-tm_sLGVRo&utm_content=224604938&utm_source=hs_automation).

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Currently, there is no legal framework for digital health in Brazil that compilates all regulatory rules regarding this matter. The

Ministry of Health and other local agencies (such as the National Health Surveillance Agency (ANVISA) and the National Supplementary Health Agency (ANS)), have issued different norms regarding digital health.

Following the global strategy on digital health (created in 2019 by the World Health Organization), the Ministry of Health delivered the National Digital Health Strategy (ESD28), which includes the Digital Health Action Plan 2020–2028 and a Monitoring and Evaluation (M&E) Plan.

The Action Plan describes the necessary resources and activities for the implementation of the Strategic Digital Health. The M&E Plan defines the organisation and governance of the M&E actions, as well as the activities to be performed and the respective responsible stakeholders.

Later, the Ministry of Health implemented the ConecteSUS and established the National Healthcare Data Network, providing health interoperability standards.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Data privacy is regulated by the Brazilian General Data Protection Act (Law No. 13,709/2018 (LGPD) (https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/)), which provides for the processing of personal data, including in digital media. The Internet Act (Law No. 12,965/2014 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)), regulated by Decree No. 8,771/2016 (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm) also applies to digital health since it sets important guidelines for the use of the internet applications in Brazil. The CIT Resolution No. 19 of June 22, 2017 (http://wwa.tjto.jus.br/elegis/Home/Imprimir/1201#:~:text=RESOLU%C3%87%C3%83O%0D%20N%C2%BA%2019%2C%20de%2022%20de%20junho%20de,do%20Estado%20do%20Tocantins%2C%20e%20adota%20outras%20provid%C3%AAncias.) of the Ministry of Health, launched the digital health strategy in Brazil (digiSUS) (https://digisus.saude.gov.br/gestor/#/). The digiSUS managing platform aims to provide municipal, state and federal health managers with tools to assist in the planning and management of SUS. Other Resolutions of the Ministry of Health, such as CIT Resolution No. 6/13 (https://bvsms.saude.gov.br/bvs/saudelegis/cit/2013/res0006_06_11_2013.html) and CIT Resolution No. 7/16 (https://bvsms.saude.gov.br/bvs/saudelegis/cit/2016/res0007_24_11_2016.html) also set important rules for implementation of new applications, health information systems or new versions of systems involving SUS.

Telemedicine services in Brazil are currently allowed, but in a limited and regulated manner. In 2022, the Federal Council of Medicine (CFM) also issued CFM Resolution No. 2.314/2022 (https://www.in.gov.br/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852#:~:text=RESOLU%C3%87%C3%83O%20CFM%20N%C2%BA%202.314%2C%20de%2020%20de%20abril,de%20servi%C3%A7os%20m%C3%A9dicos%20mediados%20por%20tecnologias%20de%20comunica%C3%A7%C3%A3o.) in this regard. Bill No. 1,998/2020 also regulates this matter and it should be analysed by the Brazilian Senate. CFM also issued other Resolutions regulating digital prescriptions and teleradiology, for example, and Law No. 13,787/2018 (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm) implements the digitalisation and computerisation of the healthcare system.

In this regard, ANVISA is also giving special attention to medical devices used in the digital health market, so it issued RDC No. 657/2022 (http://antigo.anvisa.gov.br/documents/10181/5141677/RDC_657_2022_.pdf/f1c32f0e-21c7-415b-8b5d-06f4c539bbc3), regulating software as medical devices.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

ANVISA's RDC No. 657/2022 (http://antigo.anvisa.gov.br/documents/10181/5141677/RDC_657_2022_.pdf/f1c32f0e-21c7-415b-8b5d-06f4c539bbc3) provides for the regularisation of software as a medical device (SaMD). In 2022, ANVISA also approved the proposal to update the text of the RDC Resolution No. 185/2001 (https://www.emergogroup.com/sites/default/files/file/rdc_185_2001_classification_and_registration_requirements_of_medical_products_0.pdf) to include regulation on new technologies, including medical devices in Brazil.

CIT Resolution No. 6/13 (https://bvsms.saude.gov.br/bvs/saudelegis/cit/2013/res0006_06_11_2013.html) also applies to healthcare devices and software within SUS.

In any case, the Brazilian Consumer Protection Code (Law No. 8,078/1990 (CDC)) applies to any consumer relationship, including the ones related to healthcare devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The main regulatory authorities in healthcare in Brazil are: (i) ANVISA; (ii) the Ministry of Health; (iii) ANS; and (iv) CFM.

2.5 What are the key areas of enforcement when it comes to digital health?

The key areas of enforcement regarding digital health include digital laws, data protection laws, consumer laws and the rules issued by local authorities.

Nonetheless, AI and other technologies are subject to specific laws and regulation (e.g., intellectual property rights and rules issued by the Brazilian Ministry of Sciences, Technology and Innovation).

2.6 What regulations apply to software as a medical device and its approval for clinical use?

ANVISA's RDC No. 657/2022 (http://antigo.anvisa.gov.br/documents/10181/5141677/RDC_657_2022_.pdf/f1c32f0e-21c7-415b-8b5d-06f4c539bbc3) regulates the use of SaMD in the healthcare system. Other rules related to the registration/approval of medical devices are provided for by ANVISA's RDC No. 185/2001 (https://www.emergogroup.com/sites/default/files/file/rdc_185_2001_classification_and_registration_requirements_of_medical_products_0.pdf).

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

There is no legal framework specifically regulating the use of AI or other IoT devices and their approval for clinical use.

However, Bill No. 21/2020 (https://www25.senado.leg.br/web/atividade/materias/-/materia/151547), which is under discussion in the Senate, sets forth principles and guidelines for the development and application of AI in Brazil.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Data protection and medical confidentiality.
- **Robotics**
  There are heated debates about liability in the event of a machine's malfunction that can cause potential damage to a patient's health, especially if supervised by medical professionals.
- **Wearables**
  Most wearable devices are not considered medical devices under ANVISA's regulation, so there is a lack regulation regarding them.
- **Virtual Assistants (e.g. Alexa)**
  Data privacy matters in connection with the use of such Virtual Assistants raises further discussions about the liability of their manufacturers and distributors.
- **Mobile Apps**
  Most mobile apps are not regulated by ANVISA, which results in the lack of rules regarding the safety and accuracy of their use by patients.
- **Software as a Medical Device**
  According to ANVISA's Regulatory Impact Analysis Report on SaMD (https://www.gov.br/anvisa/pt-br/assuntos/regulamentacao/participacao-social/dialogos-setoriais/arquivos/dialogo-setorial-sobre-o-relatorio-preliminar-de-air-de-software-medico/relatorio-de-definicao-e-analise-do-problema-regulatorio-v-0-4-pos-rev-ggreg.pdf#:~:text=Os%20softwares%20como%20dispositivos%20m%C3%A9dicos%20e%20v%C3%A1rios%20equipamentos,ou%20ISO%20que%20possibilite%20a%20certifica%C3%A7%C3%A3o%20do%20mesmo.), the main issues are: (i) lack of guidance to health professionals and the population about the risks in their use; (ii) difficulty in inspection, monitoring and sanitary control; (iii) lack of updated regulatory requirements due to their fast and disruptive pace of innovation; and (iv) omission of potential risks already identified by their manufacturer.
- **Clinical Decision Support Software**
  Clinical decision support software is also subject RDC No. 657/2022. The topic is still quite recent and encounters the same challenges faced by SaMD.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  The CDC holds all the chain of supply liable for any product purchased by consumers. This means that the manufacturer of a machine that uses AI and the hospital that uses such machine are equally liable before patients. Medical professionals, however, that may rely on such technologies, are not consumers and, thus, liability is highly debatable.
- **IoT (Internet of Things) and Connected Devices**
  The use of such technology in healthcare relies specifically on the absence of knowledge by medical professionals and other agents that have little to no experience in the use of these devices. These devices also face the lack of specific rules related to civil liability of the service or product provider.
- **3D Printing/Bioprinting**
  The high cost and the lack of scientific resources and knowledge about its various functionalities and efficiency.
- **Digital Therapeutics**
  Risks arising from the violation of data privacy.
- **Natural Language Processing**
  Since natural language processing concerns AI technology, it faces the same issues applied to AI.

3.2 What are the key issues for digital platform providers?

Digital platform providers are deemed application providers under the Internet Act. Their main concerns involve: (i) civil liability in relation to users; (ii) lack of specific regulation regarding emerging technologies (e.g., AI, IoT); (iii) civil liability regarding a service/product offered by the digital platform; and (iv) cybersecurity, due to the sensitivity of the data involved.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The LGPD aims to protect the fundamental rights of freedom and privacy. Therefore, the key issues for using personal data include, among others, the observance of the principles that should guide the personal data processing activities, such as: the principle of necessity and non-discrimination; processing activity grounded on a legal basis; the adoption of technical and administrative security measures; and the guarantee of rights to the data subjects.

4.2 How do such considerations change depending on the nature of the entities involved?

The LGPD is not applicable for the following purposes: (i) private and non-economic processing activity performed by a natural person; (ii) journalistic and artistic; (iii) academic; (iv) public security, national defense, state security or activities of investigation and repression of criminal offences; or (v) when the personal data come from outside the Brazilian territory and is not subject to communication and/or shared use of data with Brazilian processing agents or subject to international data transfer with a country other than the country of provenance.

4.3 Which key regulatory requirements apply?

The processing of personal data must be carried out for legitimate, specific, explicit purposes informed to the data subject and compatible with the informed purpose, and limited to what is necessary to achieve it. The processing must also be supported by one of the hypotheses provided for in the LGPD (legal basis). Specifically with regard to health data, considered by the LGPD as sensitive data, only the following legal bases apply: (i) upon provision of consent by the data subject; (ii) compliance with legal or regulatory obligations by the controller; (iii) for execution of public policies, by the public administration; (iv) for the performance of studies by research organisations; (v) for the regular exercise of rights in legal, administrative or arbitration proceedings; (vi) for the protection of the life or physical safety of the data subject or of a third party; (vii) for the protection of health, exclusively in procedures performed by health professionals,

health services or health authorities; and (viii) for fraud prevention and data-subject security, in identification and authentication processes of registration in electronic systems. Processing of sensitive personal data based on the legitimate interest of the controller or a third party is not permitted by the LGPD.

Based on the sensitivity of health data, the LGPD prohibits communication or shared use between controllers with the aim of obtaining economic advantage (except for the provision of health services, pharmaceutical assistance, healthcare and auxiliary services of diagnosis and therapy, in addition to portability or financial and administrative transactions resulting from the use and/or provision of the aforementioned services), as well as the use of such data for risk selection for contracting private healthcare insurance plans, and for the hiring or exclusion of beneficiaries.

4.4 Do the regulations define the scope of data use?

Brazilian laws and regulation provide that data can be used when the processing agents observe the principles of: purpose; adequacy; necessity; free access; data quality; transparency (subject to commercial and industrial secrets); security; prevention; non-discrimination; and accountability. In addition, the processing activity must be adequate to one of the legal bases provided for in the LGPD.

4.5 What are the key contractual considerations?

Brazil, unlike the European Union, does not oblige processing agents to enter into Data Processing Agreements (DPAs). However, this is a highly recommended practice, especially as the LGPD establishes that processing agents will be able to formulate good practices and governance rules. Therefore, the adoption of DPAs is a reality in the Brazilian market, and the agreement usually addresses the responsibilities of each processing agent, fines for non-compliance, transfer rules and deadlines for communications, among others.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The Federal Constitution states that a person's privacy, private life, honour and image are inviolable, and ensures the right to compensation for economic and non-economic damages resulting from violation thereof. It also states that confidentiality of mail, telegraphic communications, data and telephone communications is inviolable except by court orders, in the manner established by law for purposes of criminal investigations or discovery. Recently, the protection of personal data was also considered a fundamental right (Amendment No. 115/2022 to the Federal Constitution). In addition, the LGPD has an extensive list of rights provided to data subjects, which can be exercised at any time, at no cost, which include rights to: (i) confirmation of the existence of processing activities; (ii) access; (iii) correction of incomplete, inaccurate or outdated data; (iv) anonymisation, blocking or deletion of unnecessary, excessive personal data or data processed in violation of the law; (v) portability of data to another service or product provider; (vi) obtainment of information on the sharing of personal data with third parties (public and/or private entities); (vii) erasure of data processed with the consent of the data subject; (viii) information on the possibility of the data subject not giving consent, and consequences in the event of refusal; (ix) withdrawal of consent; (x) opposition; and (xi) review of automated decisions. Finally, the data subject will always have the right to file a petition against the data controller and/or the Brazilian Regulatory Authority (ANPD), and this does not prevent him/her from filing lawsuits in Courts.

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

Processing agents that violate the rules set out in the LGPD, including but not limited to unlawful processing activities, will be subject to administrative sanctions, applicable by the ANPD, ranging from a warning, financial sanctions, such as a fine based on the turnover of the economic group established in the country, blocking or deletion of data, publication of the violation, and total or partial prohibition of the exercise of activities related to data processing.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The key issue to be considered is to ensure that there is an adequate legal basis for data sharing (as provided for in the LGPD) and, if the legal basis used is consent, it will be necessary to obtain free, informed and unequivocal consent from the data subject. The formalisation of DPAs between the processing agents is also important in order to mitigate risks and to be aligned with the law. Moreover, data sharing must be provided for in privacy policies/notices.

Also, the communication or the shared use of sensitive personal data related to health among data controllers for economic gain may be prohibited, except in cases related to the provision of healthcare services, pharmaceutical and healthcare assistance.

Finally, the international transfer of personal data will only be allowed in the events provided for in Article 33 of the LGPD, which include: (i) transfers to countries or international bodies that provide a degree of personal data protection in line with the LGPD; (ii) the data controller offers and substantiates guarantees of compliance with principles, data subject's rights and a data protection system by using standard contractual clauses or binding corporate rules, for example; (iii) the transfer is necessary for international legal cooperation between public intelligence, investigation and prosecution agencies, in accordance with international law; (iv) the transfer is necessary to protect the life or physical safety of the data subject or a third party; (v) ANPD authorises such transfer; (vi) the transfer results in a commitment assumed in an international cooperation agreement; (vii) the transfer is necessary for the execution of public policy or due public services; or (viii) the data subject has provided his/her specific and highlighted consent for the transfer, with prior information on the international nature of the operation, clearly distinguishing it from other purposes.

5.2 How do such considerations change depending on the nature of the entities involved?

The LGPD does not materially change the obligations that entities of different natures will have in relation to the core aspects of the LGPD, so all data processing agents must follow the principles that guide the law.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The key regulatory requirement is to find an appropriate legal basis for the processing activity, and comply with all the principles established by the LGPD, such as purpose, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination and accountability.

6 Intellectual Property

6.1 What is the scope of patent protection?

The Industrial Property Law (Law No. 9,279/1996 (LPI)) encompasses patent protection, as well as trademarks and industrial designs. Brazil is part of the World Trade Organization, so it complies with all basic international rules and requirements provided for in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). Brazil is also part of the Patent Cooperation Treaty.

The LPI protects both patent types: (i) Patent of Invention (PI), that are products or processes considered inventive, new and that have industrial application, and; (ii) Utility Models (MU) – in Europe known as "petit" patents – are usually related to functional improvements in other technologies. PIs are valid for a period of 20 years from the date of filing with the Brazilian National Institute of Industrial Property (INPI), and MUs are valid for 15 years from filing.

Brazil has a "first-to-file" system, which provides patent protection to the first applicant to file an application for an invention. In general, the INPI follows European standards for patentability. Under the approach, creations must solve technical problems and yield technical effects to be considered inventions and, thus, patentable.

In any case, the LPI expressly states that "surgical techniques and methods, as well as therapeutic or diagnostic methods, for application to human or animals" are not subject to patent protection.

6.2 What is the scope of copyright protection?

Copyrights are ruled by the Copyright Law (Law No. 9,610/1998 (LDA)). Software is protected as a copyright, although there is a specific law in this regard (Law 9,609/1998). These laws protect copyrights related to artistic, literary and scientific creations for the author or creator. Contrary to industrial property, the registration of copyrights before the INPI is not mandatory.

Copyright protection in Brazil, among other things, also encompasses databases.

Since Brazil is part of the TRIPS Agreement and the Berne Convention for copyrights, it complies with all basic international rules and requirements related to copyrights.

6.3 What is the scope of trade secret protection?

Trade secret protection relates to confidential information that gives some competitive advantage to a company. They differ from patents and trademarks because their protection is not guaranteed by a registration. The protection of trade secrets is usually enforced by contracts and unfair competition laws.

Article 195 of the LPI lists several unfair competition crimes, which include the unauthorised use of confidential information (trade secrets) obtained during a contractual or employment relationship, or that have been obtained in an illicit or fraudulent manner.

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

Technology transfer agreements are regulated by the INPI (Resolution No. 199/2017), as provided for in the LPI. Their submission and registration with the INPI are mostly recommended for tax purposes, so academic technology transfers among Brazilian parties usually are not registered with the INPI.

In general, academic Research and Development (R&D) is strictly related to public universities and other public Science, Technology and Innovation Entities (ICTs), so the most important law in this regard is Law No. 10,973/2004 (Innovation Law – as further amended and regulated).

6.5 What is the scope of intellectual property protection for software as a medical device?

The registration of software as a copyright is not mandatory for protection in Brazil. As a rule, following the European approach, the INPI does not grant patent protection for software (source code), although a medical device could be considered an invention and, thus, protection granted as a patent.

Additionally, it is important to mention that SaMD has been regulated by RDC No. 657/2022, and the registration of this type of software must be required before the ANVISA, not the INPI.

In this regard, said Resolution establishes that certain software should not be considered medical devices, as follows: (i) for well-being, without performing activities of prevention, diagnosis, treatment, rehabilitation or contraception; (ii) used exclusively for administrative and financial management in health services; (iii) those that process medical demographic and epidemiological data, without any clinical diagnostic or therapeutic purpose; and (iv) shipped in a medical device under a health surveillance regime.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

Since industrial property rights are generally granted to individuals by the Federal Constitution, although the LPI does not expressly prohibit the registration of patents by AI, the INPI has never granted a patent indicating an AI as an inventor. Unless specific legislation is created regarding this matter, it is likely the INPI will never name an AI device as an inventor for a patent.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The most important law in this regard is the Innovation Law, which is regulated by Decree No. 9,283/2018. These laws establish several ground rules for cooperation between the Government (as well as public ICTs) and private entities, providing valuable tax incentives to them. In addition, there are several local agencies and public entities created to promote and develop R&D activities in Brazil, such as FINEP (created by Decree No. 61,056/1967) and hundreds of public ICTs.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

R&D agreements usually have strong IP sections providing for the rights related to collaborative improvements. The LPI and the Copyright Law have provisions regarding the development

of technology by employees and service providers; however, joint improvements and other improvements created under any kind of technology transfer/licence agreement should be contractually regulated.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

Agreements between healthcare service providers and non-healthcare companies must include specific provisions concerning liability of the parties, data privacy, cybersecurity, confidentiality and intellectual property rights.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Technology has radically changed patient care and hospital management. The use of AI in healthcare, accompanied by machine learning, has several applications, such as: (i) management of patient risk levels, in order to prioritise diseases that require more attention; (ii) creation of health protocols by states and municipalities to gather relevant information about diseases, such as on the evolution of COVID-19, allowing monitoring of virus dissemination; (iii) bed management, avoiding hospital collapse; (iv) automation of tasks, such as requesting medications; (v) cost and fraud reduction, since the system relies on organised processes; and (vi) personalised care, since the technology is able to identify the individual risks and needs of each patient.

8.2 How is training data licensed?

It is good practice that training data is not actual personal data, in order to protect real personal data. Otherwise, personal data subjects need to be informed that their data will be used for training data in compliance with the LGPD.

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

The intellectual property sector has a major challenge related to the evolution of machine learning, which enables evolving algorithms to teach a machine which actions to take.

Intellectual property laws in Brazil generally protect creations of the human mind, thus, theoretically, a machine cannot be considered an inventor or a copyright holder. At the time of writing, in Brazil, algorithms resulting from machine learning are not covered by intellectual property laws.

Bill No. 5,051/2019 aims to establish the principles for the use of AI, and Bill No. 5,691/2019 establishes the National Policy for Artificial Intelligence. Both Bills aim to establish that AI must respect the constitutional principles of dignity, human rights, protection of personal data and privacy. Nonetheless, even after its approval, more specific regulations will be necessary.

8.4 What commercial considerations apply to licensing data for use in machine learning?

If the data used in the machine-learning process corresponds to personal data, the use must be linked to an adequate legal basis provided for in the LGPD. To date, there is no specific regulation for data that is used for machine learning; however, the principles provided for in the LGPD must be observed, informing the data subject that his/her data may be used for machine learning.

Furthermore, since the Copyright Law protects databases organised in a creative and unique way, which constitute an intangible property of the company, its use and transfer can be the object of a licence agreement, including in a machine-learning environment.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Based on the CDC, the entire chain of products/services suppliers is liable before consumers – the CDC establishes strict liability related to products'/services' defects and errors. Additionally, the LGPD provides for administrative penalties in the event of violation of subjects' rights concerning personal data and privacy.

9.2 What cross-border considerations are there?

The international transfer of personal data is permitted by the LGPD, provided that it is in compliance with the requirements set forth in Article 33 of the referred law.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Possible violation of the LGPD, including data breach and exposure of the subject's medical data.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Non-healthcare companies may face issues involving compliance with data privacy regulation, as well as capacitation of professionals to be adequately trained to use the new technologies, in addition to any regulatory adjustments.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Despite its growing market, the digital healthcare sector lacks legal certainty with regard to venture capital and private equity firms, especially regarding liability before consumers, users and the Government in general.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Lack of specific and unique regulation encompassing all the technologies related to digital health, or at least the technologies already implemented in the healthcare system, is a strong barrier, since it creates legal uncertainty.

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 Ministry of Health, ANVISA, ANS and CFM. The approval and certification of a clinical or medical facility and/or product depend on the authorisation/registration by ANVISA. ANVISA is also responsible for the registration of medical devices in general, including SaMD.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

There are two types of healthcare systems in Brazil: the public healthcare system (SUS), and the private healthcare insurance system. The reimbursement by a private insurer depends on the type of insurance agreement held by the consumer, in that case the value differs according to the insurance plan. The SUS provides free healthcare, including the use of digital health solutions at the disposal of the population, such as ConecteSUS.

10.7 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 legal concerns involving digital health in Brazil, there are practical difficulties for the implementation of digital health systems, such as: low availability of financial resources in the public sphere; proper training for medical and administrative teams to handle these new technologies and knowledge about their risks; and the informatisation of the population in general about the new health functionalities.

Ricardo Barretto Ferreira da Silva is a Senior Partner at Azevedo Sette Advogados and Head of the TMT legal practice. He graduated from São Paulo University (USP) Law School in 1973 and is an Alumni of the Institute of World Affairs, Connecticut, USA (1973). Ricardo completed his graduate research work in taxation and corporate laws at the University of North Dakota, USA in 1974. He is an experienced attorney on Corporate Matters, Tax, M&A, Intellectual Property, TMT, Privacy, and Data Protection. Before becoming a Senior Partner at Azevedo Sette Advogados, Ricardo was a Co-founder and Chair of several international associations, such as the Brazilian Information Technology and Telecommunications Association (www.abdtic.org.br) and the International Bar Association (IBA) (www.ibanet.org); as well as a Co-founder and Managing Partner of two renowned Law Firms (CFF and BKBG) (1975–2004 and 2004–2016). He is the Editor and Co-author of numerous publications and articles in connection with IP, IT, Media, Telecoms, Privacy, Data Protection, Outsourcing and Copyright.

Azevedo Sette Advogados
Av. Pres. Juscelino Kubitschek, 1327
11th Floor – International Plaza II. 04543-011
São Paulo – SP
Brazil

Tel: +55 11 4083 7600
Email: barretto@azevedosette.com.br
URL: www.azevedosette.com.br

Juliana Gebara Sene Santos Ikeda is a Partner in the TMT legal practice at Azevedo Sette Advogados and Head of the Life Sciences and Intellectual Property areas. She first graduated from the Pontifical Catholic University of São Paulo (PUC/SP, Brazil 2006); then obtained a specialisation degree in Contracts from Fundação Getúlio Vargas, 2010; and later completed a Master's Degree in Intellectual Property Law at the University of Turin, together with the World Intellectual Property Organization (WIPO) (LL.M. 2013). Juliana also holds Certifications in the following areas: International Business Negotiation (Berkeley University); Technology Transfer Agreements (the Brazilian Association of Intellectual Property Agents (ABAPI)); and Intellectual Property (London School of Economics (LSE)). In 2022, Juliana was recognised by *Análise Advocacia* and *Análise Advocacia Mulher* as one of the most admired Brazilian lawyers in Intellectual Property and Contracts, within in the State of São Paulo, in the Construction and Engineering sector. She has also co-authored multiple articles on Contracts, IP, Technology and Life Sciences, which were published by renowned international legal publications.

Azevedo Sette Advogados
Av. Pres. Juscelino Kubitschek, 1327
11th Floor – International Plaza II. 04543-011
São Paulo – SP
Brazil

Tel: +55 11 4083 7600
Email: jikeda@azevedosette.com.br
URL: www.azevedosette.com.br

Lorena Pretti Serraglio is Coordinator of the Privacy and Data Protection practice at Azevedo Sette Advogados and she is part of the TMT practice. She is also a Consultant for the Special Data Protection Commission of the Brazilian Bar Association. Lorena has an MBA in Electronic Law from *Escola Paulista de Direito*. She graduated from the Internet Governance School of the Internet Steering Committee in Brazil and in a course on Personal Data Protection and Privacy, provided by Data Privacy Brazil. Lorena has co-authored several articles and books. She is a guest teacher of Digital Law at Senac São Paulo and a speaker on digital law, cyber security and data protection. She is recognised by *Análise Advocacia* in the specialties of Digital Law and Compliance and she is a recognised figure among technology companies, particularly in the State of São Paulo. She is also recognised by *The Legal 500*'s international rankings in the areas of Cybersecurity and Data Protection.

Azevedo Sette Advogados
Av. Pres. Juscelino Kubitschek, 1327
11th Floor – International Plaza II. 04543-011
São Paulo – SP
Brazil

Tel: +55 11 4083 7600
Email: lserraglio@azevedosette.com.br
URL: www.azevedosette.com.br

Founded in 1967, Azevedo Sette Advogados has established, along five decades of existence, a history of strength, credibility and excellence in legal services. Azevedo Sette Advogados is internationally recognised for providing solutions in different areas of law (full service), competently covering each of these practices, working on contracts, legal opinions and preventive legal analysis, as well as in the sphere of judicial and administrative litigation. With wide expertise in the high-tech sector and awareness at all times to the ongoing process of technological evolution, expansion of the technology market, and the complexity of regulatory frameworks governing the sector, Azevedo Sette Advogados has worked to assemble and consolidate a specialised team to serve the growing demand of clients in the technology sector, including digital health and Life Sciences.

www.azevedosette.com.br

Azevedo Sette
ADVOGADOS

China


Cindy Hu


Jason Gong


Jiaxin Yang

East & Concord Partners

1 Digital Health

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

Digital health is not a legal term defined under the laws and regulations of the People's Republic of China ("PRC") but is frequently referred to in commercial contexts and industry policies.

Digital health usually refers to the development and use of digital technologies to popularise health knowledge and its implementation to related fields, covering the application of digital technologies such as the Internet of Things ("IoT"), artificial intelligence ("AI") and big data in medical services and health management. Digital health usually utilises technologies such as big data and AI to provide solutions for medical treatment, clinical research, drug development, imaging diagnosis, health management and other medical and healthcare needs.

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

The key emerging digital health technologies include AI, mHealth, wearable devices, robotics, 3D printing, blockchain, global positioning system technology and 5G technology.

1.3 What are the core legal issues in digital health for your jurisdiction?

Personal privacy protection and data security are the core legal issues in digital health. In addition, the monopoly of healthcare data, the liability for medical damage caused by medical AI, and the ethical risks brought by the application of AI diagnosis and treatment technology are also common legal issues in digital health.

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

Influenced by COVID-19, China's online medical advantages have been highlighted, and the market share of digital health has increased continuously. According to the digital health report "2022 (I) China Digital Health Market Data Report", by June 2022, the market size of China's Internet medical industry has reached CNY 309.9 billion and the transaction size of the pharmaceutical e-commerce industry has reached CNY 239 billion. It is estimated that the scale of China's digital health market will increase to CNY 4,222.8 billion in 2030, with a compound annual growth rate of 30.9%.

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

According to the relevant industry data, as of June 30, 2022, the top five digital health companies are JD Health, Alibaba Health, Ping An HealthKonnect, We Doctor and Miaozhou Doctor.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core healthcare regulatory schemes related to digital health include the following:

- Law of the PRC on the Promotion of Basic Medical and Health Care.
- Regulation on the Administration of Medical Institutions.
- Administrative Regulations on Application of Electronic Medical Records (for Trial Implementation).
- Administrative Measures on Standards, Security and Services of National Healthcare Big Data (for Trial Implementation).
- Administrative Measures for Internet-based Diagnosis (for Trial Implementation).
- Administrative Measures for Internet Hospitals (for Trial Implementation).
- Administrative Regulations on Telemedicine Services (for Trial Implementation) ("Administrative Regulations on Telemedicine Services").
- Detailed Rules for the Supervision of Internet Diagnosis and Treatment (for Trial Implementation).
- Guiding Opinions of the State Council on Vigorously Advancing the "Internet Plus" Action.

- Opinions of the General Office of the State Council on Promoting the Development of "Internet Plus Health Care".
- Notice of the National Health Commission's office on the Pilot Work of "Internet Plus Nursing Service".
- Guiding Opinions of the National Healthcare Security Administration on Improving the "Internet Plus" Medical Service Price and Medical Insurance Payment Policy.
- Guiding Opinions of the National Healthcare Security Administration on Actively Promoting the Medical Insurance Payment Work of "Internet Plus" Medical Services (Guiding Opinions of "Internet Plus" Medical Services).
- Information Security Technology-Guide for Health Data Security (GB/T 39725-2020).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The other core regulatory schemes include the following:

- Civil Code of the PRC ("Civil Code").
- Anti-Unfair Competition Law of the PRC ("Anti-Unfair Competition Law").
- Cybersecurity Law of the PRC ("Cybersecurity Law").
- Data Security Law of the PRC ("Data Security Law").
- Personal Information Protection Law of the PRC ("Personal Information Protection Law").
- Administrative Regulations on Human Genetic Resources of the PRC.
- Measures for Cybersecurity Review.
- Measures for Administration of Cybersecurity of Medical and Health Institutions.
- Interim Provisions on Banning Commercial Bribery.
- Measures for the Administration of Population Health Information (for Trial Implementation).
- Measures for the Management of Scientific Data.
- Information Security Technology-Personal Information Security Specification (GB/T 35273-2020).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The regulatory schemes which apply to consumer healthcare devices or software in particular include the following:

- Law of the PRC on the Protection of Consumer Rights and Interests.
- Product Quality Law of the PRC ("Product Quality Law").
- E-Commerce Law of the PRC.
- Regulations on the Supervision and Administration of Medical Devices ("Medical Devices Regulations").
- Rules for the Classification of Medical Devices.
- Administrative Measures on the Registration and Recordation of Medical Devices.
- Measures for the Supervision and Administration of Medical Device Production.
- Measures for the Supervision and Administration of Business Operations of Medical Devices.
- Measures for the Supervision and Administration of Online Sale of Medical Devices.
- Guiding Principles for Technical Review of Mobile Medical Device Registration.
- Guiding Principles for Registration Review of Medical Device Software Registration.
- Guiding Principles for Registration Review of Network Security Registration of Medical Devices.
- Guiding Principles for Registration Review of Artificial Intelligence Medical Device.
- Guiding Principles for Classification and Definition of Artificial Intelligence Medical Software Products ("Guiding Principles for AI Medical Software Products").
- Classification Catalogue of Medical Devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The principal regulatory authorities include the following:

- The National Health Commission ("NHC"): The NHC primarily formulates and enforces national health policies and regulations pertaining to healthcare services, healthcare institutions and healthcare professionals. Internet-based diagnosis and treatment and remote consultations between healthcare institutions are both regulated by the NHC.
- The National Medical Products Administration ("NMPA"): The NMPA regulates drugs, medical devices and cosmetics, and is responsible for the safety, supervision and management of standard formulation, registration and manufacturing to post-market risk management.
- The National Healthcare Security Administration ("NHSA"): The NHSA is primarily responsible for formulating and implementing policies related to basic medical insurance ("BMI"), such as reimbursement, pricing and the procurement of drugs, medical consumables and healthcare services.
- The Ministry of Industry and Information Technology ("MIIT"): The MIIT is responsible for the management of the Internet industry, the access management of the information and communication industry, and the construction of the network and information security-guarantee system in the information and communication field. In terms of digital health, MIIT is responsible for supervising relevant technology development, personal data protection, etc.
- The Cyberspace Administration of China ("CAC"): The CAC is responsible for the overall planning and coordination of network security and relevant supervision and administration, including regulating the cross-border transfer of healthcare data, cybersecurity review of internet hospitals, network personal privacy and information protection.
- The State Administration for Market Regulation ("SAMR"): The SAMR is responsible for supervising the market order in market transactions, online commodity transactions and related services, and organising the investigation and punishment of illegal medical advertisements, anti-commercial bribery and other acts against unfair competition.
- The Ministry of Public Security ("MPS"): The MPS is responsible for enforcing the Cybersecurity Classified Protection System and investigating cybercrimes, including conducting inspections and recording filings for the related system completed by healthcare institutions (internet hospitals are included), and investigating crimes related to infringement of personal data and illegal access to information systems.

2.5 What are the key areas of enforcement when it comes to digital health?

Personal information protection, data security and cybersecurity

are the key areas of enforcement in relation to digital health. China has established the Personal Information Protection Law (effective from November 1, 2021), the Data Security Law and the Cybersecurity Law. The Multi-Level Protection Scheme ("MLPs") implemented in the field of cybersecurity, as a compulsory legal obligation stipulated by the Cybersecurity Law and relevant regulations, has become a main focus in enforcement in most industries, including digital health.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

The main applicable laws and regulations include: Medical Devices Regulations; Rules for the Classification of Medical Devices; Administrative Measures on the Registration and Recordation of Medical Devices; Measures for the Administration of the Clinical Use of Medical Devices; and Guiding Principles for AI Medical Software Products.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

In addition to the relevant regulatory provisions applicable to medical devices, AI/Machine Learning ("ML") powered digital health devices or software solutions shall also comply with the Management Specification of AI-Aided Diagnosis Technology and Management Specification of AI-Aided Therapy Technology in terms of special requirements for medical institutions to carry out AI-aided diagnosis technology and AI-aided treatment technology in relation to department setting, staffing, technical management, etc.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Medical institutions shall comply with the Administrative Regulations on Telemedicine Services in terms of personnel setting, equipment and facilities, telemedicine service process, responsibility sharing and management.
- **Robotics**
  The liability arising out of medical accidents caused by robots is difficult to identify, and the division of responsibilities among producers, operators and users of intelligent robots is more complex.
- **Wearables**
  In accordance with Medical Devices Regulations and Rules for the Classification of Medical Devices, some wearables (such as hearing aids or pain relief therapeutic instruments) are regarded as medical devices, and are subject to the relevant regulatory requirements on medical devices.
- **Virtual Assistants (e.g. Alexa)**
  For virtual assistants like Siri and Alexa, problems such as eavesdropping, leakage of personal privacy and information may occur.
- **Mobile Apps**
  Mobile medical apps involve patients' electronic medical records, health records, consultation information and image data, and are highly dependent on the network and information technology. When cybersecurity or technical security is attacked or threatened, privacy and information leakage may occur.
- **Software as a Medical Device**
  In accordance with Medical Devices Regulations, Rules for the Classification of Medical Devices, and Guiding Principles for AI Medical Software Products, Software as a Medical Device ("SaMD") will be subject to the relevant regulatory requirements on medical devices.
- **Clinical Decision Support Software**
  The main application scenarios of Clinical Decision Support Software ("CDSS") include drug allergy warning, clinical guidelines, drug dose support, remote patient monitoring service, etc. CDSS systems have been applied in Chinese medical institutions; however, there are problems such as the lack of CDSS product access standards and industry regulations.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Please refer to question 2.7.
- **IoT (Internet of Things) and Connected Devices**
  Most of the data stored or collected by the IoT terminal belongs to sensitive medical information. Once important information is leaked or maliciously modified by hackers, it will lead to cybersecurity, data and information leakage problems.
- **3D Printing/Bioprinting**
  The application of 3D bioprinting in medical treatment is still in the early stage of exploration, and no specific provisions for 3D bioprinting have been issued in China.
- **Digital Therapeutics**
  At present, digital therapy products are generally supervised as a medical device and are subject to relevant regulatory requirements on medical devices.
- **Natural Language Processing**
  Natural language processing involves a large number of personal oral languages which are fed back to the natural language processing system for identification and processing and, therefore, may lead to the problem of leakage of personal information and data.

3.2 What are the key issues for digital platform providers?

In terms of the healthcare sector, digital platform providers are highly regulated. In terms of industry access, digital platform providers need to apply for different business licences according to their business types, for example, where the business involves online data processing, voice and image communication and other business forms, the digital platform providers are required to obtain value-added telecom service qualification; where the digital platform providers provide users with drug and medical device information through the Internet, they shall obtain the qualification of an Internet drug information service. In addition, in the process of business operation, it is also necessary to comply with the above regulatory requirements on personal information protection, data security and cybersecurity.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Some of the key issues for the use of personal data include how to standardise the code of conduct in such different links as collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information so as to ensure the rational use of personal information without infringement.

4.2 How do such considerations change depending on the nature of the entities involved?

In addition to meeting the general provisions on the use of personal data, entities of different natures shall also comply with other relevant provisions, for example:

If the entity involved is a third party that obtains relevant personal information through sharing or joint processing in accordance with the terms of the relevant agreement, it shall process the personal information in accordance with the relevant agreement and shall not process personal information beyond the agreed processing purpose and method. If it infringes on individuals' rights and interests in terms of personal information and causes damage, it shall bear joint and several liability in accordance with the law.

If the entity involved is located overseas and has one of the following circumstances: 1) providing products or services to domestic natural persons; 2) analysing and evaluating the behaviour of domestic natural persons; or 3) under other circumstances stipulated by laws and administrative regulations, the said entity shall establish a special institution or designated representative within the territory of the PRC to handle matters related to personal information protection, and submit the name of the relevant institution or the name and contact information of the representative to the relevant department responsible for personal information protection.

If the entity involved falls within the definition of the critical information infrastructure operator ("CIIO"), it shall also abide by the Regulations on Security Protection of Critical Information Infrastructure.

4.3 Which key regulatory requirements apply?

The Personal Information Protection Law and other relevant laws and regulations stipulate the general rules on the collection and use of personal information. The use of personal information shall follow the principles of legality, legitimacy, necessity and integrity, and shall be open and transparent, and ensure the security and accuracy of personal information.

For example: 1) the data collection channel shall be legal, an advanced personal consent shall be obtained in accordance with the law. There must be an acknowledgment of the processing purpose, processing method, type of personal information processed, storage period, etc.; 2) the processing of personal information shall have legal basis and shall not excessively collect personal information; and 3) personal information collectors shall formulate corresponding internal systems for information protection.

In addition, it should be noted that: 1) certain activities performed outside the PRC related to processing personal information of natural persons residing in the PRC will also be regulated by Chinese laws; and 2) when providing the personal information of those located outside of the PRC, one shall also comply with the following requirements: a) passing the security assessment organised by the national network information department; b) obtaining a personal information protection certification provided by professional institutions; c) signing a contract with the overseas recipient according to the standard contract formulated by the national network information department to specify the rights and obligations of both parties; and d) special regulatory requirements of laws, administrative regulations or other conditions stipulated by the national network information department.

4.4 Do the regulations define the scope of data use?

According to the Personal Information Protection Law and other relevant provisions, the purpose, method and scope of processing personal information shall be clearly stated, and the processing shall be limited to the minimum scope to achieve the purpose of processing, and personal information shall not be excessively collected. The third party shall process personal information within the scope agreed by the individual on the processing purpose, processing method and type of personal information.

In addition, the Information Security Technology – Personal Information Security Specification (GB/T35273-2020) provides detailed guidance on data use scenarios, assumptions and scope under various circumstances.

4.5 What are the key contractual considerations?

Where a contract is signed directly between an information processor with an information provider, the terms of the contract such as scope of data information processing, processing rules, exit restrictions, security measures, requirements for deletion, destruction or return of data and liability for breach of contract should be agreed on. The name and contact information of the personal information processor shall be informed in detail, and the purpose and method of processing the personal information, the type and retention period of the personal information processed, as well as other matters that are required to be informed according to laws and administrative regulations, shall be informed.

Where two or more personal information processors jointly process personal information, in addition to clearly specifying the above information, they shall also agree on their respective rights and obligations in the terms of the contracts.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The Civil Code clearly stipulates that a natural person's personal information shall be protected by law. For any unreasonable usage of personal information which infringes on the civil rights of individuals, the infringer shall bear civil liability according to law. For example, if a medical institution or its medical staff leak personal information, or disclose medical records without the consent of the patient, the medical institution shall bear tort liability.

The Criminal Law of the PRC stipulates corresponding criminal responsibility for infringement of citizens' personal information and violation of relevant laws.

In addition, those who violate relevant laws and regulations such as the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law or the Anti-Unfair Competition Law will also face corresponding civil, administrative and even criminal liabilities.

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

The Technical Guide for Clinical Trial Data Management regulates the management of clinical trial data and the prevention and treatment of data errors and deviations from the following aspects: the responsibilities, qualifications and training of data management-related personnel; the requirements of the management system; the standardisation of test data; the main contents of data management; the guarantee and evaluation of data quality; and safety data and severe adverse drug reaction cases.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The key issues to consider when sharing personal data include the following:

- whether the sharing of personal data complies with the principles of necessity and realisation of legitimate purposes;
- whether to inform and obtain personal consent;
- whether it meets the requirements of security measures necessary for data sharing;
- whether the contract signed by all parties to data sharing include terms such as: the processing purpose; duration; processing method; type of personal information; protective measures; and rights and obligations of both parties;
- whether there is personal data that is prohibited from being shared; and
- whether a cross-border data transfer is involved.

5.2 How do such considerations change depending on the nature of the entities involved?

In addition to meeting the general data-sharing requirements, entities of different natures should also comply with other relevant provisions, for example:

If the sharing party is the CIIO, it shall also abide by the Regulations on Security Protection of Critical Information Infrastructure.

However, if the receiving party is an overseas entity, specific conditions shall be met. For example, it must have passed the security assessment organised by the national network information department, passed the personal information protection certification conducted by professional institutions, or entered into a contract with the overseas recipient according to the standard contract formulated by the national network information department to stipulate the rights and obligations of both parties.

5.3 Which key regulatory requirements apply when it comes to sharing data?

First, the provider of the shared data shall: 1) conduct the impact assessment of personal information protection in advance; 2) inform the individual of the recipient's name, contact information, processing purpose, processing method and type of personal information, and obtain the individual's consent; 3) agree with the recipient on the purpose of entrusted processing, time limit, processing method, type and protection measures of personal information, as well as the rights and obligations of both parties; and 4) supervise the recipient's processing activities of personal information.

Secondly, the recipient of the shared data shall: 1) process personal information according to the agreement, and shall not process personal information beyond the agreed processing purpose and processing method; 2) if the relevant contract is not effective, invalid, revoked or terminated, the personal information shall be returned or deleted and shall not be retained; 3) without the consent of the provider, the recipient shall not entrust others to process personal information; and 4) the recipient shall also take necessary measures to ensure the security of personal information and assist the provider in performing its personal information protection obligations.

In addition, attention should also be paid to the regulatory requirements involved in the cross-border transfer of personal information. For example, the CIIO or the personal information processor who processes personal information up to the amount specified by the national network information department shall store within China the personal information collected and generated in China. If it is necessary to provide it to an overseas recipient, the security assessment organised by the national network information department shall be passed. (If the laws, administrative regulations and national network information department stipulate that the security assessment may not be carried out, such stipulations shall prevail.)

In accordance with the Measures for Cybersecurity Review (issued on December 28, 2021 and effective on February 15, 2022), if network platform operators who hold personal information of more than 1 million users are to be listed abroad, they shall apply to the cybersecurity review office for cybersecurity review.

6 Intellectual Property

6.1 What is the scope of patent protection?

Any technical solutions by using natural laws can be the subject matter of invention patents or utility model patents. The design patent is one of the patent types stipulated in the Patent Law of the PRC, and it protects new design of the whole or part of the product in terms of shape, pattern and/or colour. After a patent is granted, unless otherwise stipulated in the Patent Law of the PRC, no entity or individual may exploit the patent without the permission of the patentee.

6.2 What is the scope of copyright protection?

The subject of copyright protection covers various works, which refers to intellectual achievements that are original and can be expressed in a certain form in the fields of literature, art and science. Computer software is one of the forms of works stipulated in the Copyright Law of the PRC. According to the Copyright Law of the PRC, copyright includes both property rights and personal rights, of which property rights mainly include: reproduction rights; distribution rights; and rental rights.

6.3 What is the scope of trade secret protection?

In accordance with Chinese laws, a trade secret refers to commercial information such as technical information and business operation information not known to the public, which is of commercial value, and for which the rights holder has adopted corresponding confidentiality measures. In accordance with the Anti-Unfair Competition Law, obtaining trade secrets by improper means, disclosing and using trade secrets obtained by others by improper means, disclosing and using trade secrets in his possession but in violation of confidentiality obligations, or abetting, luring and helping others to commit such acts are all acts of infringing trade secrets and corresponding civil liabilities can be imposed. Serious trade secret infringements are defined as a criminal offence under the PRC Criminal Law and is punishable by up to 10 years imprisonment.

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

In China, the laws currently applicable to academic technology

transfers include the Law on Scientific and Technological Progress of the PRC (revised in 2021), the Law on Promoting Transfer and Commercialisation of Scientific and Technological Achievements of the PRC (revised in 2015) and Several Provisions on the Implementation of the Law on Promoting Transfer and Commercialisation of Scientific and Technological Achievements of the PRC issued by the State Council of the PRC in 2016. Such laws and regulations have adjusted previous policies in this field and clarified that the project undertakers, on the premise of no conflict with national security or national/public interests, are legitimately authorised to own relevant intellectual property ("IP") rights arising from the government-funded projects. Furthermore, the project undertakers are encouraged to legally transfer and commercialise these IP rights in various ways. However, any transfer or exclusive license to an overseas company shall be approved by the project administration organisation.

Public universities are conducting pilot programmes in guiding scientific researchers to transfer and commercialise IP rights in line with the laws. According to a document jointly issued by four national-level Ministries in 2020, Chinese universities will gradually establish disclosure systems for service inventions, establish and perfect technology transfer and IP management and operation departments, and explore the reforming of ownership of service inventions, such as division of ownership between universities and researchers, as well as permitting the scientific researchers to apply for patents in the form of non-service inventions in the event the university declines to apply for service patents.

6.5 What is the scope of intellectual property protection for software as a medical device?

SaMD enjoys two forms of protection in China. First, as it is regarded as a type of work protected under copyright, it does not require an application and examination process. Although the protection period is long, the disadvantage is, it is the form of expression that is eligible for copyright protection and not the technical idea. Secondly, SaMD can be protected as it is considered an invention patent. It should be noted that pure algorithms or calculation rules are unpatentable subject matter under the Patent Law of the PRC: only when the technical features of the hardware are included in the claims can it be considered to be protected. Unlike copyright, what is protected by a patent is the technical solution itself and, therefore, this type of protection is thought to be more powerful.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

In accordance with the current laws and regulations of the PRC, an inventor refers to a person who has made creative contributions to the substantive characteristics of an invention. It is generally understood that the inventor should be a natural person and, therefore, based on the current effective laws and regulations, AI devices are unlikely to be recognised as inventors in China.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Please refer to question 6.4.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

In the case of collaborative improvements, a written contract is required to agree on the rights and obligations of each party; and it is necessary to take into account how to handle the failure of collaborative improvements, as well as the ownership and use of rights of patents and non-patented technologies generated in the collaboration. In the absence of such a written contract, according to the provisions of the Civil Code, the right to apply for a patent shall be jointly owned by the parties to the collaborative improvements. If one party transfers the patent application right jointly owned with other parties, the other parties shall have priority to such transfer under the same conditions. If there is no agreement or the agreement is not clear about the non-patented technological achievements, all parties have the right to use and transfer such achievements.

For Sino-foreign collaborative improvements, it is also necessary to consider the possible application of some mandatory laws and regulations. For example, if Chinese human-genetic resources are involved, especially in cases exporting Chinese human-genetic resource materials, according to the provisions of the Biosecurity Law of the PRC, an approval from the competent department must be obtained. Furthermore, as for the technological achievements produced by using Chinese human-genetic resources to carry out international cooperative research, the patent rights shall be jointly shared by the parties according to the Administrative Regulations on Human Genetic Resources of the PRC.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

When signing agreements with non-healthcare companies, in addition to meeting the above requirements for data sharing, transmission and other processing, healthcare companies shall ensure that non-healthcare companies comply with the national and industrial regulations and requirements of the business they are engaged in, have the necessary business qualifications, have the abilities to implement relevant laws and regulations, implement relevant standards and guarantee data security, and have a comprehensive management system.

According to the Measures for Cybersecurity Review, if a healthcare company qualifies as a CIIO, when it purchases network products and services, it shall anticipate the potential national security risks after the products and services are put into use. Those products and services that affect or may affect national security shall be reported to the cybersecurity review office.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

As a common form of AI, ML is widely used in AI-aided diagnosis and treatment, medical imaging, wearable devices, genetic testing, pharmaceutical research, personal health management and hospital management, etc.

8.2 How is training data licensed?

Data licensing in AI involves the licensing of relevant intellectual property rights, such as patents, software copyrights and trade secrets, and the licensed use shall apply to the Anti-Unfair Competition Law, the Patent Law of the PRC, the Regulations on the Protection of Computer Software and relevant provisions.

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

According to the existing effective laws and regulations, AI can neither be an author in the context of the Copyright Law, nor an inventor or designer in the context of the Patent Law. As a result, the existing laws and regulations do not cover this area. However, with the rapid development of AI technology, the legislation of intellectual property protection of AI-generated contents is an important issue which needs to be urgently addressed. Chinese academia has been holding discussions on this issue as well. However, to date there is no unified understanding or relevant legislative proposals.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Licensing data for use in ML in a business context mainly includes the applicable scope of licensing (duration, territory, sub-license or not), restrictions of data use, non-competition and confidentiality.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

The Civil Code, the Product Quality Law, Administrative Regulations on Telemedicine Services and relevant provisions have specified the liabilities of adverse outcomes in digital health solutions.

Where defects in medical devices and other digital health products cause personal injury or damage to others, victims may claim compensation from the manufacturer of the products or the vendor of the products. After one party makes compensation, that party has the right to seek indemnification from other parties who may be held liable.

If any damage or harm to a patient is caused during the course of diagnosis and treatment by the defects of digital health products, such patient may request compensations from the manufacturer or the relevant medical institution. After making the compensation, the relevant medical institution has the right to recover the losses from the liable medical device manufacturer.

When a dispute occurs in the course of remote medical services, the inviter shall bear corresponding legal liabilities for remote consultation, and the inviter and the invitee shall jointly bear corresponding legal liabilities for remote diagnosis. In terms of remote consultation, where medical institutions conduct remote consultation, the invitee shall provide diagnosis and treatment opinions, and the inviter shall specify the diagnosis and treatment plan. In terms of remote diagnosis, where an inviter and invitee establish a counterpart support or form a medical consortia and other cooperative relationships, the inviter shall carry out auxiliary examinations such as medical imaging, pathology, electrocardiogram and ultrasound; the invited medical institution at a higher level shall conduct diagnosis, and the specific process shall be specified by the inviter and invitee through an agreement.

9.2 What cross-border considerations are there?

According to the relevant provisions of the Personal Information Protection Law, where a personal information processor needs to provide personal information to any party outside China, it should first obtain the individual's consent and conduct advanced assessment of the impact on personal information protection. If the data involves medical and health data, advanced security assessment and review shall also be carried out.

Pursuant to the Special Administrative Measures (Negative List) for Foreign Investment Access (2021 version), the provision of medical services by foreign medical service providers in China is limited to the form of Sino-foreign joint ventures, and foreign medical service providers shall not establish medical institutions in China in the form of sole proprietorship. In addition, foreign investment in the development and application of human stem cells, genetic diagnosis and treatment technologies is prohibited in China.

Where imported digital medical devices are involved, registration or filing of medical devices shall be completed according to the Medical Devices Regulations and relevant provisions, and overseas applicants shall submit the application materials to the medical products regulatory authority through a domestic enterprise, as well as the documents certifying the approval of the marketing of such medical devices by the competent department in the country/region where the applicants are located. (It is not required to submit such documents for innovative medical devices that have not been marketed abroad.) Furthermore, the instructions and labels of imported medical devices shall meet the relevant requirements.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services mainly involve issues such as cybersecurity and data protection. Users upload data to the Cloud and Cloud service providers will manage the data. This may cause issues such as cybersecurity and data breaches and information leakage.

In addition, medical and health data are required to be stored within the territory of China, and those that need to be provided overseas shall be subject to a safety assessment and review according to the relevant regulations. As for service providers who have established data centres in multiple jurisdictions, there may be a risk of illegal cross-border data transfer.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Non-healthcare companies that plan to independently and directly engage in the digital health industry should first obtain the qualification licence for the corresponding business according to law. For example, those intending to provide online consultation, paid medical information and other services

and construct a medical big data Cloud-based platform through medical websites and apps, shall obtain the approval of regulatory agencies and the relevant qualification licences.

If non-healthcare companies such as Internet companies intend to engage in the digital healthcare industry by cooperating with medical institutions, they shall agree with the cooperative medical institutions in a written agreement on the methods of cooperation, the responsibilities and rights of each party in medical services, information security, privacy protection and other aspects.

If non-healthcare companies choose to develop and produce AI medical software, wearable medical devices and other products, they shall also comply with relevant regulatory requirements on medical devices and AI-aided diagnosis technologies.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Apart from business models, business prospects and other commercial factors, VC and PE investors should also pay attention to key issues such as market-access requirements for the industry that the target company falls into, the business qualification and business licence, core technologies and key technicians, procedures for obtaining ownership of relevant intellectual property rights, hardware facilities and cybersecurity protection, etc.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Pursuant to the Measures for the Administration of the Clinical Application of Medical Technologies and relevant provisions, medical technologies in China are subject to a "categorised" regulation system. AI-aided diagnosis and AI-aided treatment fall within the scope of "restricted technology", and a medical institution intending to carry out the clinical application of such restricted technology shall conduct self-assessment according to the standards for the administration of the clinical application of medical technologies. A qualified institution may carry out clinical application and shall report to the health administrative department for filing. New medical technologies which have not been verified in clinical practice are considered to fall within the scope of "prohibitive technology" and cannot be used in clinical diagnosis and treatment.

The clinical adoption of digital health products which fall into the scope of medical devices shall go through approval or filing procedures according to the Administrative Measures on the Registration and Recordation of Medical Devices, the Measures for the Administration of the Clinical Use of Medical Devices and relevant provisions, and shall comply with the requirements in the aspects of clinical trial institutions, systems, procurement, operation management and handling of safety involving the use of medical devices, failing which will result in administrative penalties from the competent authorities.

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 China, there are no physician certification bodies that influence the clinical adoption of digital health solutions. The qualification licence and relevant requirements for physicians engaged in clinical adoptions are mainly stipulated under the Physicians Law of the PRC, the Measures for the Administration of the Clinical Application of Medical Technologies, the Measures for the Administration of the Clinical Use of Medical Devices and relevant provisions.

The China Medical Practitioner Association mainly performs the following duties: to implement industry management, formulate self-discipline rules, provide support such as legal assistance for medical practitioners, provide continuous education for medical practitioners and organise academic meetings and seminars.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

In China, if patients have subscribed to or are covered by BMI, and the expenses of medical treatment items and medical service facilities are partially or completely covered by the BMI catalogue, the relevant expenses can be settled and reimbursed according to the medical service agreements signed between the government medical insurance agency and the designated medical insurance institutions. In addition, patients can purchase private insurance and be reimbursed for relevant medical expenses from private insurance companies.

After the promulgation of the Guiding Opinions of "Internet Plus" Medical Services on October 24, 2020, Internet Plus Medical Services was formally allowed under the medical insurance payment. The expenses of examination and prescription incurred from return visits in "Internet Plus Medical Services" designated medical insurance institutions by the insured in areas subject to overall planning can be reimbursed according to relevant regional medical insurance policies.

10.7 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.

With the advent of the digital era, digital health has undoubtedly become a key area in the construction of digital China. However, the current construction of digital health in China is still in its infancy.

We believe that in the future, China's digital health industry may have the following development trends:

First, "data" and "networks" are the core components of digital health. In the future, China may incorporate the informatics digital construction of medical institutions and medical service into new infrastructure.

In addition, as an emerging medical industry, digital health will profoundly change the medical organisational forms and medical behavioural patterns. The traditional Chinese legal governance framework, government management systems and multi-party relationship of rights, responsibilities and interests need to be readjusted or supplemented. In the future, China may: strengthen and improve the research work of digital medical legislation; improve relevant legislation in light of China's own industrial characteristics and international development trend; formulate and improve the healthcare data construction, opening, sharing and trading systems; clarify the rights and obligations of each participant in digital health; strengthen algorithm governance; and improve the risk-sharing mechanism of digital healthcare, to ensure the healthy and sustainable

development of the digital health industry in China through legislation. In November 2022, the National Health Commission and three other departments jointly released the "14th Five-Year Plan" for National Health Informatisation, which proposed the overall goal of "by 2025, we will initially build and form a unified, authoritative and interconnected national health information platform support and security system, and basically achieve the full coverage of public health institutions and the national health information platform".

Meanwhile, digital health, as a new medical model and business form, has also created new regulatory issues such as information leakage and privacy protection. In order to solve relevant problems, China will establish a governance mode compatible with the sustainable and healthy development of the digital health industry, innovate a coordinated governance model, and build a collaborative, efficient, inclusive and prudent digital medical supervision mechanism.

At last, the development of the digital health industry has accelerated the flat development of the medical service system structure. It is an inevitable trend to explore multiple co-governance in the new medical service system. In the future, industry self-regulation, platform governance, patient and medical staff rights protection may become increasingly important.

Cindy Hu focuses on the areas of corporate M&A, corporate finance and compliance. She is heavily involved in the pharmaceutical and healthcare industry, and leads the pharmaceutical and healthcare team of East & Concord.
Cindy has routinely advised well-known Chinese state-owned and private enterprises, publicly listed companies, and PE/VC funds in the area of pharmaceuticals and healthcare. She was recognised as one of the Top 15 M&A Lawyers by *ALB China*, as well as one of the Client Choice: Top 15 Compliance Versatile Practitioners by *LEGALBAND*. She was also endorsed as a Leading Lawyer in Corporate M&A by *Asialaw Profiles* and China's Top Lawyers (Corporate and M&A) by *LEGALBAND* multiple times. In 2022, Cindy's team ranked on the list of Life Sciences and Healthcare in *The Legal 500* and Pharmaceuticals and Life Sciences in *Asialaw Profiles*. Cindy is widely published both in China and internationally.

East & Concord Partners
22/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District, Beijing 100004
China

Tel: +86 10 6590 6639
Email: cindyhu@east-concord.com
URL: en.east-concord.com

Jason Gong is a partner in the Intellectual Property Department and a key member of the pharmaceutical and healthcare team of East & Concord. Jason's services cover various IP rights procurement and management, due diligence, enforcement and anti-counterfeiting, including both non-contentious, such as patent/trademark prosecution, advising on patent validity and freedom-to-operate, infringement analysis and consulting on patent portfolios, as well as contentious fields, such as patent validity proceedings, infringement litigation, customs protection and other administrative actions against infringers, and IP enforcement at fairs.
Jason has extensive experience in IP protection for the chemical industry including pharmaceutical and life sciences. He represents foreign industry giants in pharmaceutical, agrochemical and refrigerant sections, and also local prestigious universities and academic centres. He frequently provides patent-focused advice for many bio-pharma companies and start-ups.

East & Concord Partners
22/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District, Beijing 100004
China

Tel: +86 10 6590 6639
Email: jianhua_gong@east-concord.com
URL: en.east-concord.com

Jiaxin Yang is the backbone member of the pharmaceutical and healthcare team of East & Concord, with extensive experience in M&A, compliance and risk control in the healthcare sector. She regularly provides support and advice for well-known Chinese state-owned and private enterprises, foreign invested companies, as well as private equity funds on projects concerning stem cell R&D, digital health, wearable medical devices, cybersecurity and data protection.

East & Concord Partners
22/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District, Beijing 100004
China

Tel: +86 10 6510 7422
Email: yangjiaxin@east-concord.com
URL: en.east-concord.com

East & Concord Partners has a well-earned reputation as one of the largest and most comprehensive law firms in China. With more than 600 legal professionals, the firm advises multinational companies, publicly listed companies, privately owned companies, state-owned enterprises, foreign invested companies, government offices and public institutions on a wide range of areas. Headquartered in Beijing, the firm has eight offices strategically located throughout China. The firm has also established extensive cooperation with many well-known international law firms so as to satisfy the development need for economic globalisation.
With more than 20 years of experience, the firm has gained a leading position and earned clients' trust and recognition in areas including: banking and finance; M&A; anti-dumping and anti-subsidy; pharmaceutical and healthcare; infrastructure and project financing; intellectual property; government legal affairs; cybersecurity and data protection; and dispute resolution.

en.east-concord.com

天達共和律師事務所
East & Concord Partners

France


Anne-France Moreau


Lorraine Maisnier-Boché


Caroline Noyrez


Julie Favreau

McDermott Will & Emery AARPI

1 Digital Health

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

"Digital health" is not defined under French law. The French Public Healthcare Code (**FPHC**) refers to "*telehealth*", which includes two forms of remote medical practice by means of information and communication technologies: (i) "*telemedicine*", "which brings one or more healthcare professionals (**HCPs**) together or with a patient, and, where appropriate, other professionals involved in the patient's care", consisting of tele-consultation, tele-expertise, tele-surveillance, tele-assistance, and medical regulation; and (ii) "*telecare*", "which brings a patient together with one or more pharmacists or paramedic[s]".

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

Internet of Things (**IoT**), wearables, virtual reality, augmented reality and metaverse are among key emerging technologies. IoT is one of the fastest-growing digital health trends, with applications in healthcare that benefit patients, families, physicians, hospitals, and insurance companies. The proliferation of healthcare-specific IoT products opens up immense opportunities and the huge amount of data generated by these connected devices holds the potential to transform healthcare. The French government is proactive in this area, notably with the development of the use of digital health tools among patients through the Digital Health Space (*espace numérique de santé*), which is going to be used as national medical records and a secure messaging system between health professionals and patients, and will reference health application for patients.

1.3 What are the core legal issues in digital health for your jurisdiction?

- **Applicable Regime**: the product's regulatory status will determine the relevant pre- and post-commercialisation considerations. Notably, the period for medical device (**MD**) regulatory review has increased in Europe due to the entry into force of the new MD regulations (see question 2.6).
- **Regulatory Evolution and Reimbursement Pathways**: regulations evolve rapidly and reimbursement pathways can be obscure. For instance, telemedicine has been effectively regulated since 2018 in France and the regulatory framework continues to evolve. In 2022, new legislation opened the reimbursement of telesurveillance by the health insurance scheme (**HIS**), subject to certain conditions which will be specified by future decree. A new transitional coverage system was also set up to grant reimbursement for one year for presumed innovative therapeutic or disability compensation MDs. On the other hand, tele-consultation is no longer fully reimbursed by the HIS and the Social Security Financing Bill for 2023 may require authorisation of teleconsultation companies (for coverage) and restrict the at-home practice.
- **Data protection**: digital health is likely to involve the collection, storage, transfer, and processing of (highly sensitive) personal health data, subject to the General Data Protection Regulation (**GDPR**) and the French Data Protection Act (**DPA**) No. 78-17 of 6 January 1978 as modified. Soon, digital health will also be impacted by the European Health Data Space Regulation (**EHDS**) introduced by the European Commission in May 2022, which aims at empowering patients to control and use their health data across any Member State and to foster a genuine single market for digital health services and products. French law also adds security and interoperability requirements specifically applicable to healthcare information systems (see question 2.2).

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

According to a study by the *Institut Montaigne*, in association with McKinsey & Company, the digital health market could generate up to 22 billion euros per year in France. Both public and private actors are betting on this sector. French digital health start-ups raised more than one billion euros between the first and third quarters of 2022.

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

To our knowledge, the five largest digital health companies in France (by revenue) are Doctolib, Alan, Withings, Owkin, and Kry (Livi).

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

European and French legislators have addressed many aspects of digital health; however, there is no comprehensive regulatory

scheme yet. At the French level, such regulations are mostly codified in the FPHC – e.g. anti-kickback and transparency provisions, advertisement of MDs, medical ethics, and manufacturing and distribution of medicinal products. Provisions from other codes may also apply to specific aspects of healthcare. Regulatory agencies also play an important role in the construction and implementation of guidelines to facilitate implementation.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

- **Regulations on MDs**: (see question 2.6).
- **Regulations on anti-kickback and transparency requirements**: (see question 2.1).
- **Regulation and reimbursement**: (see question 1.3 and good practice guidelines set by regulatory agencies).
- **Regulations on electronic medical records**: health data security and interoperability requirements; implementation of a Digital Health Space (see question 1.2) and upcoming EHDS Regulation which fosters the development of electronic medical records at the EU level (see question 1.3).
- **Regulations on data protection**: (see section 4).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

There is no specific regulatory scheme for "consumer devices" as a stand-alone category. General regulations cover various aspects of consumer devices' life cycle. However, the line between wellness consumer devices and MDs with a medical purpose may be difficult to draw, and the latter (including software) are subject to a specific regime (see question 2.6).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

Some of the principal regulatory authorities in France are the following:

- **Directorate General for Care Provision (DGOS)**: reports to the French Ministry of Health and plays the role of interface with healthcare institutions. It must notably ensure the quality, continuity, and proximity of care.
- **National Agency for the Safety of Health Products (ANSM)**: responsible for authorising clinical trials, monitoring adverse reactions related to health products, inspecting establishments engaged in certain activities, and authorising health product imports. The ANSM regularly publishes influential guidelines and situational analyses and may impose administrative sanctions.
- **Data Protection Authority (CNIL)**: responsible for ensuring the protection of personal data. Its role is to alert, advise, and inform the public, and it controls and sanctions data controllers and processors through the issuance of injunctions and fines.
- **National Health Authority (HAS)**: notably responsible for the pricing and reimbursement of health products and the optional certification of prescription assistance software. The HAS regularly publishes guidelines, including guidelines relating to digital health issues.
- **Regional Health Agencies (ARS)**: responsible for the regulation of healthcare provisions at a regional level, including implementation of a digital health policy.
- **National Digital Health Agency (ANS)**: responsible for assisting the State in implementing digital health regulation, specifically by issuing recommendations and standards regarding security and interoperability, as well as by developing national health software and projects.

2.5 What are the key areas of enforcement when it comes to digital health?

Some of the key areas of enforcement regarding digital health in France are:

- **Defective MDs**: manufacturers of connected implants and high-risk medical assistance software are exposed to product liability claims.
- **Data Protection**: digital health likely involves the processing of personal health data, considered as highly sensitive. Failure to meet data protection (including security) requirements may therefore result in severe sanctions, such as an injunction to stop the processing or fines of up to 20 million euros or 4% of total worldwide annual turnover, which can be publicly issued.
- **Regulatory Requirements**: existing and future digital health solutions cover an extensive and highly diversified field, and market access may depend on stringent regulatory requirements.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Like other MDs, the software is subject to pre- and post-commercialisation requirements (CE-marking, materiovigilance, etc.) set forth by: (i) the EU, Regulation (EU) 2017/745 on MD (**MDR**) or Regulation (EU) 2017/746 on *in vitro* diagnostic MDs (**IVDR**) (directly enforceable in France and fully operative respectively since May 2021 and May 2022); and (ii) in France specifically, by the FPHC. These regulations broaden the range of technologies covered (e.g. devices aimed at medical prediction and prognosis are now expressly included), set forth a stricter classification regime (a new rule has notably been introduced for stand-alone software MDs, such as most health apps), and added rules on clinical performance evaluation of MDs. It is worth taking note, however, that France has requested postponement of the implementation of these new regulations due to insufficient regulatory capacity and transitional guidance. Regulatory authorities have also issued guidelines tailored to software MDs.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Artificial Intelligence (**AI**) and Machine Learning (**ML**)-powered MDs are subject to MD regulation, data protection regulations (the GDPR and French regime on automated decision-making), and bioethics rules. Other rules may apply as there is no comprehensive regulatory framework. The EU Commission has proposed harmonised rules regarding AI applications (the **AI Act**) which would pre-empt national regulatory frameworks, although monitoring and enforcement would remain the responsibility of Member States. Recently, the EU Commission has also announced the AI Liability Directive aiming at complementing and modernising the EU civil liability framework by introducing specific rules to damages caused by AI systems.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Depending on the digital health product or service, different legal regimes may apply. Health data protection, security requirements, liability issues, and reimbursement of such products or services are also key.
- **Robotics**
  Several potential legal regimes may apply to robotics. Liability allocation is one issue, as well as the consideration of the regime of product responsibility.
- **Wearables**
  The monitoring involved by wearables, specifically when collecting precise and daily information that can reveal health status, requires strict compliance with data protection laws. Depending on the features, MD regulations may also apply.
- **Virtual Assistants (e.g. Alexa)**
  The monitoring involved by virtual assistants, depending on the way they can be activated and how they record information, and the use of AI to train them, requires strict compliance with data protection laws and security requirements and triggers some questions regarding algorithm transparency. Upcoming AI-based regulation should also be closely monitored.
- **Mobile Apps**
  Data protection and security requirements, specifically for health and/or monitoring apps, and the issue of liability, are key. Depending on the features, MD regulations may also apply.
- **Software as a Medical Device**
  MD and health data protection, including additional public health requirements regarding interoperability and security, will apply. Upcoming AI-based regulation should also be closely monitored. Proper liability allocation is key.
- **Clinical Decision Support Software**
  MD regulation will apply. Health data protection, including additional public health requirements regarding interoperability and security, will also apply. Proper liability allocation is key.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Training an AI- or ML-based health solution requires processing large amounts of personal data and health data, triggering compliance requirements with data protection and security, specifically for sensitive data. Algorithm transparency and IT security must be ensured. MD regulations will also apply (see question 2.7).
- **IoT (Internet of Things) and Connected Devices**
  Data protection and security requirements, specifically for health and/or monitoring devices, as well as the issue of liability, are key. Depending on the features, MD regulations may also apply.
- **3D Printing/Bioprinting**
  3D bioprinting means the creation of living tissues via the additive manufacturing technology of 3D printing. MD regulation will likely apply, depending on the intended use.
- **Digital Therapeutics**
  Digital therapeutics are held to the same standards of evidence and regulatory oversight as traditional medical treatments. In addition, data protection and security requirements, as well as the issue of liability, are key.
- **Natural Language Processing**
  Natural language processing is at the crossroads of AI and personal data processing. Algorithm transparency, data protection compliance, and in some cases, medical device regulations, are key. Depending on the support service, the issue of the illegal practice of medicine can be relevant.

3.2 What are the key issues for digital platform providers?

Providers may face specific regulatory constraints depending on the nature of the services offered, but the landscape is evolving rapidly. The landscape is constantly evolving, with, for example, the publication of the Health Insurance Good Practice Charter for Teleconsultation of 6 April 2022, which provides obligations for solution providers and physicians. Discussions for a better supervision of teleconsultation will continue, notably by requiring a healthcare professional to be present during the consultation (other than a doctor) and should be closely monitored. Security and interoperability requirements are higher for digital health platform providers (e.g. if medical data is processed, the platforms may only use the services of a certified health-data-hosting service provider and must comply with security and interoperability standards, especially regarding data access). A certification scheme for interoperability has been considered but not yet implemented.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Personal data is subject to the GDPR and its key principles, mainly lawfulness, fairness, transparency, proportionality, purpose limitation, and data minimisation, and to the French DPA requirements, specifically regarding health data.

4.2 How do such considerations change depending on the nature of the entities involved?

Data protection laws apply regardless of the nature of the entities, whether public or private. However, some entities may be subject to derogations depending on the importance of the data processing operations (e.g. SMEs).

4.3 Which key regulatory requirements apply?

In order to carry out personal data processing, the data controller must implement the following compliance steps:

- maintain a record of processing activities under its responsibility;
- inform the individuals of the processing's existence; and
- ensure that the agreements entered into contain adequate provisions to properly determine the parties' capacities, roles, and responsibilities.

Health data is also subject to the following specific requirements under the GDPR and additional national obligations:

- its processing is, by principle, prohibited, except when based on a specific legal ground;
- its processing must also be justified by a public interest and authorised by the French Data Protection Authority unless it falls under exceptions; and
- organisational and technical security measures must be adapted to the level of data sensitivity.

4.4 Do the regulations define the scope of data use?

The scope of data use is determined, to the extent that the data processing must be lawful, in view of its purpose and conditions of implementation of its operations.

Some specific restrictions do exist such as the prohibition to sell health data that is directly or indirectly identifiable.

4.5 What are the key contractual considerations?

Regarding business-to-business relationships, the requirement to enter into an agreement depends upon the capacities of the stakeholders:

- in a data controller and data processor relationship, an agreement must be entered into, the provisions of which are expressly defined by the GDPR. Security requirements are essential;
- in a joint data controller relationship, an agreement must be entered into, the provisions of which are not specifically defined. However, it is highly recommended to precisely allocate the parties' roles and responsibilities, depending on the actual level of involvement; or
- in an independent controller relationship, an agreement is not required but may be recommended if material personal data exchanges are taking place.

Regarding business-to-consumer relationships, the data controller has an obligation to provide relevant information to the individuals, and, in some cases, to obtain their express consent; failing to do so will make lawful use of the data impossible.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Data is an incredibly important business asset. It is thus highly important to negotiate adequate contractual provisions, in order for the capacities to be in line with the business needs to use data, to properly allocate responsibilities, and to avoid sanctions (see question 4.3).

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

There is no specific regulatory framework under French law; however, regulatory authorities generally address the question through the principle of transparency. While the French Code of relations between the public and the administration (*Code des relations entre le public et l'administration*) specifies the information to be provided by the administration to a person who is the subject of an individual decision taken on the basis of an algorithmic processing, the GDPR provides for the obligation for data controllers to inform data subjects of the existence of automated decision-making and, in particular, to communicate meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing for them.

The prevention of bias and structural discrimination is also at the core of the AI Act, which intends to provide for mandatory requirements applicable to high-risk AI systems in order to serve this purpose.

In September 2022, the French Supreme Administrative Court suggested to designate the CNIL as the authority in charge of the application of the AI Act. It is therefore very likely that the CNIL will pursue and expand its work relating to data inaccuracy, bias, and discrimination in the coming years.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Data protection laws, as well as specific requirements regarding the sharing of medical data, specifically where covered by medical secrecy, are applicable.

5.2 How do such considerations change depending on the nature of the entities involved?

Data protection laws apply regardless of the nature of the entities, whether public or private, except where requirements are specifically applicable to health professionals.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Sharing personal data must always be subject to entering into an agreement (see question 4.5) and to adequate security measures during transmission.

Personal data transfers to recipients located outside the EU, in a country that does not ensure an adequate level of protection, must be covered by appropriate safeguards, notably data transfer agreements (standard contractual clauses (**SCCs**) adopted by the EU Commission).

However, further to the *Schrems II* decision (CJEU, 16 July 2020, C-311/18, *Facebook Ireland and Schrems*), data controllers must conduct a risk assessment before using SCCs and must also implement strong safeguards to ensure the protection of personal data from access by foreign authorities. In France, the French centralised public health database (the **Health Data Hub**) has been subject to various proceedings regarding potential transfers of health data to the US through the hosting service provider. This issue may be impacted by the recent adoption by the US of a Data Privacy Framework (EO 14086, 7 October 2022), which may lead to the adoption of a new adequacy decision for the US facilitating personal data transfer.

If data is covered by medical secrecy, a specific regime for "shared medical secrecy" generally requires patient consent to share its medical data with any party outside the healthcare team.

6 Intellectual Property

6.1 What is the scope of patent protection?

In order to be covered by a patent issued by the French Industrial Property Office (**INPI**), an invention must be new, involve an inventive step, and have an industrial application. In principle, computer programs and mathematical methods are not patentable *per se*. However, a computer program that produces a non-obvious "technical effect" and certain AI-related inventions directed to a technical subject-matter may be patentable. Patents offer strong protection but are limited in scope (to the patent claims) and in duration (20 years). This protection also requires public disclosure of the invention as patent applications are published 18 months after being filed.

6.2 What is the scope of copyright protection?

Copyright protects an original work in a fixed form and excludes ideas, concepts, or mathematical formulas that may not be subject to copyright. A software's architecture, source code, object code, and preparatory design material are eligible for copyright protection, but not the algorithm. The copyright holder benefits from moral rights, which are perpetual, inalienable, and not subject to statutes of limitation, and economic rights which last 70 years after the author's death or after the works' disclosure where it belongs to a legal person. Original works are protected without formalities from their day of creation.

6.3 What is the scope of trade secret protection?

In 2016, the European Commission enacted Directive (EU) No. 2016/943 of 30 July 2018, which protects secret information with commercial value. In France, information protected under trade secrets is defined as any information that is: (i) not generally known or easily reachable by specialists; (ii) of commercial value, actual or potential, because of its secret nature; and (iii) subject to reasonable protective measures by its legitimate holder to keep it secret. Trade secret protection may apply to corporate algorithms.

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

There is no specific academic technology transfer rules scheme in France. Since 2019, France Biotech, an industry association, has been developing tools (negotiation process, templates, access to existing agreements) to facilitate and accelerate technology transfer and, in collaboration with BPI France, has begun to suggest improvements to the technology transfer process. A working group on technology transfer, of which France Biotech's Health Technology Transfer Observatory is a member, is currently being set up.

6.5 What is the scope of intellectual property protection for software as a medical device?

Intellectual property protection for Software as a Medical Device (**SaMD**) will depend on the features and functionality of the product, and the nature of the specific market. A particular SaMD may be protected simultaneously by more than one type of intellectual property protection (patent, copyrights, trade secret, trademarks, design).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

No. The European Patent Office has already refused patent applications designating an AI as the inventor (January 2020).

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Industrial property rights allocation mostly depends on the specific contract executed between the government sponsor and the inventor(s). When the public authority plans to order products that are likely to be protected, particular attention must be paid to the proper management of intellectual property rights in order to ensure that it will be able to use the products ordered in accordance with its needs. In order to help public and private entities in the negotiation and performance of their IP-related agreements, standard intellectual property provisions, adapted to the different public contracts, are made available by the government.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The main consideration is to identify the applicable regulations and define a clear intellectual property scheme regarding the results generated during a partnership, depending on the allocation of responsibility between the parties during development. Academics often request joint ownership of results (independent of inventorship).

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

There are many considerations to assess, including: ensuring business continuity with respect to the product and/or process; warranties on the compliance/regulatory capabilities; cross-border concerns; and data breach indemnity.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

ML is proliferating in the digital health sector to assist HCPs' practice and research. AI can provide assistance in decision-making and make the decision itself, although only under very strict circumstances (notably to protect the subjects' data).

8.2 How is training data licensed?

Training data is protected by intellectual property rights as an entire database if it is original, or, if not, the owner can demonstrate a substantial investment in obtaining, verifying, and presenting data. In this regard, training data can be licensed, subject to compliance with regulatory requirements. Open databases may also be used without the need for a licence.

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

The author of a creation is a natural person and protection automatically arises (see question 6.2). Regarding computer programs, rights may be vested in his or her employer (a company) if the employee acted within his or her duties or pursuant to the employer's instructions. The European Patent Office has already refused patent applications designating AIs as inventors (January 2020).

8.4 What commercial considerations apply to licensing data for use in machine learning?

In addition to securing the necessary rights to use training data, data integrity and reliability are key considerations, as well as obtaining transparency guarantees regarding ML algorithms.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

- **Civil liability**: the producer of the device may be strictly liable for the provision of a defective product in case of harm to the user. Claims may also be brought against economic actors involved in manufacturing or distribution under fault-based regimes.
- **Criminal liability**: manufacturers, distributors, users, and other actors involved in digital health may be liable for specific offences described in the FPHC, or ordinary offences.
- **Regulatory liability**: regulatory authorities may impose administrative sanctions on manufacturers that fail to meet regulatory requirements related to or resulting in adverse outcomes in digital health.

9.2 What cross-border considerations are there?

There are many cross-border considerations likely to impact the business model of industrials engaging in the field of digital health, including:

- **Cross-border healthcare**: Directive 2011/24/EU on patients' rights in cross-border healthcare (as modified) sets out the conditions under which a patient may receive medical care from an HCP located in another EU country – it covers healthcare costs, the prescription, and the delivery of medications and MDs.
- **MDs and local representation**: to place an MD on the EU market, a non-EU manufacturer must designate an "*authorised representative*" in the EU (Art. 11, MDR).
- **Data transfer**: see question 5.3.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The key challenges with Cloud-based services for digital health lie in the setting up of sufficient security and governance mechanisms to enable users to demonstrate compliance with the strictest legal regime applicable to their operations. It is also crucial to ensure data interoperability so that data sharing can be efficient between different healthcare institutions. The impact of the legal restrictions on personal data transfers must also be taken into account for Cloud-based services that are not exclusively hosted within and accessible from the EU (please see question 5.3).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The digital healthcare market is a highly regulated, complex sector to navigate through – solid knowledge of the industry and the norms is key.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

A threshold consideration is whether the digital solution will provide the necessary features, functions, and tools to meet the market needs, as well as comply with the above-mentioned regulatory requirements.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Despite the growing number of digital health technologies, the evolution of methodologies to perform timely, cost-effective, and robust assessments has not kept pace. Key barriers in France include the lack of comprehensive regulation and a sometimes-obscure methodology for reimbursement 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?

The SNITEM (*Syndicat National de l'Industrie des Technologies Médicales*) is the main representative (non-certifying) of the medical technology industry and is proactive in the field of MD regulation.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

They can be reimbursed (by both), although a strict procedure applies. MDs must be CE-marked and any digital health solution must undergo an HAS assessment, be registered on a governmental list, and be prescribed by an HCP to be reimbursed in France.

10.7 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.

Several so-far innovative and marginal practices were rapidly developed under derogatory schemes during the pandemic, and legislators are now slowly selecting the measures they wish to entrench in common law and the ones they either keep derogatory or strike down. In addition, public opinion is having an increased impact on the services offered in the digital health marketplace.

Acknowledgment

The authors would like to acknowledge the fifth author of this chapter: Alice Villagrasa.

Alice Villagrasa focuses her practice on life sciences and corporate advisory matters. Her particular strength is within regulatory matters and she assists French and foreign companies operating in the pharmaceutical, medical device, and cosmetic industries. Prior to joining McDermott, Alice interned at several international pharmaceutical companies.
Tel: +33 1 81 69 99 32
Email: avillagrasa@mwe.com

Anne-France Moreau counsels companies founded on an R&D innovation with a focus on the pharmaceuticals, medical devices, digital health and cosmetic(s) industries. She assists French and non-French groups in the preparation and negotiation of partnering agreements such as collaborations, licences, manufacturing and supply agreements. She also handles regulatory matters in this respect.

McDermott Will & Emery AARPI
23 rue de l'Université
Paris, 75007
France

Tel: +33 1 81 69 15 53
Email: amoreau@mwe.com
URL: www.mwe.com

Lorraine Maisnier-Boché focuses her practice on data protection and information technology (IT) law. She has deep experience in the digital and IT sector as well as the healthcare industry, frequently advising healthcare professionals, hospitals, governmental entities, insurance companies, medical device manufacturers, software editors and hosting service providers on complex IT projects. Lorraine has a strong background in data protection, and regularly advises on GDPR compliance programmes, international data transfers, marketing and profiling actions, sensitive data (e.g. personal health data), audits and security issues.

McDermott Will & Emery AARPI
23 rue de l'Université
Paris, 75007
France

Tel: +33 1 81 69 14 77
Email: lmaisnierboche@mwe.com
URL: www.mwe.com

Caroline Noyrez focuses her practice on transactional and regulatory matters in the fields of pharmaceuticals, medical devices, biotechnologies and cosmetics. She assists French and foreign companies in the life sciences sector in their market access strategies and advises them on the preparation of their strategic contracts.

McDermott Will & Emery AARPI
23 rue de l'Université
Paris, 75007
France

Tel: +33 1 81 69 99 01
Email: cnoyrez@mwe.com
URL: www.mwe.com

Julie Favreau focuses her practice on data protection, cybersecurity and IT law. In particular, she advises clients on compliance with the requirements of EU data protection and privacy legislation. In this regard, she has worked with clients across a broad spectrum of industries, with particular strength in the automotive, health and eCommerce sectors. She holds a Master's degree in e-commerce and digital economy law from Paris I – Panthéon-Sorbonne University and is a recent graduate with an LL.M. from the University of Queensland (Australia).

McDermott Will & Emery AARPI
23 rue de l'Université
Paris, 75007
France

Tel: +33 1 81 69 14 85
Email: jfavreau@mwe.com
URL: www.mwe.com

Germany


Jana Grieb


Dr. Deniz Tschammler


Dr. Claus Färber


Steffen Woitz

McDermott Will & Emery Rechtsanwälte Steuerberater LLP

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 technologies in your jurisdiction?

Prescription and reimbursement of medical apps: A new system for the reimbursement of medical smartphone apps (*Digitale Gesundheitsanwendungen* – "DiGA") has been introduced under the statutory health insurance ("SHI") regime in 2021. The DiGA concept applies to apps that are CE-certified medical devices under the Medical Device Regulation ("MDR") risk class I or IIa. 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 has to 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. These positive effects in patient care have to be established with a comparative study which demonstrates the advantages of using the app, as opposed to not using it. Such study must generally be retrospective. It does not have to be a genuine clinical trial. Valid concepts are epidemiological studies, or studies using methods from other scientific fields such as healthcare research.

At present, BfArM has approved 34 medical apps. The number of reimbursed medical apps will likely increase quickly as the system becomes more established.

Similar to the DiGA concept, a new system for the reimbursement of digital care applications (*Digitale Pflegeanwendungen* – "DiPA") has been 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 had set the legal basis for telemedicine, including video consultation by physicians, and their coverage by private and public payers. The practical implementation of these laws has been accelerated significantly due to the pandemic and related restrictions on public life. The number of video consultations, online prescriptions and other types of remote patient treatment have meanwhile reached an all-time high. Physicians are now also allowed to issue a certificate for sick leave in a video consultation. Simultaneously, restrictions on the advertisement of telemedicine have, to some extent, been lifted.

Regardless of the above, 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 implementation shall be completed in 2023. The ePA is a central element of digital and networked healthcare. Since 2021, patients insured with SHI are entitled to be provided with the benefits of ePA upon request, and all physicians and psychotherapists must have the necessary equipment to transfer data to the ePA. The aim of the ePA is to centrally store patient data in one virtual place if the patient consents and to the extent covered by the patient's consent. Patient data include, *inter alia,* treatment data and vaccination records. As of 2023, the ePA shall also facilitate research and development, i.e. patients shall now be able to make data from their ePA available for research projects on a voluntary basis. The ePA will now also include medication records and data collected through DiGA.

1.3 What are the core legal issues in digital health for your jurisdiction?

Digital health trends are a major challenge for the German health sector, which is still characterised by many traditional rules and practices. The objective of the German government is to provide a functioning and secure healthcare telematics infrastructure that sets a digital framework and facilitates cooperation between various players in the domestic health markets. The telematics infrastructure seeks to achieve a balance between protecting the patients' fundamental rights of autonomy and confidentiality of their health data on the one hand, and creating digital health services and a high level of work efficiency across the health sector on the other hand. One of the key issues of digital health is the handling of sensitive patient data, the extensive use of which has considerable value for research and development, but is at the same time limited by a number of local, national and EU regulations, including the EU Regulation 2016/679 (General Data Protection Regulation – "GDPR").

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

The market for digital products and services in the healthcare sector is growing rapidly. There are various estimates on the market size, depending on the notion of digital health (as outlined under question 1.1 above) and the relevant key figures. The size of the market is already estimated today to be in the tens of billions, with a strong upward trend.

1.5 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 or IBM play a significant role in the digital health market. 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.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Digital health products, including medical apps, often qualify as medical devices or *in vitro* diagnostics and, therefore, fall within the scope of Regulation 2017/745 on medical devices ("MDR") and Regulation 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* – "MPDG").

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 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").

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The laws on data privacy, in particular the 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 products 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 healthcare professionals ("HCP") is subject to various healthcare compliance regulations. Their purpose is to protect independent medical decisions of HCP, patient health and fair competition among healthcare providers. To this end, the regime in particular seeks to prevent any undue influence on HCP. The applicable healthcare compliance provisions are manifold and complex. They equally apply to any cooperation and business activities in the digital health sector.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

While there is no specific national scheme for "consumer healthcare devices", such products are subject to the laws and regulations described above. Under EU law, consumer products are generally subject to the General Product Safety Directive ("GPSD"). In the digital health sector, however, the GPSD is of minor relevance because the more specific medical device regulations, including the MDR, would typically apply instead of GPSD.

With the implementation of the EU directive on digital content in the German Civil Code (*Bürgerliches Gesetzbuch* – "BGB"), the German legislator has reinforced consumer protection in this area. Where digital apps are marketed to consumers, manufacturer obligations under these provisions may even go beyond the general regulatory obligations under the MDR.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

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* – "G-BA") 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") was created specifically with regard to the task of developing a suitable and functioning healthcare telematics infrastructure, including an electronic patient health card, electronic patient files and e-prescriptions.

2.5 What are the key areas of enforcement when it comes to digital health?

Compliance of medical device software ("MDSW") with the sector-specific laws and regulations is mainly supervised by regional market surveillance authorities and notified bodies. This includes regular and *ad hoc* audits. Legal violations by the manufacturer of MDSW may lead to reputational damage and qualify as an administrative or criminal offence. Depending on the circumstances of the individual case, they may result in fines, orders of corrective and preventive measures, or a market ban.

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.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

MDSW must bear a CE-mark in accordance with the MDR or IVDR. For that purpose, these products 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 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. More specifically, they may continue to market their products under the previous MDD regime until 2024 if they have issued a declaration of conformity before the MDR has become applicable.

The Medical Devices Coordination Group ("MDCG") of the European Commission issued several guidelines on qualification and classification of MDSW.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

Germany has not enacted a specific law on AI so far. Products that include AI 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 software has to comply with the requirements of the MDR or IVDR.

The EU Commission published a draft regulation on AI on 21 April 2021. The regulation is expected to come into force no earlier than 2024. As things currently stand, the draft regulation shall not supersede to the EU medical devices regime but apply in parallel. AI systems shall be subject to regulatory requirements that increase with the level of risk associated with them. High-risk AI, including certain AI systems for medical technology, shall be subject to comprehensive legal obligations imposed on the respective operator.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Despite being liberalised to a substantial extent (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 treatment case may not require further medical examination in the doctor's practice. Moreover, telemedicine and virtual care services typically involve the collection and storage of sensitive patient data and, thus, require comprehensive data protection compliance management.
- **Robotics**
  Robotics are machines that have the capacity to (partly) substitute healthcare professionals. Such machines will mostly qualify as medical devices (see question 2.6). Where publicly owned hospitals purchase robotics, the transaction is subject to public procurement laws and a formal tender procedure must be regularly conducted.
- **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. Moreover, it would be challenging for third-party software that runs on these devices and has a medical purpose to meet the reliability standards required for MDSW.
- **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 or IIa may be approved for reimbursement under the German Digital Care Act (*Digitale-Versorgungs-Gesetz*, "DVG") and the German Digital Health Applications Regulation (*Digital-Gesundheitsanwendungen-Verordnung*). They can then be prescribed by physicians and reimbursed by SHI funds, similar to medical aids.
- **Software as a Medical Device**
  As with mobile apps, other software that implement health-related features may equally qualify as MDSW (see above).
- **AI/ML powered digital health solutions**
  Digital health solutions powered by AI and machine learning can be a powerful tool for medical diagnostics and monitoring.
  The training of neural networks and similar AI/machine learning 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 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. The processing of personal

health data needs to comply with the GDPR. This usually means that the processing will be a service provided on behalf of a healthcare provider.

- **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).
- **Natural Language Processing**
  Natural Language Processing ("NLP") describes techniques and methods for automatic analysis and representation of human speech. The purpose of NLP is direct communication between humans and computers based on natural language (see question 8.1). NLP may be one phase of text and data mining ("TMT"), the purpose of which is to detect new correlations in databases by means of algorithms. NLP is, *inter alia*, used in pharmaceutical research.

3.2 What are the key issues for digital platform providers?

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. 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. Consequently, they will often need to obtain valid consent from end-users in order to perform their services.

As platforms handle health data, they are also subject to increased data security requirements. They may not rely on email, which is often unencrypted, but need to establish a more secure channel for communicating with patients instead.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The use of personal data is governed by the GDPR. Such data must be processed lawfully (i.e. on a legal basis), transparently and fairly. They must be collected for a specific purpose (purpose limitation), limited to what is necessary (data minimisation), be accurate, be kept only as long as necessary (storage limitation) and finally be kept securely (integrity and confidentiality) (Article 5(1) of the GDPR). Health data is 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 healthcare professionals and their auxiliaries is subject to criminal liability under Sections 203 and 204 of the German Criminal Code (*Strafgesetzbuch* – "StGB").

For connected medical devices and other equipment, the Telecommunication-Telemedia Data Protection Act (*Telekommunikation-Telemedien-Datenschutzgesetz* – "TTDSG"), 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 upcoming EU Data Act (Proposal for a Regulation on harmonised rules on fair access to and use of data, procedure file 2022/0047(COD)) would also cover digital health products and services, and require the vendors to make available both personal data and non-personal data to the user and third parties requested by the user.

4.2 How do such considerations change depending on the nature of the entities 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 healthcare professionals 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 healthcare professionals 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.

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 need to 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.

4.3 Which key regulatory requirements apply?

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 needs to:

- 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 which 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 health providers in Germany will usually require a DPO.

Healthcare professionals 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.

4.4 Do the regulations define the scope of 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.

For health data in particular, the exceptions from the ban on the processing of special categories of data only apply to certain purposes. By way of example, healthcare professionals can use health data for the provision of medical services and related administrative purposes. However, if they exceed this scope – e.g., if they want to anonymise data to share it with the vendor of their equipment – they will need to look at a different exception. This often means that they need to obtain consent from their patients.

4.5 What are the key contractual considerations?

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 on 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 proposed EU Data Act, providers would also be required to inform the users about the non-personal data generated by a product or service before entering into a contract.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

German law does not generally provide for ownership in data as intellectual property or otherwise. Data can only be protected as part of a database under the *sui generis* database protection rights set out in Sections 87a *et seq.* of the German Copyright Act (*Urheberrechtsgesetz* – "UrhG"), which transposes Directive 96/9/EC. This protection, however, only comes into play if there was a substantial investment specifically in the acquisition, verification or presentation of the contents of such database. Efforts undertaken to collect data for other commercial purposes, such as providing healthcare services or developing medical software, are not specific to the creation of the database and will thus not be considered. In addition, the proposed EU Data Act would clarify that databases containing data obtained from or generated by the users would not be eligible for protection. Such measures could also apply when data is shared in accordance with the proposed EU Data Act.

Failing a protection as a database, data can only be partially protected as a trade secret under the German Trade Secret Act (*Geschäftsgeheimnisgesetz* – "GeschGehG"), which transposes Directive (EU) 2016/943. For this protection to apply, adequate measures against unauthorised access must be taken, e.g., including non-disclosure agreements with any person with whom the data is shared. Such measures could also apply when data is shared in accordance with the proposed EU Data Act.

Often, the ownership of the data is overshadowed by the rights of the patient or other data subjects under the GDPR. If the collection or processing of personal data is based on consent (as opposed to, e.g., the research exemption), this consent can be revoked at any time, and the data subsequently needs to be deleted. This usually means that data ownership is not the primary concern, provided that data is not aggregated or otherwise anonymised.

4.7 How are issues with 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.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Under the GDPR, there must be a legal basis for sharing personal data. In digital health markets, this often means that the healthcare professional collecting health and other personal data for purposes of diagnosis and treatment needs to 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, in particular, a recent decision of the Court of Justice of the EU (16 July 2020, C-311/18 – Schrems II) indicates that such contractual undertakings would not be effective and need to be supplemented with additional measures. The EU and the United States have agreed on a new Data Privacy Framework that would make these considerations obsolete when the recipient participates in the framework. 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 do such considerations change depending on the nature of the entities 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 healthcare professionals for the purposes of diagnosis or treatment is usually covered by an exception 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 exception. However, professional secrecy must be taken into account, and it must be ensured patients' secrets will only be shared with other persons subject to professional secrecy or written confidentiality undertakings.

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) may be subject to additional restrictions from state data protection laws and governmental policies when sharing health data.

5.3 Which key regulatory requirements apply when it comes to sharing data?

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 needs to apply. In many cases, this requires obtaining the patient's or data subject's consent. For this consent to be valid, the data subject needs to 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.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patent protection 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. In digital health markets, the core technology (e.g., sensors and hardware) is generally patentable, even if patents remain mostly used in this rapidly developing environment. The number of worldwide Internet of Things ("IoT") patent applications increased substantially to over 130,000 per year; the health sector is contributing significantly to this development.

6.2 What is the scope of copyright protection?

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 take the form of a computer program, e.g., a statement, program language or mathematical algorithm, provided that 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 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 What is the scope of trade secret protection?

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. In order to actually maintain secrecy, companies must – in accordance with the new GeschGehG – implement a confidentiality program 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 academic technology transfers in your jurisdiction?

Academic technology transfer from university employees to their university employer is subject to certain employee privileges under the German law on employee inventions because of the freedom of teaching and research. As opposed to other 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 claims a service invention which 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 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 What is 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, programs that immediately trigger a technical effect or directly optimise data-processing hardware are considered patentable. The same rules apply to copyright, 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?

So far, an AI device has not been named as the inventor of a patent in Germany. Several applications for the registration of patents "invented" by an AI device have already been rejected in Germany.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

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* – "BMBF") for Research and Development Projects ("NKBF 98"), e.g., require that the results be made available to research and teaching in Germany 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 (TFEU) and the corresponding EU Commission Communication on Research, Development and Innovation (2014/C 198/10). Under these rules, any transfer of funded inventions to commercial undertakings must be remunerated at the market price.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Collaborations in the digital health sector are mostly subject to extensive contractual agreements, that aim at a fair balance of IP rights allocation and commercialisation rights on the one hand, and regulatory responsibilities and product liability on the other hand.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

When cooperating with healthcare companies or healthcare professionals, non-healthcare companies should avoid granting any benefits, both unilaterally (e.g., gifts) and as part of (bilateral or multilateral) cooperation agreements. In such agreements, therefore, services and consideration must be equivalent, i.e. any remuneration must be at arm's length (principle of equivalence).

When granting benefits, companies should avoid the impression that there are any commercial expectations associated with such benefits. In particular, benefits must not create an incentive for the healthcare company or healthcare professional to make a certain procurement or therapy decision. In other words, if companies grant any benefits, this should be for legitimate objective reasons and kept separate from other businesses or commercial interests (principle of separation).

In the event of a cooperation with healthcare companies or healthcare professionals, any details of such cooperation should be agreed upon in written form and as transparently as possible. In particular, companies should avoid any (additional) verbal agreements or other non-transparent arrangements as these give the impression of secrecy (principles of transparency and documentation).

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning usually refers to the use of an algorithm ("neural network") that is trained with representative input data (e.g., images or sensor information) and the desired output. The algorithm is thus trained to recognise patterns in input data and to produce a certain output.

Machine learning can be a powerful tool for diagnostic purposes to assist healthcare professionals and to monitor the success of patient treatment. It can also be used for the early detection of potential health issues, even in consumer devices such as smartwatches or smartphones.

8.2 How is training data licensed?

Training data is often protected under the *sui generis* database protection rights set out in Sections 87a *et seq.* of the UrhG, which transposes Directive 96/9/EC on the legal protection of databases. In this case, it can be licensed in the same manner as other intellectual property.

Licensing training data will often be challenging, as it includes personal health data, which is under strict protection under the GDPR regime. Consequently, training data can often be licensed in anonymised form only. One of the main considerations is how to ensure that it will not be possible to re-identify individuals.

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

As a general rule, intellectual property can only be produced and owned by human beings, not by machines. For this reason, improvements made without active human involvement do not fall under the protection of most intellectual property rights.

In some cases, the results may be protected by *sui generis* database protection rights (see question 8.2 above). Unlike other types of intellectual property, this protection only requires a substantial investment, but not necessarily an intellectual achievement.

Furthermore, the improvements might be protected as trade secrets of the entity that made them.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The main consideration is the ownership and/or access to the results of the training, i.e. the trained algorithm. As the algorithm may often not be protected by intellectual property rights (see question 8.3), it is crucial to clearly define the rights and obligations of each party with respect to its further use in the commercial agreement.

As training data will often include personal health information, it is also important to agree on liability and indemnification provisions in case the use of the licensed data turns out to be a violation of the GDPR. This could, e.g., be the case if the consent given by the patients is invalid or if the data has not been properly anonymised.

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 BGB, as well as product liability under the Product Liability Act (*Produkthaftungsgesetz* – "ProdHG") that each cannot be restricted by a contract on the other hand. MDSW is subject to liability under the ProdHG, even if not offered in a material object as data carrier.

9.2 What cross-border considerations are there?

Liability rules are predominantly subject to Member State law. With regard to cross-border matters, the EU Regulation 593/2008

("Rome I Regulation") and the EU Regulation 864/2007 ("Rome II Regulation") regulate the applicable national legislation. Under Art. 4 of the Rome II Regulation, applicable law is determined on the basis of where the damage has occurred, irrespective of the country in which the act that has caused the damage took place. There are two general exemptions from this rule: (i) if the parties reside in the same country, the law of that country shall apply; or (ii) if a tort is apparently more closely connected to a country other than where the damage occurred or where both parties live – in that case, the law of that other country is applicable. Furthermore, exemptions apply with regard to certain types of liability. For product liability, specific rules apply according to Art. 5 of the Rome II Regulation. Here, the place where the product was acquired can become decisive. Under the Rome I Regulation, parties are, under certain conditions, allowed to determine the applicable law by contract. In the absence of a contractual choice of law, with regard to services, the law of the service provider's residence is applicable. However, there are exemptions to this rule with regard to consumer contracts, where generally the law of the consumer's country of residence is applicable.

Given that cross-border liability cases can result in severe legal consequences and significant loss of reputation in all countries concerned, cross-border digital health companies should adopt a global compliance regime and establish an organisation that takes into account the specific legal requirements and pitfalls of each national legal system concerned.

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* – "GIGV") 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 with regard to physician practices and medical care centres (*Medizinische Versorgungszentren* – "MVZ"). As hospitals are entitled to hold MVZ, this is an option for corporate entities to indirectly operate MVZ and thereby employ physicians.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barriers include high-market entry, reimbursement and compliance requirements. The market entry of MDSW is largely restricted by certification procedures under the new MDR and IVDR regimes that often require the involvement of notified bodies. However, as the new regulations maintain the general certification system and do not introduce a genuine approval requirement for MDSW (unlike for drugs), they are still regarded as an efficient market-clearance system. 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 healthcare professionals. 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.

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 German Physicians' Chamber (*Bundesärztekammer* – "BÄK") supervises all physicians practising in Germany. The Panel Doctors' Associations (*Kassenärztliche Vereinigungen* – "KV") 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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.

With some delay, the electronic prescription ("e-prescription") is now being introduced in Germany. Since September 2022, pharmacies must be able to process e-prescriptions. From January 2023, the use of e-prescription shall be mandatory for physicians. Patients can decide to manage their e-prescription via smartphone using a secure e-prescription app and send it digitally to the pharmacy of their choice, or request a hardcopy of the access data required to redeem their e-prescription at the doctor's office.

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.

To strengthen cross-border patient safety, the national e-health contact point is to be established by mid-2023, in order to facilitate availability of social insurance data to physicians in other EU countries.

Acknowledgment

The authors would like to thank Dr. Katharina Hoffmeister for her contribution to the preparation of this chapter. Katharina focuses her practice on healthcare and life sciences with a focus on the pharmaceutical industry and industry-specific data protection and compliance issues in the healthcare market.

Jana Grieb, Counsel, 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 & Emery Rechtsanwälte Steuerberater LLP
Oberlindau 54-56
60323 Frankfurt/Main
Germany

Tel: +49 69 951145 252
Email: jgrieb@mwe.com
URL: www.mwe.com

Dr. Deniz Tschammler, Partner, based in Frankfurt, counsels pharmaceutical companies, manufacturers of medical devices and *in vitro* diagnostics, providers of healthcare platforms as well as their investors in complex sector-specific projects. He advises his clients on the various regulatory challenges of the German and European health market, transactions and strategic collaborations, disputes in competition and with authorities, market entry and reimbursement pathways, data protection and the establishment of compliance organisations.

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Oberlindau 54-56
60323 Frankfurt/Main
Germany

Tel: +49 69 951145 029
Email: dtschammler@mwe.com
URL: www.mwe.com

Dr. Claus Färber, Counsel, based in Munich, represents clients on 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 communications (M2M).

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 151
Email: cfaerber@mwe.com
URL: www.mwe.com

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 & Emery Rechtsanwälte Steuerberater LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 181
Email: swoitz@mwe.com
URL: www.mwe.com

India

Manisha Singh

Pankaj Musyuni

LexOrbis

1 Digital Health

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

Digital health is a broad term, referring to providing a connecting link between digital technologies and the healthcare sector with the aim of improving healthcare efficiency and providing more personalised care to patients. Though the terms "digital health", "digital medicine", and "digital therapeutics" are not expressly defined in India, the Digital Information Security in Healthcare Act of 2018 (the DISHA) explains "digital health data" as providing an electronic record of an individual's health-related information. Usually, the said data refers to: the requisite details of an individual's physical and mental health condition; health services provided to the individual; the donation of any body part or bodily substance by the individual; and testing and examination data. Notably, the Telemedicine Practice Guidelines (TPG), issued by the Indian government earlier in March 2020, aim to regularise the practice of telemedicine. These guidelines concur with the definition provided by the World Health Organization (WHO), which defines telemedicine as "the delivery of healthcare services by all healthcare professionals using information and communication technologies when distance is a critical factor". Using information and communication technology (ICT) in healthcare, numerous tools and services are employed to prevent, minimise, treat, and monitor disease patterns. The application of genetics and digital technologies for early disease detection and timely management exemplifies the concept of digital health. The Ministry of Health and Family Welfare (MoHFW), of the Indian government, is in charge of this industry.

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

Some of the key emerging technologies in India's digital healthcare system are as follows: digital diagnostic tools, such as wearables; distance monitoring software and hardware and remote tracing diagnostic tools; telemedicine; mobile health; machine learning; medical imaging; big data; the Internet of Medical Things (IoMT); robot-assisted surgery; self-monitoring healthcare devices; electronic health records (EHRs); targeted advertising; personal genomics; personalised or precision medicine; biomarker tools; e-pharmacies; Cloud computing; Artificial Intelligence (AI); and augmented- and virtual-reality solutions.

1.3 What are the core legal issues in digital health for your jurisdiction?

Data security is vital for safeguarding the confidentiality of health-related information communicated between patients and healthcare providers, as well as recommendations and outcomes. The Information Technology Act of 2000 (IT Act), the Data Protection Rules of 2011, and the Intermediaries Guidelines of 2011 are designed to refer to these in all circumstances and to meet this demand; however, no standards have been developed to mandate the implementation of data protection and security due to their stringent compliance. In addition, as the number of digital and other innovative healthcare technologies increases, so do concerns about patient privacy and data security. There are substantial concerns over data abuse and privacy duties, despite the fact that the bulk of healthcare providers' data collection, storage, and use would comply with India's present data privacy legislation. The absence of proper education and training for staff responsible for collecting, processing, and handling patient data on the digital health platform also contributes to the current situation. The Personal Data Protection Bill was tabled in the Lok Sabha on December 11, 2019. The bill created the Data Protection Authority, whose objective is to safeguard individuals' personal data. In addition, the lack of a comparable law is a key source of concern. On August 4, 2022, the Indian government withdrew the Personal Data Protection (PDP) Bill, 2019, from Parliament. According to the administration, the new law will likely be one of four new laws tackling social media, digital technology, telecommunications, and privacy. In place of a comprehensive law, the government intends to establish specialised statutes for specific facets of the digital technology industry. In addition, a new act that is part of a "comprehensive legal framework" would replace the PDP statute. The DISHA has not yet become law. The DISHA will establish national and state health authorities in an effort to prevent the disclosure of health-related information to third parties. The MoHFW has also made a National Digital Health Mission-Related Health Data Management Policy to protect the privacy of people's digital health data.

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

A significant growth in India's digital adoption has been observed due to growth of the digital healthcare market and supportive government policies. Considering revenue, the digital healthcare

market in India has been valued at over USD 195 billion in 2021 and is expected to grow at a compound annual growth rate (CAGR) of more than 16% from 2022 to 2030, as predicted by Global Market Insights, a market research and consulting firm.

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

Novartis, Stryker, Edwards Lifesciences, Centura Health, and Hologic are among the top five largest digital healthcare technology companies. PharmEasy, cult.fit, Innovaccer, Tata Digital Health, and Practo are more promising digital health start-ups in India.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

In India, digital health is governed by a few laws, guidelines, and standards. Several regulations apply universally to digital health technology, despite the fact that each digital health tool or business model is independently governed. Relevant legislation includes the IT Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules of 2011 (SPDI Rules), and the Information Technology (Intermediaries Guidelines) Rules of 2011 (Intermediaries Guidelines). The IT Act, SPDI Rules, and Intermediary Guidelines comprise India's general data protection framework. Online transactions and the transfer of electronic data are now permitted owing to the better security provisions of the IT Act. The IT Act governs a vast array of online activities, including the authentication of digital signatures and the legal standing of electronic records. The IT Act addresses various types of cybercrime, including hacking and denial-of-service attacks.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

India's current legal framework for e-health protection is governed by the IT Act and the SPDI Rules, which provide some protection for the collection, disclosure, and transfer of sensitive personal data such as medical records and histories. In contrast, legislation has lagged behind technological advances and failed to address a number of crucial issues. Thus, medical institutions and healthcare providers in India are increasingly storing patient data in electronic medical records (EMRs) and EHRs. According to the Clinical Establishments (Registration and Regulation) Act of 2010, each clinical institution is required to maintain an EMR for each patient, whose registration must be maintained. The MoHFW put out the EHR Standards for the first time in 2013. In December 2016, they were updated and made public.

The EHR Standards are a set of global standards that can be used by healthcare providers to create and manage EHRs. Some of the key ongoing digital health initiatives being implemented by the MoHFW include: Reproductive Child Healthcare (RCH); Integrated Disease Surveillance Program (IDSP); Integrated Health Information System (IHIS); e-Hospital; e-Sushrut; Electronic Vaccine Intelligence Network (eVIN); Central Government Health Scheme (CGHS); Integrated Health Information Platform (IHIP); National Health Portal (NHP); National Identification Number (NIN); and Online Registration System.

These programmes are well established in the medical field and continue to generate vast quantities of data that can be utilised for the public's benefit. As health is a state responsibility, the National Health Mission (NHM) subsidises states for connected services such as telemedicine, teleradiology, teleoncology, tele-ophthalmology, and hospital information systems.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The Designs Act of 2000 usually protects consumer devices. Only characteristics of shapes, configurations, patterns, ornaments, or the composition of lines or colours that are applied to an "article" are considered "designs". The graphic user interface (GUI) of applications and the design of the devices are the two major aspects of digital health that require design protection. A GUI may be protected by the Designs Act, specifically Article 14-04 of the Design Rules, 2001, which covers "Screen Displays and Icons". In addition, the Central Drugs Standard Control Organisation (CDSCO) has published a draft list of risk classifications for medical devices governed by the New Definition Notification. The risk-classification list classifies medical devices into 24 broad categories (as defined by international classification standards), with separate classifications for standalone software.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The CDSCO is the primary regulatory body responsible for enforcing the "Drugs and Cosmetics Act, 1940" and "Rules made thereunder". Additionally, the Medical Council of India regulates medical practice. Moreover, the Office of the Controller General of Patents, Designs, and Trademarks (CGPDTM) is in charge of intellectual property protection, while the Copyright Office is in charge of copyright. Both are divisions of the Department for Promotion of Industry and Internal Trade (DPIIT). The Indian Council of Medical Research (ICMR) has also done a lot to promote research in support of the National Digital Health Blueprint (NDHB) from the MoHFW.

Typically, the following significant acts govern the legal and regulatory framework:

- The IT Act, the SPDI Rules, and the Information Technology Rules of 2011 are all included in the IT Act.
- The New Telecom Policy of 1999 Requirements for Other Service Providers.
- The Drugs and Cosmetics Act of 1940 and the Drugs and Cosmetics Rules of 1945.
- The Indian Medical Council is run by the Indian Medical Council Act of 1956 and the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations of 2002.
- The Drugs and Magic Remedies Act of 1954 and the Drugs and Magic Remedies Rules of 1955 regulate the use of drugs and magic remedies.
- Commercial Communication Customer Preference Regulations of 2010 and Unsolicited Commercial Communications Regulations of 2007.
- The Clinical Establishments Act of 2010.

2.5 What are the key areas of enforcement when it comes to digital health?

The enforcement of standards that maintain the security, confidentiality, and privacy of patients' health and medical records is crucial. Due to the fact that private health information and records are kept under lock and key and are only used for data interpretation for market analysis, marketing, and regulatory sharing, it is very important to keep track of data protection and violations.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

The CDSCO, a division of the Directorate General of Health Services (MoHFW), is India's primary regulatory body for medical devices and diagnostics. The head of the CDSCO is the Drug Controller General of India (DCGI). The DCGI oversees the approval of certain drugs (vaccines, large-volume parenterals, blood products, and r-DNA-derived products), medical devices, and new drugs. In India, the Drugs and Cosmetics Act and Rules (DCA) govern the production, importation, sale, and distribution of medical devices.

Only the following notified medical devices are currently regulated as "drugs" in India under the Drugs and Cosmetics Act 1940 and Rules thereunder:

(i) substances used for *in vitro* diagnosis and surgical dressings, surgical bandages, surgical staples, surgical sutures, ligatures, blood, and blood-component collection bags with or without anticoagulant; and

(ii) substances, including mechanical contraceptives (condoms, intrauterine devices, tubal rings).

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

There are currently no formal regulations.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - A. Adoption of technology.
  - B. Evidence.
  - C. Technical training.
  - D. Record keeping and data management.
- **Robotics**
  - A. Energy storage.
  - B. Ethics and security.
- **Wearables**
  - A. Cost of device.
  - B. Battery life.
  - C. Safety, security, and privacy.
- **Virtual Assistants (e.g. Alexa)**
  - A. Lack of accuracy.
  - B. Lack of analytical interpretation.
- **Mobile Apps**
  - A. Competitive market.
  - B. Promotion and marketing.
  - C. Data management and privacy.
- **Software as a Medical Device**
  - A. Software development lifecycle.
  - B. Product safety and security.
  - C. Data collection, analysis, and privacy.
- **Clinical Decision Support Software**
  - A. Development lifecycle.
  - B. Product safety and accuracy.
  - C. Data analysis.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  - A. Lack of precision.
  - B. Lack of interpretation.
  - C. Irregularity in analytics.
  - D. Reliance.
  - E. Transparency and governance.
  - F. Long-term cost.
- **IoT (Internet of Things) and Connected Devices**
  - A. Compatibility of operating systems.
  - B. Identification and authentication of devices and technologies.
  - C. Integration of Internet of Things (IoT) products and platforms.
  - D. Connectivity.
  - E. Data analytics, security, and privacy.
  - F. Consumer awareness.
- **3D Printing/Bioprinting**
  - A. Piracy.
  - B. Misinterpretation of results.
  - C. Lack of training skills.
- **Digital Therapeutics**
  - A. Lack of accuracy.
  - B. Lack of interpretation and understanding.
- **Natural Language Processing**
  - A. Understanding of natural language.
  - B. Reasoning about multiple documents.
  - C. Identification of data and evaluation of problems.

3.2 What are the key issues for digital platform providers?

Providers of digital platforms are typically preoccupied with comprehending and managing the transitional phase of implementing new technologies. Therefore, some of the most important things for digital platform providers are to replace and improve their IT systems, train their employees, understand the importance of market demand and in-line supply, and have good leadership.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Regarding the use and implementation of personal data, data privacy is of paramount importance. In 2013, India's first EHR Standards were proposed. In consideration of their applicability in India, they were chosen from the best available, previously implemented international EHR standards. As a result, the 2016 EHR Standards document was alerted and made available in national IT systems for adoption by healthcare institutions and providers. The MoHFW aided in its adoption by making standards like the Systematized Nomenclature of Medicine Clinical Terminology (SNOMED CT) free to use in India and by appointing an interim National Release Centre to manage the

clinical terminology standard, which is gaining global acceptance among healthcare IT stakeholder communities. The MoHFW has also proposed a new bill, the DISHA, to regulate data security in the healthcare industry. This Act is intended to protect the privacy, confidentiality, security, and standardisation of EHRs. The MoHFW plans to establish the DISHA in order to promote and adopt e-health standards, enforce privacy and security measures for electronic health data, and regulate the storage and exchange of EHRs.

4.2 How do such considerations change depending on the nature of the entities involved?

Hospitals, research organisations, and technological service providers are among the entities participating in data collection, record keeping, and information exchange. In addition, these procedures can be modified in response to ongoing experiences and problems encountered during the transition, lag phase, and linking of the consumer and service provider.

4.3 Which key regulatory requirements apply?

The MoHFW plans to establish a national digital health authority as a statutory body to promote and adopt e-health standards, enforce privacy and security measures for electronic health data, and regulate the storage and exchange of EHRs. The proposed National eHealth Authority (NeHA) under the MoHFW will also oversee the development of an integrated health information system in India. It is proposed that it will serve as a promotional, regulatory, and standard-setting body to guide and support India's digital health journey and the subsequent realisation of ICT's benefits in the health sector. It also describes the intended functions and governance structure of the NeHA. The DISHA aims to formally establish the NeHA and promote the online exchange of patient data to prevent duplication of efforts and resources.

4.4 Do the regulations define the scope of data use?

Yes, the regulations define the scope of information use with beneficiary and service provider permission, as well as the "sensitive health-related information" and "sensitive personal information" criteria.

4.5 What are the key contractual considerations?

Contracts are the best way to make sure that the different parts of the investigation, from data collection to data use, are kept private and confidential. For example, employees and other influencers who take part in the research should sign non-disclosure and personal privacy agreements, and there should be more options for when pre-defined contractual conditions are broken.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Sampling with intent and data confidentiality are major concerns, and the absence of clearly defined legal remedies presents obstacles. There is a very important need and requirement to protect and secure full rights so that people can get better care and a better healthcare system based on evidence.

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

A comprehensive legislative framework governing the collection and dissemination of personal data, as well as concerns regarding data inaccuracy, bias, and/or discrimination, is urgently required. There are no comprehensive regulations governing the processing of non-sensitive personal data or information.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

When sharing personal data, some of the most important things to think about are flexibility and those things related to data collection and transfer, security, and privacy during the transformation process, and information sharing, trust, responsibility, and accountability.

5.2 How do such considerations change depending on the nature of the entities involved?

Such considerations are crucial and heavily dependent on the total number of participants and scientific entities. Also, the goal of using data protection and privacy to get results quickly may affect data sharing, which is an important factor that all parties involved should evaluate at each step of the process.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The MoHFW created the DISHA proposal with the intention of protecting healthcare data in India and giving consumers complete control over their health data. For instance, if a patient visits the doctor for a check-up and the doctor looks up the patient's previous medical history and enters the current diagnostic results into an EHR, the DISHA ensures that the information is secure as it moves throughout the healthcare system. The DISHA outlines three primary objectives for data protection: establishing a national and state digital health authority; enforcing privacy and security measures for electronic health data; and regulating the storage and exchange of electronic health information. In addition, the proposal calls for the establishment of national and state electronic health authorities (NeHA and SeHA) to provide Indian citizens with comprehensive data protection and healthcare management, as well as to ensure and monitor data portability.

6 Intellectual Property

6.1 What is the scope of patent protection?

The Patents Act of 1970, which provides patent protection and is consistent with the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), has been adopted and implemented by India. In addition to meeting the patentability requirements of novelty, inventive step, and industrial applicability, to obtain patent protection in India, the invention must fall outside the scope of Sections 3 and 4 of the Act. Section 3(k) of the Patents Act, which prohibits the patentability of a computer programme by itself, is applicable because digital

health applications rely on software and a computer programme. In addition, the Delhi High Court clarified that not all computer programmes are exempt from Section 3(k) and that the invention is patentable if the computer programme demonstrates a "technical effect" or "technical contribution".

According to Section 3(i) of the Patents Act, a patent cannot be granted if the programme or method relates to "a process for the medicinal, surgical, curative, prophylactic, or other treatment of human beings or any process for a similar treatment of animals to render them disease-free or to increase their economic value or that of their products". In contrast, the apparatus and method for using an *in vitro* mechanism are patentable.

6.2 What is the scope of copyright protection?

The Copyright Act of 1957 protects intellectual property in India. Copyrights can protect original literary, dramatic, musical, or aesthetic works, cinematograph films, and sound recordings. Although registration of copyright is not required, it serves as *prima facie* evidence in establishing the legal claim. Because digital health applications are essentially software, they fall under the definition of "computer programme" and are therefore protected by copyright laws.

6.3 What is the scope of trade secret protection?

There is no specific law in India that governs the handling of confidential information and trade secrets. In the new digital health industry, however, non-disclosure and confidentiality agreements are usually used to protect this kind of sensitive information.

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

The idea of academic technology transfer is in its infancy in India. Despite the fact that universities and some businesses have embraced this concept and developed rules for strategically deploying innovations and rewarding inventors, the majority of organisations have not. In addition, intellectual property protection in the digital health industry is still in its infancy; however, it is growing exponentially, and academic and research institutions are becoming increasingly aware of the importance of protecting and disseminating their knowledge through technology transfer. This trend appears to be gaining momentum and producing better results. Typical rules and activities for academic technology transfer include, but are not limited to, the following steps: evaluating and assessing the proposed invention in terms of patentability and commercialisation; protecting intellectual property in different areas related to the technology in question; and searching for and finding the best partner for licensing and monetising the proposed technology and how the invention works.

6.5 What is the scope of intellectual property protection for software as a medical device?

Section 3(k) of the Patents Act prohibits the patentability of computer programs in general. The Delhi High Court has clarified that Section 3(k) does not apply to all computer programs and that such programs can be patented if they demonstrate a "technical effect" or "technical contribution". A patent cannot be granted under Section 3(i) of the Patents Act if the program or process relates to "a process for the medicinal, surgical, curative, prophylactic, or other treatment of human beings or any process for a similar treatment of animals to render them disease-free or to increase their economic value or that of their products". The *in vitro* mechanism's apparatus and method of use are patentable.

As digital health applications are fundamentally software, they should be classified as "computer programs" and granted copyright protection under Indian law. A trademark can also be registered in class 9, which includes computer software and computer programs.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

In India, an AI device cannot be listed as the inventor of a patent.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

There are currently no specific regulations for government-funded inventions.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

To make sure collaborative improvements work, a number of things can be considered, such as the collaboration's main goals, information about all eligible members and parties involved, management of governance and contract management, confidentiality and evaluation of existing intellectual property and technology transfer procedures, and information on existing intelligence.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

In terms of internal communications and providing services externally, the working concepts and work-flow procedures of healthcare and non-healthcare organisations are vastly different; however, customer satisfaction is the top priority for both sectors. When evaluating agreements, approaches to information sharing must be evaluated in addition to the confidentiality protocol for data exchange, data protection, security, and privacy.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

The key roles of machine learning in digital health include: facilitating the use of numerous methods and processes to reduce cost, time, and effort; facilitating disease identification and early detection; assisting with drug development and production; examining behaviour modifications based on machine learning; keeping and securing medical records; outbreak prediction; and clinical experimentation, data collection, and data mining.

8.2 How is training data licensed?

In the absence of specific regulations governing AI, Cloud computing, and machine learning in India, activities utilising these technologies must adhere to standard IT laws and regulations. A confidentiality agreement between the licensee and the owner of the data, as well as a plan for how the data will be used, would be helpful.

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

This is presently not applicable in India. In addition, algorithms are not patentable in India.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Important factors to consider include the authenticity of licensed data, permission for multiple users and beneficiaries, consideration for purposes such as "know your customer", restriction and limited access across multiple locations and multiple users, data privacy and security, quality, using rights, term, and termination.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Liabilities for adverse outcomes may be civil or criminal, and they vary between service practitioners and service providers, such as institutes and internet service providers. In addition to filing a civil complaint, the remedies provided by the Consumer Protection Act may be used in civil proceedings. In the event of a doctor's negligence, a customer may also file a complaint with the Medical Council of India's ethical committee. The Indian Penal Code also talks about criminal responsibility, which is important for digital health solutions.

9.2 What cross-border considerations are there?

Utilising data applications and localising data are of the utmost importance.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

A constant concern in digital health is the high cost of establishing and maintaining health information technology, as well as storing data while protecting confidentiality and privacy. Another important thing to consider is the security and privacy of data management at different stages of transformation.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Non-healthcare businesses must recognise that the healthcare industry adheres to stringent manufacturing and marketing requirements, as well as sound business planning and data privacy and security practices. Moreover, consumer protection regulations apply to the healthcare sector.

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 consider a number of key factors before investing in digital healthcare businesses. These include a good business plan, market opportunities, strategic partnerships, an understanding of the business's financial and key matrices, the business's potential risk, the expected valuation, regulatory compliances, and protection of intellectual property.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The primary barriers to the widespread adoption of digital health technologies in clinical settings are data interoperability, particularly health records, data security, and privacy.

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?

Currently, there are no such certifying bodies.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

There are currently no explicit reimbursement standards or formal accreditation for solution providers.

10.7 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 recent years, India's digital healthcare has become increasingly focused on innovation and technology. The Indian government announced in its Union Budget for 2022 the release of an open platform for the National Digital Health Ecosystem, which will include digital healthcare provider registries and access to health facilities. The Indian government has also announced that the National Telehealth Programme will be launched in 2022, granting individuals of all ages access to high-quality mental health counselling and care services. It is anticipated that the programme will establish 23 telehealth mental health centres in India. Eighty per cent of healthcare systems plan to increase their investment in digital healthcare tools over the next five years. India's innovators are developing cutting-edge health-tech products and solutions. These digital health innovations are being implemented through the Ayushman Bharat Digital Mission (ABDM). Recent implementation of the ABDM bolsters India's efforts to digitalise healthcare.

Also introduced in 2022 was the Unified Health Interface, a digital healthcare platform that connects healthcare service

providers and patients for bookings, consultations, etc. India is currently enacting legislation concerning digital healthcare, information security, and the protection of personal data. Given the rapid evolution of the healthcare industry, a robust and unified digital health law may be introduced very soon.

Manisha Singh is the Founder Partner of LexOrbis. Manisha is known and respected for her deep expertise in prosecution and enforcement of all forms of IP rights and for strategising and managing global patents, trademarks, and designs portfolios of large global and domestic companies. She is also known for her sharp litigation and negotiation skills for both IP and non-IP litigations and dispute resolution. She is involved in a large number of intellectual property litigations with a focus on patent litigations covering all technical fields – particularly pharmaceuticals, telecommunications, and mechanics. She is an active member of many associations like INTA, APAA, AIPLA, AIPPI, LES, FICPI, and is actively involved in their committee work. She is an active writer and regularly authors articles and commentaries for some of the top IP publications.

LexOrbis
709–710 Tolstoy House
15–17 Tolstoy Marg
New Delhi-110001
India

Tel: +91 11 2371 6565
Email: manisha@lexorbis.com
URL: www.lexorbis.com

Pankaj Musyuni is an Advocate registered with the Bar Council of India, as well as a patent agent. He has a Master's degree in pharmaceutical science and management. He regularly advises clients on IP strategy and portfolio management. Pankaj has in-depth knowledge of patent law and the healthcare regulatory framework in India, as well as extensive experience in patent filing, drafting, prosecution, and advisory matters, especially in the chemical, pharmaceutical, and start-up fields. He has written several articles and delivered talks at various forums on patent law practice, the regulatory landscape, and clinical research.

LexOrbis
709–710 Tolstoy House
15–17 Tolstoy Marg
New Delhi-110001
India

Tel: +91 11 2371 6565
Email: pankaj@lexorbis.com
URL: www.lexorbis.com

Israel


Eran Bareket


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.*"

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.

1.2 What are the key emerging digital health technologies 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 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 are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health in Israel are:

- How conventional healthcare regulation is to be applied to digital health services.
- Secondary use of health data and how it is de-identified (determining standards of de-identification/hiding identity) – currently regulated in part by the Director-General circular on secondary uses of health data.
- Ownership of health data and rights of use.
- Ownership of products developed based on health data.
- Rights of state hospitals and healthcare organisations to hold equity in start-ups.
- Privacy protection of holders of health data – regulated by the Protection of Privacy Law, 5741-1981 and the Protection of Privacy Regulations (Data Security) 5777-2017.
- Creating a uniform platform for collaborations based on databases of different entities (competition law, standardisation of information, etc.).

The Israeli Ministry of Health ("MOH") published in April 2017 "a Digital Health Strategy" document, which sets forth the key enactments for creating a digital health support policy:

- Regulation for the use of health data (goals, manner of use, users, transparency).
- Regulation for the use of remote medical care (the manner in which the service is provided and service provider obligations).
- Regulation for the access of personal electronic health record files by patients.
- Regulation for determining the minimum content of the electronic health records.
- Regulation applying on outcome measures of health data, which collect and monitor health data.
- Regulation for the development and maintenance processes of clinical information systems.
- Regulation for aspects of cyber protection of data.

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

According to the Start-Up Nation Central's report, Israeli digital health companies raised more than $1 billion in the first half of 2021. There is no publicly available data regarding market size in terms of revenues.

1.5 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, among the companies that raised significant amounts in 2021 (see question 1.4 above) are: K Health, a developer of an AI-based personal health assistant; C2i Genomics, a developer of a liquid biopsy for cancer tumour monitoring; Viz.ai, a developer of AI-powered stroke care technology; TytoCare, which developed a handheld device for on-demand remote medical exams; and Ibex Medical Analytics, a developer of cancer diagnostic software for use by pathologists.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The General Director ("GD") of the MOH published a few circulars referring specifically to digital health, as listed below:

- GD Circular, dated 17 January 2018, regarding secondary uses of health data.
- GD Circular, dated 17 January 2018, regarding collaborations based on secondary uses of health data.
- GD Circular, dated 11 November 2019, regarding patient access to personal health data: "*Healthcare under your Control*."

The health data circulars currently prescribe the extent of protection over health data. In general, unless otherwise specified by law or approved by an explicit opt-in, any data under secondary use will be de-identified. Furthermore, any secondary use of health data for research purposes must be pre-approved by the Helsinki Committee.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The following general regulations apply as well to digital health:

- National Health Insurance Law, 5754-1994.
- Public Health Ordinance, 1940.
- Public Health Regulations (Clinical Trials in Human Subjects), 5741-1980.
- Patient's Rights Law, 5756-1996.
- Public Health Ordinance (Food) (New Version), 5743-1983.
- Protection of Privacy Law, 5741-1981 and Protection of Privacy Regulations (Data Security), 5777-2017.
- Class Actions Law, 5766-2006.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The relevant laws applying to consumer healthcare devices or software are:

- As of December 2019, the Medical Equipment Act, enacted in May 2012, is not yet in force.
  The MOH nonetheless operates a MAD division (medical accessories and devices), which registers and grants marketing authorisations for medical devices. On a formal level, such registration and approval is voluntary. In practice, hospitals and health maintenance organisations ("HMO") will not purchase non-approved devices. In addition, the MOH guidelines govern the process of obtaining MOH approval to import and sell medical equipment.
- The Liability for Defective Products Law, 57-401980 is a general law that imposes no fault liability for bodily injury resulting from faulty devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The MOH is responsible for registration and marketing approvals (see question 2.3 above), regulates the approval of clinical trials and regulates secondary use of health data.

The Privacy Protection Authority regulates maintenance of databases containing private data and privacy requirements applicable to uses of such data. The privacy protection commissioner has enforcement authority in cases of unauthorised use of data.

In general, the Authority for Law, Technology and Information (responsible for, among other things, the protection of privacy) is the entity responsible for regulating, monitoring and enforcing Israeli privacy laws, including personal data in digital databases. As mentioned above, uses of health data and collaborations involving health data are also regulated and monitored by the MOH.

The courts have jurisdiction over all issues.

2.5 What are the key areas of enforcement when it comes to digital health?

Further to what is stated in question 2.4 above, because 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.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software MADs are registered as medical accessories, e.g., CoroFlow Cardiovascular Measurement System & Accessories (software which 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.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

To date, no regulations applying specifically to AI have been enacted in Israel. Notwithstanding the above, digital health devices based on AI were registered in Israel by the MAD Department in accordance with customary guidelines applying to such devices abroad.

It is to be noted in this regard that the Israel Innovation Authority and the Ministry of Justice published in March 2021 a call seeking information from the public about the characteristics of the required regulations and the regulatory restraints in the field of AI, with an emphasis on the experimentation and the implementation of AI systems. In view of the above, one can assume that the Innovation Authority will issue a circular referring to the AI field.

3 Digital Health Technologies

3.1 What are the core 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 guidance regarding the technologies below, creating vagueness for the entities active in the digital health field.
  - Regulation of medical practice – the issue arises when practitioners are outside the country's jurisdiction.
  - Misdiagnosis – the risk of misdiagnosis increases when medical services are provided without doctor supervision.

- Privacy – collection, use and security standards for health data.
- Lack of continuity in medical treatment – if a patient receives medical services from different providers, then his medical data will be scattered among different entities. This may make it more difficult to provide optimal treatment in relation to the patient's complete medical history.

- **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.
  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.
- **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. Hence, the same general considerations apply.
- **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? (See question 2.3 in this regard.)
- **Clinical Decision Support Software**
  Clinical decision support systems are currently being developed by various start-ups in Israel. Today there is no regulation that sets conditions for the implementation of such systems. Some key issues are the need to convince physicians of the reliability of the system on the one hand and the need to prevent over-reliance on the system on the other hand.
- **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, simulate professionals' behaviour, by using machine learning. 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.
- **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, 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 which 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**
  We are not aware of any digital therapeutics widely used in Israel.
- **Natural Language Processing**
  Natural Language Processing ("NLP") may be used as part of machine learning 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 instructions regarding its application in digital healthcare.

3.2 What are the key issues for digital platform providers?

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 GD circular on patient access to personal health data, "*Healthcare under your Control*").

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The main issues that need to 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; privacy protection of the data; revenue sharing; data use; and data sharing. See further below.

4.2 How do such considerations change depending on the nature of the entities 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 apply always, regardless of the nature of the entities.

4.3 Which key regulatory requirements apply?

In general, the manner in which health data is used is not statutorily regulated, except for regulation in connection with the protection of data privacy (Protection of Privacy Law, 5741-1981 and Protection of Privacy Regulations (Data Security) 5777-2017). The MOH has issued circulars aimed at regulating secondary use of health data (see question 2.1). Additional relevant law provisions and guidelines include the Patient's Rights Law, 5756-1996, the MOH's guidelines for maintaining the confidentiality and privacy of patients' personal data, and a document of ethics rules of the Israel Medical Association.

4.4 Do the regulations define the scope of 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 What are the key contractual considerations?

The main contractual issues that need to be taken into account 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, 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 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Even though the traditional intellectual property rights do not necessarily apply to data, the key legal issues regarding the securing of comprehensive rights are ownership and exclusivity in the use and collection of the data. For example, exclusivity in the use of data may be beneficial, and the manner in which the data is used is crucial in order to ensure an appropriate use, in accordance with the applicable regulations.

4.7 How are issues with 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.

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.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The key area to be considered is the Protection of Privacy Law; for example, does such sharing require consent of the data subject? The general rule is that sharing/disclosure of identified data requires informed consent, while sharing/disclosure of properly de-identified data does not.

Since the use of personal health data (including de-identified data) for research is considered a "clinical trial", the necessary approvals must be obtained beforehand.

5.2 How do such considerations change depending on the nature of the entities involved?

According to the circulars of the GD of the MOH that apply to medical organisations, personal health data should also not be used for inappropriate social purposes, with an emphasis on discrimination in insurance or employment.

In addition, sharing medical data possessed by medical organisations is subject to regulation set by the MOH.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The Protection of Privacy Law, 5741-1981 prohibits the use of personal data or its delivery to another not for the purpose for which it was provided; this presumably does not apply to de-identified data.

In addition, the Protection of Privacy Regulations (Data Security) 5777-2017 states that, in the event of a contract of a database owner with an outside entity for the purpose of receiving a service, a number of provisions must be stipulated in the agreement, including: the data that the outside entity may process and the purposes of the use permitted in the contract; the manner of implementation of data security obligations the holder has; the contract term; and the return of the data to the owner at the end of the contract.

When it comes to medical data, there are specific conditions for data sharing. 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. Data sharing should also be done to advance the medical field. Moreover, this circular prohibits use for improper social purposes, with emphasis on discrimination in insurance or employment. Exclusive use of secondary health data is limited.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patent protection is governed by the Patents Law, 5727-1967. The law defines a patentable invention as one that is a product or process in any area of technology, which is novel, has inventive step and has utility and industrial application. However, the law excludes a certain type of invention: a process for human medical treatment. Diagnostic and veterinary methods are not excluded *per se*.

A discovery, scientific theory, mathematical formula, game rules and computer software *per se* are not patentable, due to case-law precedents. In general, if the invention involves a technological solution to a technological problem, it is patentable, whether the solution is in the software or not. There is no specific legislation applicable to digital health inventions, and every application is examined on its merits.

6.2 What is the scope of copyright protection?

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 ("GUIs") 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.

6.3 What is the scope of trade secret protection?

Trade secret protection is governed by the Commercial Torts Law, 5759-1999. A trade secret is defined as "business information, of all kinds, which is not in the public domain and is not easily disclosed by others lawfully and the confidentiality of which affords its owners a business advantage over their competitors, provided that its owners take reasonable steps in protecting its confidentiality". The law prohibits misappropriation of a trade secret which is defined as: (1) taking a trade secret without the owner's consent by improper means, or the use of the secret by the acquirer; (2) use of a trade secret without the consent of its owner where the use is contrary to a contractual obligation or a duty of trust the user has to the trade secret owner; and (3) acquiring a trade secret or using it without the consent of its owners, where it is clear that the trade secret has been unlawfully obtained according to (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.

6.4 What are the rules or laws that apply to 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 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 What is 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 (see above).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

This question is being 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 applications were rejected by the examiner on the ground that, while DABUS can be deemed as the inventor, it is not a legal entity and therefore has no capacity of having or transferring a right. Thus, the applicant (the owner of the machine) cannot be deemed as the owner of the invention since he did not derive title to the invention from DABUS. The applicant appealed to the Registrar and a hearing took place on 2 August 2022. The cases are currently awaiting the final decision of the Registrar.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

The Law for the Encouragement of Industrial Research and Development 5744-1984 sets forth the establishment of the Israel Innovation Authority ("IIA") (previously known as 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 State grants funding, generally 50 per cent of the capital required for the completion of the development plan including protection of IP. 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 Israel Innovation Authority should be exploited in Israel and cannot be transferred to a foreign entity without receiving prior permission from the IIA.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

In general, the following points should be addressed:

- the Research and Development ("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; and
- 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 considerations apply in 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.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Healthcare and academic entities, as well as companies, use machine learning in order to develop personalised, preventive, predictive and participatory medicine, including medical tools. For example, machine learning is used for drug repurposing or digital pathology (analysis of pathology slide images). In research performed in Israel, a deep learning algorithm trained on a linked data set of mammograms and electronic health records was found to be able to assess breast cancer at a level comparable to radiologists and to have the potential to substantially reduce missed diagnoses of breast cancer.

8.2 How is training data licensed?

There is neither specific legislation nor case law on the subject, but it seems that a licence must be obtained; as such, activity will more probably than not be considered fair use.

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

Ownership of an enhanced machine learning 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 intellectual property created by machine learning, 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 intellectual property rights. It is important to note that in Israel if the invention is a method in the field of healthcare (like 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 considerations apply to licensing data for use in machine learning?

Some of the main commercial considerations are:

- restrictions on the ability of the owner/possessor of the data to out-license the data (for example, due to privacy law restrictions);
- preventing misuse of licensed data (e.g. unlawful copying or unlawful disclosure to third parties); and
- remuneration to be received (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).

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.

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 about stealing patient medical data and the risk of cyber-attacks.

Oracle recently decided to set up a data centre in Israel, which will include two Cloud servers: one designed for the government and security forces, with a particularly high level of security; and the other for the business sector, corporate clients, as well as start-ups.

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 might 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 intellectual property 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 regulatory defined as MAD (medical accessories and devices), 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 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 Privacy Protection Authority 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.

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
URL: www.gilat-bareket.rcip.co.il/en

Alexandra Cohen holds an LL.B. degree, 2016, from Tel Aviv University.
She handles various aspects of intellectual property rights, including patents, trademarks, designs and copyrights, and represents clients in litigation proceedings before Israeli courts and the Registrar of Patents, Designs and Trademarks. She also provides services with respect to commercial law as well as privacy law and regulations.
In 2016, Alexandra started her internship at Gilat, Bareket & Co. and gained experience in patents, trademarks, copyrights and commercial wrongs litigation. As of 2018, Alexandra continues her practice as a lawyer at Gilat, Bareket & Co.

Gilat, Bareket & Co., Reinhold Cohn Group
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: alcohen@gilatadv.co.il
URL: www.gilat-bareket.rcip.co.il/en

Reinhold Cohn Group (RCG) is the leading Intellectual Property consulting firm in Israel. RCG offers a full breadth of Intellectual Property-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 Intellectual Property assets by securing optimal protection.
Reinhold Cohn Group and its team of professionals are internationally renowned for excellence and continually ranked amongst the top tiers in leading international and local guides.

www.gilat-bareket.rcip.co.il/en

Gilat Bareket Attorneys at Law | Reinhold Cohn Group

Italy


Sonia Selletti


Giulia Gregori


Claudia Pasturenzi

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 (ICT) 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 (WHO)). 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 technologies in your jurisdiction?

Though technological advancement occurs at a fast pace, technology applications and their use do not take place at the same speed. The factors that slow down the use of technologies in healthcare in Italy mainly concern costs related to the initial economic investment, cultural resistance of a part of the population (not necessarily the elderly, which according to some studies have shown to be able to use digital technologies for healthcare purposes), and regulatory compliance.

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, the electronic medical prescription, reservations for online healthcare services (through the *Centro Unico Prenotazioni* (CUP), electronic health records, digitalised reports, telemedicine and teleconsultation.

As for future prospects for improving patient care and rendering healthcare services more efficient, medical apps, the Cloud, artificial intelligence (AI), robotics in surgical interventions (at present primarily used in the most advanced healthcare structures), virtual-reality systems for the simulation of complex surgical interventions and bionics must be included. As a service, digital health insurance is remarkable.

1.3 What are the core legal issues in digital health for your jurisdiction?

The main legal issues are: protection of privacy (please see section 4); safety; and liability for damages to the subjects involved in their use. Informed consent is even more important: the user must be properly informed in accordance with current legislation. This includes the scope of the health act, the use of innovative (digital) means and the benefits/risks that may result. The use of new healthcare IT implies requirements and training for the various subjects involved (healthcare professionals (HCPs), healthcare organisations (HCOs), suppliers, producers, developers, patients, etc.), and wise liability management.

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

The COVID-19 pandemic has enhanced the value of "digital" solutions in every field. The continuing technological acceleration in the Italian healthcare system is part of a socio-economic context that had been moving along this path – albeit at a different speed – for years; a situation clearly reflected in the introduction of electronic health records or the first regulations governing telemedicine.

Given their potential as regards health safeguards and costs, it is reasonable to expect that digital solutions will become increasingly widespread over the next few years. This is also the direction taken by Italy's National Recovery and Resilience Plan (PNRR) (a document drawn up by the Italian Government to illustrate how it intends to manage the funds of the Next Generation EU programme set up by the EU in response to the pandemic). The PNRR subdivides its interventions into six main missions, including digitisation, health and ecological transition), which provides for a substantial fund to be set up, on the one hand to strengthen so-called proximity networks, intermediate structures and telemedicine for territorial healthcare, and on the other hand to enable the upgrade and development of the existing technological and digital structures in the health sector.

Another important step towards the digitisation of Italy's national health system is the introduction of telemedicine to ensure the application of the criteria and reimbursement procedures set out in the so-called Essential Assistance Levels. The authorities have begun this process (although it is not yet completed) which is a central objective of their forthcoming actions.

In this context, it is vital that the development of digital health be accompanied by specific, uniform legislation guaranteeing appropriate regulation and support, so that all the potential offered by digital technology can be exploited in full.

1.5 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 Dedalus Italia S.p.A., 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.

In strategic terms, it is important that companies active in digital health form relationships with the public sector in order to establish essential public/private collaboration, generating positive synergies. Public investment and private investment are a means to make the health service stronger.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

In Italy, the public system for protecting citizens' health is structured around the *Servizio Sanitario Nazionale* (NHS), established with Law no. 833/1978 and inspired by the principles of universality, equality and equity in access to care, as per Art. 32 of the Italian Constitution, which protects health as a "fundamental right of the individual and an interest of the community", and entrusted to the State and public bodies of the NHS. In one word: the State identifies the fundamental principles and determines the essential assistance levels (LEA) guaranteed as a standard throughout the country; the Regions establish health policies for local organisations and access to care. Health services are provided by the public structures of the NHS (hospitals and local health facilities), as well as by private structures duly authorised and accredited to exploit health activities with charges borne by the NHS.

Healthcare also includes the supply of medicinal products (mostly reimbursed by the NHS) through authorised public or private pharmacies which guarantee full coverage of the entire country, including areas at a geographical disadvantage.

This system of a public nature also leaves private operators with margins of entrepreneurial autonomy.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The organisation of the Italian NHS (see question 2.1) has seen a new "model" emerge in recent years, which is destined to have a significant impact on the management of healthcare in Italy: the use of new technologies in the delivery methods of patient services.

Healthcare is one of the sectors of public administration that has seen the greatest growth in the use of new technologies, which serves to improve the quality of care and make it more economic, efficient and effective. While waiting for standardised regulations, the Health Authority (primarily the Ministry of Health) has issued specific guidelines such as for telemedicine ("soft law" is efficient and flexible enough to "rule" fast-evolving sectors). Furthermore, on 9 November 2021, the Superior Health Council has published a document relating to AI and the role it plays in the healthcare world, in particular in diagnostic imaging, analysing its risks and regulation. The document lists a series of operational proposals aimed at both the safe introduction of AI software into clinical practice and the implementation of infrastructures and governance methods that can make our jurisdiction internationally competitive in the planning and development of systems of AI.

The current health emergency situation due to the pandemic has highlighted the need for the urgent implementation of digital media to promote remote healthcare services, given the restrictions on the movement of people and provisions on social distancing imposed at a national level. The competent authorities have put guidelines in place to provide stakeholders with guiding principles for the implementation and use of these technologies.

The digitisation promoted by the PNRR (see question 1.4) is the opportunity to create a more agile and efficient health system, and above all, a system with a greater focus on patient needs. To this end it will therefore be vital to establish regulatory schemes for optimal governance of the central elements where digitisation plays a key role, i.e.:

- development of telemedicine, to further enhance the potential of this tool which has already grown significantly during the COVID-19 health emergency;
- enhancement of data through Big Data Analytics, AI and Machine Learning, to overcome existing fragmentation and take full advantage of the wealth of data held by various national, regional and local operators;
- enhancement, circulation and accessibility of the Electronic Health Record; and
- investment in digital skills, which are essential to sustain the cultural transformation of the system as a whole.

In any case, as regards digital health solutions, the application of more general laws, such as those relating to product safety, medical liability, medical devices and intellectual property is certainly important.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The wide expansion of mobile devices and apps with their software has rapidly turned to tools for medical purposes generating mHealth which not only includes wellness and lifestyle apps, but also real medical-therapeutic apps.

The rapid development of technology does not go hand-in-hand with regulatory provisions, such that applicable regulatory schemes are derived from specific legislation existing at an EU and even US level in an interpretative manner.

Consumer protection legislation applies for apps in general, which provides for obligations and responsibilities of the various parties involved in the distribution chain (Legislative Decree 206/2005 (the Consumer Code)), as well as e-commerce legislation, which requires general and pre-contractual disclosures (Legislative Decree 70/2003), and the legislation on privacy EU Regulation no. 2016/679 (GDPR) and the Italian Privacy Code. Where the app falls within the definition of a medical device, the

legislation on medical devices also applies (EU Regulation no. 2017/745 (MDR) and the recent Legislative Decree 137/2022, which is an adaptation of the Italian legislation to MDR).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

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 the 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 the research; and the Privacy Authority, as the controller of the application of the GDPR and the Privacy Code and guarantor that the processing 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. In Italy, the Ethics Committee 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.

2.5 What are the key 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 healthcare professionals – 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.
- 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.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software as a medical device is governed by MDR on medical devices (including active implantable medical devices), applicable in Italy as of 26 May 2021 and by Regulation EU no. 746/2017 (IVDR), which governs *in vitro* diagnostic medical devices and will be applicable in Italy from 26 May 2022 (until then Legislative Decree 332/2000 applies). Local decrees have been issued to complete the framework: no. 137/2022 (adaptation to MDR); and no. 138/2022 (adaptation to IVDR). Such rules, *inter alia,* recognise the possibility to sell medical devices online (within certain limits).

That said, the first essential step is to ascertain if and when software falls within the definition of a medical device. The assistance of technical experts is advisable as well as careful evaluation of the legal profile: proper qualification will enable correct and effective market access.

For the purpose of correct juridical qualification of software, in addition to the above Regulations, it may be useful to refer to the "MDCG 2019-11 Guidance on Qualification and Classification of Software in MDR and IVDR of the Medical Device Coordination Group" (MDCG) set up in accordance with Art. 103 of MDR (and pursuant to Art. 98 of IDVR), whose aim is to help manufacturers establish when their software products qualify as medical devices.

More examples can be found in the "Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices" (version 1.22 of 2019). Still on the subject of medical device software, reference may also be made to:

- the "Guidance on Clinical Evaluation (MDR)/ Performance Evaluation (IVDR) of Medical Device Software" of the MDCG, March 2020;
- the "Guidance on Cybersecurity for Medical Devices" of the MDCG, December 2019; and
- the European Commission document "Is your Software a Medical Device?" (March 2021), which sums up the key steps for correct qualification of software.

2.7 What regulations apply to artificial intelligence/ machine learning powered digital health devices or software solutions and their approval for clinical use?

There are no specific regulations regarding AI/machine learning powered digital health devices or software solutions and their approval for clinical use. When such instruments qualify as medical devices, the relevant regulations apply (*cf.* question 2.6). Otherwise, the distinguishing characteristics of each solution will have to be identified in order to establish the relevant regulations.

Useful pointers for contextualising the question are provided by the WHO guidance on Ethics & Governance of Artificial Intelligence for Health, drawn up as a result of deliberation among leading experts in ethics, digital technology, law, human rights, as well as experts from Ministries of Health. The guidance lists six principles to be followed to ensure that AI operates in the public interest in all countries.

On 28 September 2022, the EU Commission adopted the Proposal for an Artificial Intelligence Liability Directive (AILD), which could have an impact on Italian legislation. The purpose of the AILD proposal is to improve the functioning of the internal market by laying down uniform rules for certain aspects of non-contractual civil liability for damage caused with the involvement of AI systems.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Despite its enormous potential, telehealth encounters difficulties in finding full application in the services offered by the NHS (largely due to cultural factors, but also due to the absence of a funding model that is consistent with existing legislation). However, there is no lack of initiatives that have been launched by the public sector, which have seen a sharp

increase as a result of the pandemic health emergency, with the implementation of remote consulting services in order to ensure the continuity of care for segments of at-risk populations (cardiology, cancer), apps to allow the rapid and immediate monitoring of patients in home surveillance, and inpatient remote monitoring kits (consisting of a smartphone and a Bluetooth pulse oximeter) in order to keep contact with health personnel to a minimum.

Less recent is the use of telemedicine in the private sector. For example, this can include digital outpatient clinics that provide digital platforms dedicated to telemedicine services through which telephonic and/or video consultations can take place with a specialised doctor and insurance companies, which integrate health coverage with telemedicine services. 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. 38585/2019). This represented an important clarification for the development of new digital health initiatives. Furthermore, in the context of the remote provision of health services, the Regional Administrative Court considered that, in the absence of a data analysis and processing function for medical purposes (which cannot be found in the mere archiving and classification of the same), the software platform used cannot be qualified as a medical device (Regional Administrative Court of Milan, decision no. 452/2022). These indications are important for the many projects of public administrations aimed at implementing the infrastructures necessary for telemedicine and which also involve private operators.

- **Robotics**

  The use of robots in the healthcare sector (in the surgical and rehabilitation field, implantable robotic systems, robotic pharmaceutical cabinets and "social" robots, already used in some hospitals, etc.) requires:
  - continuous software updates and maintenance to remedy malfunctions that can lead to multiple issues related to liability; and
  - protection from risks related to hacking, deactivation or erasure of robotic memory.

  Openness to this technology 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.
- **Wearables**

  Examples of wearables are countless and range from fitness to medicine, from the classic pedometer and sensors for monitoring blood glucose levels, to smartwatches that perform electrocardiograms and provide warnings in the event of atrial fibrillation.

  The two main advantages are:
  - providing continuous monitoring and creating a valuable source of real-life data; and
  - being able to collect data from healthy people, enabling the development of preventive medicine.

  Wearables can also be used in clinical trials, by allowing reliable or near real-time data to be obtained. By using devices that directly transfer data to researchers, the risk of transcription error is avoided and the number of visits to the research centre is reduced.

  As sensitive issues: the management of security and the protection of information collected; and the qualification of certain instruments as medical devices to ensure the application of the relevant legislation.

  Additional knowledge is needed from the user and the physician, and a culture based on scientific evidence must be spread in order to gain awareness as regards actual use.
- **Virtual Assistants (e.g. Alexa)**

  The Virtual Assistant is software that interprets natural language processing (NLP) and communicates with the user for the purpose of providing information or performing certain operations.

  The main issues consist of the management of the large amount of data and the liability of subjects involved in their creation and use.

  Often, this software will process users' data in order to divide them into groups according to their behaviour. This activity falls within the definition of profiling, hence it is necessary to take the precautions provided for by current legislation. This also helps to prevent a violation 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, the Italian Privacy Authority has adopted the 2015 Guidelines (still applicable to the extent compatible with the GDPR).

  Privacy legislation applies with reference to geolocation systems, which are often used by Virtual Assistants.
- **Mobile Apps**

  There are many apps used in the health sector, which offer a wide, constantly evolving range of updated content: wellness and fitness apps; apps for time management (e.g. reminder apps); management apps (e.g. geolocation apps for services and professionals); apps for self-diagnosis and diagnosis assistance (e.g. apps for measuring eyesight, apps for interpreting laboratory test results), etc.

  The main problems 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 the app 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 (see question 4.1).
- **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 softwares currently fall into risk class I (affixing the CE marking without the intervention of the notified body), MDR establishes stricter rules that may potentially lead to an increase in the risk class, with the consequent involvement of the notified body.

  The correct qualification of the software is the first step to properly approach the market: a mistake in its qualification can damage the idea. The regulatory process is equally important; it is recommended to have the support of experts and local advisors.

  Correct management of personal data and responsibilities of the manufacturer, distributors and users are remarkable issues.
- **Clinical Decision Support Software**

  Clinical decision support software uses technologies such as Machine Learning, NLP and Big Data Analytics to assist physicians with clinical decision-making tasks, delivering

actionable recommendations and providing complimentary materials like data reports, guidelines, clinical document templates and more. 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**
  A 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. The outsourcing relationship requires a specific contract to govern these profiles.
- **IoT (Internet of Things) and Connected Devices**
  One of the main problems related to Internet of Things (IoT) is 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**
  3D printing is the technology that allows the creation of three-dimensional objects by joining or printing layers of material based on digital models. Among the main fields of application 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).
  The spread of 3D printing technologies in the healthcare sector certainly has an innovative scope that involves a multitude of corporate and professional entities. It faces many ethical and regulatory challenges, including the correct qualification of the systems in question (namely the applicability of legislation on medical devices), product safety, manufacturer and user responsibility, as well as the processing and protection of data collected by said systems and intellectual property. To date, the legal framework is still fragmented and the application of the rules remains uncertain.
- **Digital Therapeutics**
  As of the time of writing, there is no regulatory definition of Digital Therapeutics, although according to a definition proposed by the Digital Medicine Society – Digital Therapeutics Alliance (widely upheld by the scientific community), the concept includes software-controlled technologies that provide evidence-based therapeutic interventions to prevent, manage or treat a medical disorder or disease.
  Operating in a digital environment, Digital Therapeutics use a variety of techniques, ranging from simple reminders and calculations to gamification, cognitive behavioural therapy or virtual reality, in order to help patients to manage their clinical condition. The core issues concern correct qualification of Digital Therapeutics, which 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 Digital Therapeutics. It is still not clear which regulatory authority (the Ministry of Health for medical devices or the AIFA for pharmaceuticals) should be responsible for the authorisation and management of these new therapeutic tools. 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.
- **Natural Language Processing**
  The difficulty of an algorithm in understanding human language is an issue. Knowledge of the meaning of each single word is not sufficient to correctly interpret a message and can lead to contradictory and meaningless communications with the consequent risk of system unreliability.
  It is necessary to develop new 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 issues for digital platform providers?

The main issue is the liability for illegal content uploaded to the platform.

As regards copyright, according to the Italian Court of Cassation (decision no. 7708/2019 and recently no. 39763/2021), the hosting service provider is jointly liable with the user who uploaded protected content, in the event that:

i. it is aware of the offence committed by the recipient of the service;
ii. the unlawfulness of the conduct of others is reasonably ascertainable; and
iii. it has the opportunity to take action after being informed of the illegal content uploaded.

With regard to the second point, the Court referred to the degree of diligence, saying that it is reasonable to expect this from a professional network operator due to the "technological development existing at the time that the event took place", referring to AI as a tool to locate illegal content uploaded to the web.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The key issue is the processing of personal data on a large scale thanks to the use of new technologies, the Internet and virtual servers. The huge flow of information that derives from the use of digital technologies in the health sector implies the need to solve a series of issues related to the process and protection of personal data (very often of a "sensitive" nature, as it is related to health), in compliance with the GDPR and Legislative Decree 196/2003 (the Privacy Code), which can impose compliance with more rigorous obligations and requirements than those of other sectors.

Other issues are related to the circulation of health data, the outsourcing and delocalisation of systems and services (considering that Cloud services and software on which digital health technologies are based are managed by service providers, hence

the data is no longer stored on the user's physical servers, but is allocated on the systems of the supplier, which often keeps data of varying users with different or even conflicting interests and needs), as well as the storage of data in geographic locations often regulated by different legislation. These profiles are difficult to adjust at a national level, and require "discussion at both a European and international level, in consideration of all of the implications on the processing of personal data" (see the document of the Italian Privacy Authority "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*" of 16 November 2011).

Another critical issue is that of the identification of a legal basis suitable for legitimising the processing of health-related personal data as carried out through digital tools.

This issue emerged with particular reference to the contact tracing apps used during the COVID-19 health emergency as a direct tool to detect contact among users of the app who tested positive for the virus (such as the "Immuni" app, see question 3.1). The Italian Privacy Authority has clarified that the health emergency does not automatically represent a legal basis for particularly invasive processing of data, such as the tracing of contacts by a public or private data controller. The only processing activities with an adequate legal basis are those based on national law and any other processing activities aimed at contact tracing are deemed to be carried out in violation of legislation on the protection of personal data.

Health facilities that equip themselves with telemedicine tools in order to comply with personal distancing measures to provide remote diagnoses or therapies are not required to request specific consent to the processing of the personal data, as long as the data subject is provided with complete information with reference to the processing activities carried out.

On the other hand, since health facilities that process patient data through digital health services are dealing with special categories of data on a large scale, they should carry out a data protection impact assessment, in accordance with Art. 35 of the GDPR (on this specific matter, see decisions no. 49 of 12 March 2021 and no. 201 of 13 May 2021, with which the Italian Privacy Authority assessed the GDPR compliance of two apps implemented by two different health facilities in order to enable patients' relatives to monitor the diagnostic condition of patients who access A&E).

4.2 How do such considerations change depending on the nature of the entities involved?

The Decree Law 139/2021 (the Capacity Decree) introduced changes to the Privacy Code, providing that 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. The Decree Law also eliminated the requirement for the authority to consult the Italian Data Protection Authority before activating high-risk processing – for example, relating to health data.

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 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 healthcare professionals, regardless of whether they operate as freelancers or within a public or private healthcare facility.

4.3 Which key regulatory requirements apply?

The main regulatory source is the GDPR, along with national provisions applicable to data processing activities carried out in the context of digital health. With provision no. 55/2019 above, the Italian Privacy Authority established that the relevant processing activities "only in a broad sense, for care, but not strictly necessary" require, "even if carried out by health professionals", a legal basis other than the need to pursue the purposes of care referred to in Art. 9(2)(h), of the GDPR, "to potentially consist of the consent of the data subject or another legal basis". These processing activities can include those connected to medical apps if data (including health data) are collected for purposes other than telemedicine, or if these data are accessed by subjects other than health professionals and not bound by professional secrecy. Data controllers operating in the health sector that perform various particularly complex operations (e.g. healthcare companies) shall submit the information required by the GDPR to the data subject in a progressive manner, providing:

- information to patients in general only as related to processing activities included in providing ordinary health services; and
- information to patients actually involved in additional processing as regards these specific activities (such as the delivery of online medical reports).

With regard to the storage period of personal data, the Italian Privacy Authority references to sector provisions that provide for the specific retention times of health-related documentation, in addition to more general rules, including Art. 2946 of the Italian Civil Code, which establishes a 10-year term for rights such as those deriving from contractual liability, among others.

4.4 Do the regulations define the scope of 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 What are the key contractual considerations?

If a contract between the data controller and another party involves data processing on behalf of and according to the instructions of the data controller, this party must be considered a data processor. Processing activities carried out by a data processor are governed by a specific contract or other legal act in accordance with EU or Member State law, which contains the requirements provided for in Art. 28 of the GDPR. Given the special nature of tools used by digital health, the data controller must pay attention to the contractual rules carried out by the data processor, as well as the implementation by the latter of suitable technical and organisational measures provided for in Arts 32 *et seq.* of the GDPR, identifying the provider that offers suitable guarantees of compliance with privacy provisions, and in consideration that it could lose direct and effective control over its data by relying on a remote supplier. The data controller

may acquire a prior declaration (supported by documents) from the supplier on the measures taken to comply with the GDPR and carry out periodic audits.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The key legal issues with securing comprehensive rights to data relate not so much to the jurisdiction as to the means used to process data and to provide the information as at Arts 13 and 14 of the GDPR.

When personal data is processed through apps or other digital tools, the information required by the GDPR is not always supplied in an adequate and sufficiently clear manner, partly because of the difficulties involved in making this information available in full and as smart information on these digital tools.

Furthermore, exercise of the rights envisaged by the GDPR must be guaranteed by making it easy for the data subject to forward requests to the data controller.

The data controller must enable the data subject to submit a request without the requirement of any particular formalities (for example, by registered letter, fax, email, etc.) and to this request, the data controller must provide an appropriate response within one month from its receipt (this period can be extended by two months, if necessary).

If the response to an application is not received within the indicated time frame or is not satisfactory, the data subject may contact the judicial authority or the Italian Privacy Authority.

Violation by the data controller of the provisions on the rights of the data subject is subject to administrative pecuniary sanctions of up to 4% of the total annual worldwide turnover of the previous year.

4.7 How are issues with 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*. With particular reference to the issue of discrimination, the Italian Privacy Authority has recently issued a fine amounting to 2.6 million euros against an Italian food delivery company which implemented a treatment of personal data of its employees based on an algorithm, putting in place different violations of the GDPR, also generating discrimination among workers. With this provision, the Italian Authority ordered the company to lay down measures preventing inappropriate and/or discriminatory applications of the reputational mechanisms based on the feedback from customers and business partners (decision no. 234 of 10 June 2021).

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The identification of subjects who have access to the personal data processed 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 do such considerations change depending on the nature of the entities involved?

Data-sharing operations require more caution for health-related data processing as performed by healthcare professionals. 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

National provisions other than those contained in the GDPR do not exist, which, in this regard, constitutes the main regulatory reference. For the transfers of data outside the EU, in addition to the intention to carry out the transfer, the data controller must also indicate the condition of lawfulness of such transfer in the disclosure among those expressly provided for in Art. 44 *et seq*. of the GDPR. Such transfers are only allowed to countries that guarantee the same level of protection of personal data as provided for by legislation in Member States and, only residually, with the express consent of the data subject.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patents for inventions are governed by Legislative Decree 30/2015 (Industrial Property Code (IPC)). The Code does not provide a definition for a patentable invention, but 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. The following, in particular, shall not be regarded as inventions: (i) discoveries, scientific theories and mathematical methods; (ii) schemes, rules and methods for performing mental acts, playing games or carrying out business, and computer programs; and (iii) presentations of information. 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 What is the scope of copyright protection?

The term copyright is used to refer to the protection offered by copyright law, which in Italy is Law no. 633/1941, which gives the creator the exclusive right to use his/her work. This right lasts for the entire life of the creator, and up to 70 years after his/her death. Copyright ceases with its first sale, which means that once the creator puts a work on the market, he/she can no longer oppose the subsequent circulation of the work being sold

or given to third parties, without prejudice to the prohibition on copying, duplicating or renting it (copyright fees must be paid for these activities). 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 What is the scope of trade secret protection?

Legislative Decree 63/2018 enforced the EU Directive on the protection of confidential know-how and confidential business information, expanded the protection already present in the Italian legal system in the IPC and increased penalties for violations carried out through the use of IT tools.

What is protected are "trade secrets" (Art. 98 of the IPC), that is, company information and technical-industrial know-how, including commercial know-how, subject to the legitimate control of the holder. The qualification of secrecy depends on the following conditions, and namely that the information:

a. is secret, in the sense that as a whole, or in the specific configuration and combination of its elements, it is generally unknown or not easily accessible to experts and operators in the sector;
b. has economic value, given that it is secret; and
c. is subject to measures deemed reasonably adequate to keep it secret by subjects who legitimately exercise control.

The protection is extended to data relating to tests or other secret data, the processing of which involves a considerable commitment, and whose presentation is subject to the authorisation of market placement of chemical, pharmaceutical, or agricultural products involving the use of new chemical substances.

The legitimate holder of trade secrets has the right to prohibit third parties from acquiring, revealing to third parties, or using these secrets in an abusive way without consent, unless they have been obtained independently. It is recommended to draft non-generic confidentiality agreements that explain which information must be considered secret and which is public, as well as the relative scope of dissemination. In addition to these agreements, it is advisable to think of specific organisational policies applicable to those who will access the data.

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

The technology transfer includes all of the activities underlying the passage of a series of factors (knowledge, technology, skills, manufacturing methods and services) from the field of scientific research to that of the market. This is a process that results from the collaboration between academia and industry, whose main objective is to make technology accessible to the public. As such is based on research and innovation, it is crucial to consider the protection of intellectual property, which renders the technology transfer safer and more efficient by promoting the use of the innovation by existing or newly-created companies (spin-offs and start-ups). This protection usually falls under the patent protection for inventions or copyright. For inventions created in universities (or public research institutes) the reference is Art. 65 of the IPC, a provision that is not entirely clear as regards its scope and interpretation. It outlines two "scenarios". The first is of "institutional research", in which the patentable inventions made by researchers will be owned by the researchers themselves, and not by the university or public research entity. The researcher is responsible for filing the patent application and informing the institution, and the latter is granted the right to receive at least 30% of the profit of the invention in the event that it is actually exploited economically, also through the grant of licences to third parties. It is then explicitly expected that the entities can establish different ways of distributing the profit by regulatory means, which cannot reduce the benefits of the researcher below the threshold of 50% of the total. The other "scenario" concerns the so-called "funded" research, i.e. that carried out within the framework of specific research projects financed by public or private third parties, for which the entity is entitled to ownership of the invention and can clearly negotiate the rules for the use of the results with the financing party.

6.5 What is the scope of intellectual property protection for software as a medical device?

In principle, software is considered a literary work of art, and is protected by copyright. In this sense, Legislative Decree 518/92 (enforcing directive 91/250/EU) expresses itself on the legal protection for computer programs, which integrated the law on copyright (Law no. 633/1941). Copyright does not protect the idea, but only its expression, and the expression of a software is in its code. Thus, copyright concerns the source code and the object code, but not their function. This means that anyone can create software with a function similar to that of the first author, as long as they do so without copying the source code and object code. The protection of copyright is automatic with the creation of the work. It is possible to register the program in the Public Software Register at the Italian Society of Authors and Publishers (SIAE) in order to obtain proof of authorship. Copyright must be governed in any software contract (development, licence, transfer).

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 Software as a Medical Device (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. This is especially the case for SaMD, where the regulatory complexity of the qualification as a medical device is added to the complexity of the patent.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

The ownership of patents invented by AI devices is a topical issue and is still being debated in a number of jurisdictions.

In 2019, the European Patent Office (EPO) refused two applications indicating an AI system as the inventor on the grounds that the European Patent Convention requires the inventor to be a natural person. The applicant filed appeals against the EPO decision, which are still pending.

To date, there are no rulings on the matter.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

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.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

In 2012, the Italian Ministry of Education, University and Research (MIUR) issued a first call for proposals for the development and strengthening of the National Technological Clusters to create a close link between the industrial system, research system, and national and regional institutions, in order to support strategic national lines on research, development and training of human capital. ALISEI (Advanced Life Science in Italy) is the Life Sciences Cluster that promotes and enhances cooperation and innovation, putting online the best know-how within Italy (businesses, universities, public research entities, advanced production and high value-added services structures), acts as the driving force behind the process of transferring knowledge and technologies from the multidisciplinary research sector to the industrial pharmaceutical-biomedical sector, and serves to facilitate the attraction of public and/or private capital, which is fundamental for the development of innovative projects. The link between the various subjects of the network is generally obtained with specific agreements that may have varying legal nature, depending on the scope and purpose pursued, such as: consortia; contractual joint ventures; 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. It is crucial that the role of each party be defined in all types of agreements, as well as the contribution, participation methods (governance), ownership, sharing of results and intellectual property and its economic exploitation.

7.2 What considerations apply in 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.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

AI is a matter of great interest in Italy and also includes the Public Administration. On 24 November 2021, Italy adopted the Strategic Program for AI 2022–2024; the result of the joint work of the Ministry of University and Research, the Ministry of Economic Development and the Minister for Technological Innovation and Digital Transition. The Program outlines strategic policies to enhance the AI system in Italy, through the creation and enhancement of skills, research, development programs and AI applications, also in the healthcare sector.

Digital healthcare is affected by the use of machine-learning systems, which help physicians improve diagnoses, predict the spread of disease and customise treatments. AI allows the remote monitoring of patients' health conditions (telehealth), optimisation of the management of administrative issues and plays a fundamental role in "precision medicine", an emerging approach that takes individual variability into account in order to develop custom treatments. Through the use of smart machines that analyse a huge amount of data, it is not only possible to make early diagnoses and identify a life-saving therapy faster than traditional methods, but also allow reliable predictive medicine-based approaches. This will allow the research activity to be more effectively focused, such as the potential optimal identification of patients enrolled in clinical studies. Robotics is making a valuable contribution in operating rooms (such as tools that allow surgical intervention in a more precise and less invasive manner through the supply of maps of the parts of the body, prepared on the basis of AI algorithms, thus allowing a shorter hospital stay for patients and economic savings for healthcare facilities).

8.2 How is training data licensed?

The stipulation of a specific contract is necessary in order to obtain the training data of third parties, in which the scope of the agreement must be outlined, specifying if the ownership of the data is transferred or exclusive or non-exclusive use is granted (i.e. licence), the duration of the agreement, any right of withdrawal, rights of termination, privacy profiles that may be relevant, as well as the liability of each party. The contents of the agreement varies according to the actual needs of contractors and is based on the principle of autonomy of the parties (Art. 1322 of the Italian Civil Code), without prejudice to the principle of compliance to the law and the limitation of acts contrary to it.

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

Italian legislation poses some obstacles to the recognition of intellectual property rights for that created by machine-learning software. The Italian Civil Code and Copyright Law (Law 633/1941) focus on the personal creation of the work and seem to exclude the ownership of copyright by subjects other than the creator and his/her successors. At present, it appears that AI-equipped software, despite having created the work, cannot hold the consequent rights. However, even the creator (natural person) of the software may not be the owner of the rights to work created by the software, due to the lack of the requirement of personal creativity. It is evident that using this thesis potentially has negative consequences for technological development and may de-incentivise investments. An alternative route currently being explored is aimed at pre-empting the investigation of the "creative act" when programming the software. Entries of software programming would thus become central and coincide with human creativity, which is an essential requirement for the attribution of an exclusive right.

8.4 What commercial considerations apply to licensing data for use in machine learning?

One of the main issues is the identification of the criteria for the adequate financial valorisation of intangible resources, such as machine-learning data. There are several criteria for estimating the value of intangible resources (e.g. the determination of creation costs and discounting of income consequent to use of the resource, the discounting of presumed royalties that the company would pay if it did not own the resource, etc.). The choice depends on the type of intangible resource, the purposes and context of the assessment, and the ease with which reliable information is found on the resource and market on which it is placed.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

To date, the model of imputation of man's indirect responsibility for any adverse outcomes produced by the use of digital health technologies has been used without any particular problems. However, as complex as these technologies may be, the damage can always lead back to the person who planned, built or used this tool.

This "traditional" model of imputation of liability has been questioned following the advent of the latest generation of AI systems that operate on the basis of algorithms open to structural self-modification, determined by the experience of the system itself (machine learning), giving rise to completely unpredictable and inevitable behaviour on behalf of the programmer and/or user. Given this situation, a doctrine theorised the possibility of identifying the liability of the intelligent entity, whether cumulatively or independently of the liability of the programmer and/or user.

The Italian Council of State recognised the legitimacy of a decision by which the Public Administration ordered the transfer of civil servants on the basis of an algorithm, where there is:

- full knowledge upstream of the algorithm used and criteria applied; and
- the imputability of the decision to the entity holding power (which must verify the logic and legitimacy of the choice and results entrusted to the algorithm) (decision no. 2270/2019).

9.2 What cross-border considerations are there?

In case legal relationships may arise from the supply of the technological service such as to involve multiple subjects in different countries, thus involving multiple legal systems (such as a supplier in a country other than that of the user who uses the technological service, but everything could be further complicated by the competing liability of third parties), 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.

According to the rules of international law (Law 218/1995), EU Regulations apply (applicable only to Member States), which give priority to the rights of parties to determine the jurisdiction and the law applicable to the relationship by consensus, introducing the so-called "connection criteria" to designate the applicable jurisdiction and law only in cases where nothing has been agreed upon otherwise between the parties.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services are services offered on-demand by a supplier to an end user through the Internet (e.g. data archiving, processing or transmission).

In healthcare, Cloud systems assist in innovating services provided to patients and healthcare facility management. In Italy, an example of an active Cloud-based service that is subject to specific legislation (namely Prime Minister Decree 178/2015) is the Electronic Health Record (*Fascicolo Sanitario Elettronico*), through which the HCPs and patient can update, view and share all of the health data of the latter.

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 (also taking the methods to manage information and data entered in the Cloud into account).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Non-healthcare companies must carefully know and take into consideration the healthcare sector rules and regulatory frameworks, among which, for example, are as follows:

- about the authorisation for the healthcare activity;
- about the relationships with HCP public employees: in Italy, the performance of non-institutional assignments by public employees is subject to specific requirements (prior authorisation from the body to which it belongs is required); and
- about the marketing of compliant products: among these, not only the compliance requirements (for example, medical device standards if the medical app is qualified as such), but also the rules on information and advertising to consumers.

The evaluation of the legal environment is crucial in supporting the business model.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Once again, the knowledge of the legal framework is crucial for each choice functional to an investment, in order to identify the strengths and possible critical points of the project.

The evaluation requires an interdisciplinary approach, hence it is advisable to have a highly specialised and differentiated team that is constantly updated. On this point, given that the digital sector evolves on a continuous basis, we must consider the issue of obsolescence, which characterises the digital sector, which, in comparison to the others, is in constant evolution.

The market needs must then be analysed, while considering that the two main trends in the health sector consist of, on the one hand, unmet medical needs and, on the other hand, sustainability of the health system.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The main barriers are due to various factors, linked both to economic and organisational issues as well as the possibility of access to digital health solutions by healthcare professionals and patients.

In particular, digital health solution technologies involve costs that require the use of funds that public health facilities may not always have at their disposal.

Another key barrier is purely organisational, and depends on the autonomy of each region in its need to prepare resources and implementation tools. Organisational intermediation by the region appears necessary in order to obtain the structured configuration of the service, to define the procedures, competencies and responsibilities of the structures and professionals involved, as well as the related costs. In Italy, this implies that the legislative-regulatory structure, organisational models and welfare strategies implemented for this purpose by the regions differ from one to another, with consequent non-standardisation and fragmentation of the development and diffusion of these systems on a national level.

In addition, access to digital health solutions requires the availability of infrastructures (e.g., Internet connection) and devices (e.g., tablets and/or smartphones), to which some portions of the population of patients and healthcare professionals do not have easy access.

A further obstacle to the widespread clinical adoption of digital health solutions could be that regarding issues of health liability.

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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Italian law includes provisions guaranteeing the free supply of aids, equipment and prostheses for disabled patients (for example, made-to-measure ocular prostheses, acoustic equipment, corsets, wheelchairs, walking frames, incontinence catheters, etc.).

At the moment, there are no laws providing for reimbursement by the NHS or the free supply of apps or other digital solutions, although the question is certainly under discussion, considering that the growing spread of digital health tools requires the introduction of specific regulations to guarantee that patients have access to digital health solutions that provide them with clinical or therapeutic support.

In other words, the need is felt to identify which access and reimbursement models are usable and sustainable for the new digital tools, also because, besides the close attention paid to the creation of regulatory and clinical development procedures, consideration should be given to the fact that the generation of significant revenue flows is, and will be, one of the main challenges in this sector on all markets.

In this context, the orientation also among private insurers is to identify bespoke insurance packages that enable the user to choose personal prevention, diagnosis, treatment and convalescence services, which facilitate access to digital health solutions.

10.7 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.

Worthy of note are digital therapies, that is, technologies controlled by a software, which provide real therapeutic interventions based on evidence of effectiveness (evidence-based) aimed at preventing, managing or treating a disease or a medical disorder.

This trend of the digital health ecosystem is demonstrating great potential for the treatment of various diseases, including addictions and chronic diseases.

The still unexplored potential of these digital therapies and the complexity of these new frontiers inevitably leads to various profiles of possible criticality, starting with the gaps in the regulatory landscape, which make it difficult to accurately frame these new tools.

Among the main issues we mention the legal framework of digital therapies (and, in particular, whether such therapies qualify as devices or medicines) and the responsibility of digital technologies (the functioning of digital therapies is generally subordinated to the implementation of intelligent algorithms that allow interaction with the patient and, consequently, the clinical benefit). This feature opens up the previously discussed question of the responsibilities of digital technologies.

Furthermore, the specific elements of digital therapies would require *ad hoc* discipline to offer the regulatory clarity necessary for potential vulnerabilities also with reference to privacy and cybersecurity.

Sonia Selletti graduated in law from the University of Pavia in 1991. She was admitted in Milan in1994. 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 gained 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 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. She is co-author of *e-patient e social media, Il Pensiero Scientifico Editore*, 2016.
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 2 885 561
Email: sonia.selletti@studiolegaleastolfi.it
URL: www.studiolegaleastolfi.it

Giulia Gregori graduated in law from the University of Pavia in 2011. She has been a member of the Milan Bar Association since 2019.
Giulia has been working with Astolfi e Associati since 2013 where she mainly works in the field of pharmaceutical and healthcare law. She has also gained experience in data protection law.
She is an Editorial Assistant and 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 2 885 561
Email: giulia.gregori@studiolegaleastolfi.it
URL: www.studiolegaleastolfi.it

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 2 885 561
Email: claudia.pasturenzi@studiolegaleastolfi.it
URL: www.studiolegaleastolfi.it

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 advise Italian and foreign clients in both extrajudicial and judicial matters.

www.studiolegaleastolfi.it

Japan


Kenji Tosaki


Masanori Tosu

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 technologies 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 are the core legal issues in digital health for your jurisdiction?

The core legal issue for a digital health product is the applicability of the regulations under the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices ("PMD Act") to such product as a medical device, which may impose a greater burden on the provider. Medical devices authorised under the PMD Act are also usually subject to reimbursement under the National Health Insurance ("NHI") system, which makes it easier to disseminate the product in medical settings.

The core legal issue for a digital health service is whether or not such service constitutes a medical practice. In principle, medical services can only be provided by physicians or other qualified health care professionals ("HCPs"). In addition, there are certain restrictions on how and where HCPs may provide medical services.

The core legal issue common to both digital health products and services is the regulation of personal information and data. While medical and health-related information would be subject to stricter regulations as sensitive information, the utilisation of personal information and data is essential for the digital health field, and law amendments and special laws were enacted to promote such utilisation.

1.4 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.

1.5 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.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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 Ministry of Health, Labour and Welfare ("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 2.6.

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 HCPs. 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 shall be met.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The application of the regulations under the Act on the Protection of Personal Information ("APPI") is a key issue. For the details of the regulations, please see the responses to questions 4.1 through 5.3.

In addition, 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 regulatory schemes apply to consumer healthcare devices or software in particular?

Consumer healthcare devices or software that fall under the category of medical devices are subject to the regulations under the PMD Act. Please see the responses to questions 2.1 and 2.6.

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 Act Against Unjustifiable Premiums and Misleading Representations ("AUPMR").

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The principal regulatory authorities for the PMD Act are the 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 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 AUPMR is the Consumer Affairs Agency.

2.5 What are the key 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.

2.6 What regulations 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 GCP must be observed. Recently, the MHLW published evaluation indices for the safety and efficacy of SaMD that induces behavioural changes for disease treatment.

2.7 What regulations apply to artificial intelligence/machine learning 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. In addition, an expert committee at the PMDA is currently discussing methods for the examination of adaptive AI devices that are intended to autonomously change their performance after being marketed.

3 Digital Health Technologies

3.1 What are the core 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 response to question 2.6.
- **Clinical Decision Support Software**
  Please see the responses to questions 2.6 and 2.7.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Please see the response to question 2.7.
- **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 response to question 2.6.

- **Natural Language Processing**
  If the product falls under medical device, the PMD Act shall apply.

3.2 What are the key issues for digital platform providers?

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 issues to consider for use of personal data?

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 ("IRB") approval and informed consent, would also apply.

4.2 How do such considerations change depending on the nature of the entities 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).

4.3 Which key regulatory requirements apply?

Business operators that handle personal information (including medical institutions and academic research institutions) must take safety control measures, and they are required to supervise their employees and contractors.

Special obligations are imposed on business operators that handle Anonymously Processed Information or Pseudonymously Processed Information, such as the prohibition of acts that re-identify the principal.

4.4 Do the regulations define the scope of data use?

Apart from certain exceptions stipulated in the APPI, the use of personal information 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 What are the key contractual considerations?

It is advisable to confirm that (i) the provided personal data has been acquired appropriately, and (ii) the provision thereof has been authorised properly through the necessary procedures (e.g., consent of the principal) under the APPI and Ethical Guidelines, as applicable, and to request warranties from the counterparty, as necessary.

When outsourcing the handling of personal information, it is advisable to stipulate the security control measures to be taken by the contractor, as well as the reporting obligation and audit provisions to confirm the compliance status.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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. 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.

4.7 How are issues with 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.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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. On the other hand, 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 do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Apart from certain exceptions stipulated in the APPI, the provision of personal data without the consent of the principal is not permitted. 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.

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.

6 Intellectual Property

6.1 What is the scope of patent protection?

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". 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 What is the scope of 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 What is the scope of trade secret protection?

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 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 What is 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?

No, an AI device cannot be considered an inventor of a patent under Japanese law.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

With respect to certain intellectual property rights that are associated with the results of government-contracted research and development ("R&D"), 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.

7 Commercial Agreements

7.1 What considerations apply to 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 considerations apply in 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.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning is playing a role in improving the accuracy of diagnosis using images such as CT and MRI. Machine learning is also expected to improve the accuracy of disease diagnosis by learning from past electric medical records, and to identify mental illness by performing natural language processing of patient's statements. In addition, machine learning is expected to play a role to efficiently perform a vast amount of analysis and work in pharmaceutical R&D and the genome analysis area.

8.2 How is training data licensed?

Training data may be protected under the Copyright Act of Japan. The Copyright Act provides that a database that involves creativity, by reason of the selection or systematic construction of information contained therein, is protected as a work. Training data may fall under a database and its selection of data or systematic organisation of data may involve creativity. In such situation, the training data can be treated and licensed as a copyrighted work. Even when training data is not treated as a copyrighted work, there is a possibility that training data is treated as "Shared Data with Limited Access" under the UCPA. Wrongful acquisition, use and disclosure of "Shared Data with Limited Access" can be treated as "Unfair Competition" under the UCPA, and the person who wrongfully acquired, used or disclosed the data may be enjoined to do so and/or be held liable for the damages under the UCPA. "Shared Data with Limited Access" is defined as "technical or business information that is accumulated to a significant extent and is managed by electronic or magnetic means as information to be provided to specific persons on a regular basis (excluding information that is kept secret)". In the case where the training data falls under this definition, the training data can be licensed as "Shared Data with Limited Access". Even when training data does not fall under a copyrighted work or "Shared Data with Limited Access", some businesses still enter into a "licence agreement" on training data. However, as use of such training data without authorisation does not cause any liability, such "licence agreement" is just a declaration that the "licensor" will not object to the use of the training data by the "licensee".

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

If there is no active human involvement in the software development at all, no intellectual property 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 considerations apply to licensing data for use in machine learning?

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.

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.

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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Digital health solutions may be reimbursed under the NHI. 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 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.

Under the APPI, the provision of medical information to a third party requires the opt-in consent of the principal. However, the Next Generation Medical Infrastructure Act ("NGMIA") allows an opt-out for the provision of medical information to a certified entity performing anonymous processing of medical information to enhance utilisation of Anonymously Processed Information in the medical field. There are plans to amend the NGMIA in the near future to resolve a number of issues that are currently preventing effective utilisation.

Kenji Tosaki is a partner at Nagashima Ohno & Tsunematsu. His practice focuses on dispute resolution. He specialises in intellectual property litigation and complex commercial litigation, and he also covers the area of TMT, including data protection matters.
In the area of intellectual property 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
URL: www.noandt.com/en

Masanori Tosu is a senior associate 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

Korea

Jin Hwan Chung

Eileen Jaiyoung Shin

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 & communication technology, which includes telemedicine, mobile health, health information technology and hospital digitaliation systems, such as electronic medical records (EMRs) and electronic health records (EHRs).

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

Korea is one of the leading countries in the field of digital health. The picture-archiving and communication system (PACS) was introduced in the mid-1990s, and EMRs and EHRs were introduced in early 2000s. In recent years, software as a medical device (SaMD) products have become a key emerging part of the digital health industry, and the Ministry of Food and Drug Safety (MFDS) established a guideline for the regulatory approval of digital health products in August 2020.

1.3 What are the core legal issues in digital health for your jurisdiction?

First, under the Medical Service Act, which requires medical services to be provided by healthcare professionals at a medical institution, it can be difficult to adopt and implement new digital health technologies in a swift and broad manner (e.g., limited allowance of telemedicine).

Second, due to Korea's universal national health insurance system, any new digital health technology or product is required to be evaluated and included in the national health insurance system in order for it to be widely used in the healthcare service market.

Third, the Personal Information Protection Act of Korea imposes very strict restrictions on the collection and use of personal data, and these restrictions can present substantial challenges in developing and using new digital health technologies and products.

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

According to the data announced by the Ministry of Trade, Industry and Energy, the revenue of the digital health industry in Korea in 2020 was around KRW 1,354 billion (USD 1 ≒ KRW 1,200). It is understood that the Korean digital health industry has grown by at least 10% annually since then.

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

No public data is available.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

A bill to promote and provide a framework for digital health was submitted to the National Assembly in 2022, but has not yet been enacted. As such, currently, there is no general statutory regulation governing digital health in Korea.

The Medical Devices Act is the current statutory regulation that serves as the central regulatory scheme for digital health. If a digital health product falls within the scope of medical device, prior approval or certification by the MFDS is required for market entry. If a product is classified as a wellness product, no prior approval or certification is required. In this connection, the MFDS has established guidelines for digital health product approval, mobile medical app and wellness products, etc.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Certain new digital heath technologies are required to undergo the new health technology assessment (nHTA) pursuant to the Medical Service Act prior to use at a medical site. Further, telemedicine is restricted under the Medical Service Act.

Korea implements a universal public health insurance system based on the National Health Insurance Act: every medical institution is required to provide medical services under the national health insurance system, and every citizen is required to contribute a health insurance premium based on his/her income or assets. As such, it is important for a digital heath product or service to be eligible for reimbursement under the National Health Insurance Act for commercial success in the market.

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.

The Personal Information Protection Act, 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.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

As explained in question 2.1, the Medical Devices Act and the MFDS guidelines provide the basic regulatory scheme. Having said that, if a digital health product falls within the scope of medical device, prior approval or certification by the MFDS is required for market entry. However, if such product is classified as a wellness product, no prior approval or certification is required.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

Regarding medical device qualification or requirements, the MFDS is the principal regulatory authority under the Medical Devices Services Act. If a particular digital health service relates to telemedicine or another type of medical service, or if the eligibility for national health insurance reimbursement becomes an issue, the Ministry of Health and Welfare (MOHW) is the authority in charge. Further, the Personal Information Protection Commission will have the authority if personal data protection issues are concerned.

2.5 What are the key areas of enforcement when it comes to digital health?

Since it is more likely that digital health technologies or products may fall within the purview of medical device, the MFDS will be the primary law enforcement authority relevant for Korea. The MOHW will be involved if the digital heath technology is required to undergo the nHTA prior to be used by healthcare professionals or the eligibility of the national health insurance reimbursement is concerned.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

First, an SaMD should be approved or certified by the MFDS. Further, if an SaMD is classified as new medical technology under the Medical Service Act, such SaMD will be subject to the nHTA, as explained above. In addition, as Korea adopts a universal national health insurance system without allowing patients or medical service providers to opt-out, the SaMD may be required to be reviewed for eligibility for the national health insurance reimbursement.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

The Medical Device Act and the MFDS's guidelines based thereon will apply.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Under the Medical Service Act, telemedicine is allowed only between physicians: (a) physicians can receive support for patient treatment and diagnosis from other physicians via telecommunication devices; but (b) "physician-to-patient" telecommunication is not permitted.
  However, the government permitted "physician-to-patient" telemedicine on a temporary basis, so as to cope with the COVID-19 pandemic, by amending the Infectious Disease Control and Prevention Act in December 2020. Since then, the government has attempted to convert such temporary telemedicine scheme to a permanent one by amending the Medical Service Act, and continues to discuss with medical societies the details of telemedicine (e.g., permitted disease or treatment, prerequisite conditions, national health insurance reimbursement, etc.); however, no notable consensus has yet been reached by the government and medical societies.
- **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 the MFDS's market approval. As medical services can be provided only by healthcare professionals under the Medical Service Act, wearable devices are not allowed 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**
  Notable SaMD products are introduced in Korea, and it is understood that significant investments continue to be made for SaMD development. According to the MFDS data, 49 SaMD products were newly approved in 2022 while only six products were approved in 2018. The MFDS has displayed a keen interest in continuing to issue regulatory guidelines and policies for SaMD.
- **Clinical Decision Support Software**
  The majority of SaMD products approved by the MFDS may be classified as clinical decision support software. According to the MFDS data, 31 SaMD products were classified as clinical decision support software among 49 SaMD products that were approved in 2022.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Artificial Intelligence/Machine Learning Powered Digital Health Solutions can also require the MFDS's market approval if the product is deemed a medical device.

According to the MFDS guideline, artificial intelligence-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 innovative medical devices under the Act on Nurturing the Medical Devices Industry and Supporting Innovative Medical Devices.
- **Digital Therapeutics**
  Among the 49 SaMD products approved in Korea, 17 products are digital therapeutics. The diseases for which these digital therapeutics are intended to be used include ADHD, mild cognitive impairment, developmental disorder, alleviation of addiction as well as insomnia.
- **Natural Language Processing**
  No particular development has been made from a regulatory or governmental policy perspective.

3.2 What are the key issues for digital platform providers?

Digital platform providers face many challenges under the current regulatory scheme:

(1) "Physician-to-patient" telemedicine and online dispensing of drugs are strictly restricted under the Medical Service Act and the Pharmaceutical Affairs Act.

(2) It is difficult for a digital platform provider to collect and manage patients' data from diverse medical institutions so as to provide tailored services to each patient under the data privacy laws.

(3) It is generally accepted that Korean medical institutions are highly digitalised; however, due to the lack of a standardised system, there are technical difficulties in achieving system connection among medical institutions.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The Personal Information Protection Act regulates the collection and processing of (i) "general" personal information, (ii) "sensitive information" which is deemed to present clear risks of invading the data subject's privacy – including information relating to health or sex life (this includes the subject's historic and current medical history, physical/mental disability and sexual orientation, but excludes information on blood type), genetic information, bio-identifying information (information relating to a person's physical, physiological or behavioural characteristics collected through certain technological methods for the purpose of identifying/certifying a particular individual), and (iii) personal identifying information such as resident registration number, passport number and foreigner registration number.

"General" personal information can be processed in the following circumstances: (i) upon the consent of the data subject; (ii) if particularly required by law or if necessary for the purposes of complying with the law; or (iii) if necessary for the purposes of executing and performing a contract with the data subject.

In the case of "sensitive information", processing is allowed only if (i) consent for the use of "sensitive information" separate from consent for the use of "general" personal information is obtained from the data subject, or (ii) the processing of the information is specifically required or permitted by law. Additionally, if the data subject is less than 14 years of age, consent by such data subject's legal representative is required.

4.2 How do such considerations change depending on the nature of the entities involved?

No change is recognised, in principle.

4.3 Which key regulatory requirements apply?

The following main duties apply with respect to the processing of personal data:

- Duty to implement safety measures for the protection of personal data: protection measures in accordance with the "Personal Information Safety Measure Standards" must be implemented to prevent the loss, theft, leaking, forgery, modification or damage of personal information. Additionally, bio-identifying information (i.e., information relating to a person's physical, physiological or behavioural characteristics collected through certain technological methods for the purpose of identifying/certifying a particular individual) must be encrypted when transmitting or storing.
- Duty to prepare and disclose a privacy policy: a privacy policy including legally mandated matters must be disclosed through methods such as uploading on the processors homepage.
- Duty to designate a personal data protection officer: a personal information protection officer must be appointed to comprehensively take charge of personal information processing.
- Duty to notify and report personal data leakage.

4.4 Do the regulations define the scope of data use?

The Personal Information Protection Act stipulates as its basic principle that only minimal personal information necessary for the relevant purpose should be legally collected, and that the information should not be used for any purpose other than the purpose it was collected for.

When obtaining the data subject's consent, the "purpose of collection and use of the personal information" must be disclosed to the data subject, and the Personal Information Protection Act provides that the collected information cannot be used for any purpose other than the purpose disclosed to the data subject.

4.5 What are the key contractual considerations?

As explained in question 4.1 above, the Personal Information Protection Act requires a data subject's consent for the processing of personal information, unless such processing is specifically permitted or required by law. As far as health data or medical data is concerned, the data subject's informed consent is required.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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.

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

The current Personal Information Protection Act and relevant laws do not stipulate explicit regulations with respect to data inaccuracy, bias and/or discrimination.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The Personal Information Protection Act separately regulates (i) "third party provision" of personal data where data is provided for the third party's own business objectives or own benefit, and (ii) "third party outsourcing" where the personal data is transferred to the third party for the third party's processing of data for the purpose of the data processor.

Third party provision of personal data requires the data processor to obtain consent from the data subject, outlining the following items: (i) the identity of the third party recipient; (ii) the third party's purpose of using the personal data; (iii) the items of personal data to be provided; and (iv) the retention and use period of the personal data by the third party.

5.2 How do such considerations change depending on the nature of the entities involved?

No change is recognised, in principle.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The same rules apply as explained in question 5.1 above.

6 Intellectual Property

6.1 What is the scope of patent protection?

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 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.

6.2 What is the scope of copyright protection?

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 What is the scope of trade secret protection?

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 by the holder of said information, and trade secret was defined as being information "maintained in confidence through reasonable efforts" prior to the amendment on January 8, 2019 (effective July 9, 2019), but has since been amended by deleting the phrase "through reasonable efforts", and therefore, represents information "maintained 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 academic technology transfers in your jurisdiction?

The Technology Transfer and Commercialisation Promotion Act applies to 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 What is 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?

Although there is no explicit judgment from the courts regarding this matter yet, the Korean Intellectual Property Office (KIPO) recently issued an invalidation for a patent application claiming to have been invented by artificial intelligence on the grounds that "patent applications with AI instead of a natural person as the inventor are not permitted". The applicant has since filed an administrative lawsuit against this decision.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

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, 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.

7 Commercial Agreements

7.1 What considerations apply to 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 considerations apply in 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.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Medical services by artificial intelligence, especially machine learning, are rapidly moving away from post-treatment centred on analogue devices and towards preventive healthcare based on intelligent healthcare solutions by combining ICT. Preventive healthcare refers to analysing healthcare big data based on data science and intelligent solutions in order to take pre-emptive measures to prevent diseases from occurring.

Machine learning is simply a process to produce a model as a result of training using statistical techniques on a given data. Large-scale data preparation is important for constructing a more accurate prediction model, although it is necessary to prepare a complete, accurate and consistent dataset by properly processing raw data through pre-processing.

Such machine learning can be used for digital healthcare, real-time monitoring of patients, disease prediction and diagnosis, which tracks the causes of abnormal conditions for individuals in digital health and provides personalised health care guides.

8.2 How is training data licensed?

The right to use a training dataset is essentially regulated by contract between the parties giving and receiving the data.

Generally, data can be protected with intellectual property rights (e.g., copyright, trade secrets) if certain requirements are met. If a licence is granted for data protected with intellectual property rights (e.g., copyright, trade secrets), certain restrictions on its use may apply not only from the licence agreement, but also from the relevant intellectual property laws.

For training datasets, the dataset itself may be protected as a copyright if individual data is protected as copyright, or if the dataset meets the requirements of a database under the Korean Copyright Act (a compilation that systematically arranges or organises materials that individually allows access to or search of such materials).

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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.

Differing views exist regarding whether or not the creation of artificial intelligence, such as machine learning, will be protected with intellectual property rights, with those in favour stating that it will promote the development of cultural industries, and those against it voicing concerns of monopoly.

There are conflicting views on how to attribute the creation of artificial intelligence to individuals between those that view that it should be attributed to (i) the developer of the artificial intelligence, (ii) the owner of the artificial intelligence, or (iii) the artificial intelligence itself. Among these, the view that intellectual property rights should be attributed to the artificial intelligence itself can be understood to be in anticipation of the emergence of strong artificial intelligence with self-awareness that can conduct work without direct orders from humans.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Various commercial considerations should be taken into account when licensing data for machine learning. In such cases, machine learning 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 machine learning using the data, and the right to sublicense should all be considered.

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.

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 the 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 medial 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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 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

Email: jinhwan.chung@leeko.com
Tel: +82 2 772 4711
URL: www.leeko.com

Eileen Jaiyoung Shin is a partner in the Corporate Practice Group at Lee & Ko. Eileen is also a partner in the Healthcare/Life Sciences Team of Lee & Ko, and 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

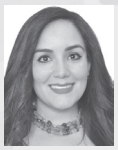
Email: eileen.shin@leeko.com
Tel: +82 2 772 4831
URL: www.leeko.com

Lee & Ko is a premier full-service law firm in Korea which has been actively servicing multi-national clients since its establishment in 1977. Lee & Ko is comprised of 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

Mexico


Christian López Silva


Carla Calderón


Marina Hurtado Cruz


Daniel Villanueva Plasencia

Baker McKenzie

1 Digital Health

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

While there is no legal definition for digital health under Mexican law, 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.

The most ambitious initiative to date has been the stand-alone "General Digital Health Law". This initiative, for example, includes the following definition of Digital Health: "*[A]ctivities related to health, services, and methods, which are performed at distance with help of ITs and other technologies. It includes telemedicine, tele-education in health, and encompasses diverse technologies such as IOT, AI, machine learning, macro data, robotics and other technological developments that may exist.*"

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, "*expands 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 technologies in your jurisdiction?

Telemedicine, electronic prescription, medical apps, online platforms for e-commerce, online communities of physicians or patients, different digital platforms for health services, electronic health records and online pharmacies.

1.3 What are the core legal issues in digital health for your jurisdiction?

As the existing legal framework was designed to address a physical world (including products, services and establishments) and not digital or virtual environments, the applicability of old rules to new situations is far from clear, generating great legal uncertainty, which turns into commercial uncertainty and risk.

Some adopt the position that existing regulation can be made applicable through standard legal interpretation. Others, however, argue that the new situations are in fact not regulated.

For us, the two core legal fields in relation to digital health are announced in the term itself and therefore are: (i) the regulation of information technologies, which encompasses privacy; and (ii) the regulation of health.

At the same time, considering that neither of those regulatory fields are harmonised internationally, but that the nature of the operations of the digital health industry are typically of a cross-boundary nature, this adds a further layer of legal complexity.

Now, digital health applications generate an important amount of health data, which then becomes a strong currency driving further innovation. Therefore, legal issues such as ownership, access, processing, use and commercialisation of data, in different contexts and multiple platforms, become crucial factors.

There are, of course, other legal implications that are also very important to consider, such as intellectual property, tax, product liability and contracts, which can also impact the development of a market of digital health, although the regulatory aspect is fundamental.

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

According to Statista, in 2022, the revenue of the digital health market in Mexico amounted to US$1.44 billion. This market reports a 300% growth in 2022 and is expected to grow to US$1.96 billion in 2025.

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

EvaPacs, Zenda.la, Okani, Fitpass and Prixz.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Mexico does not have a comprehensive and dedicated regulation for digital health. However, the health regulatory framework

applies to a large number of product and services categories, which can capture digital health applications.

The framework law is the GHL, from which stem several Secondary Regulations that set forth rules for: (i) products, including drugs and medical devices; (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, technovigilance and good manufacture practices.

Noteworthy, the product category of medical device ("MD") is very relevant for digital health applications. MDs include the sub-categories of medical equipment, prostheses, diagnostic tools, dental products, surgical & healing products and hygienic products.

More recently, a new sub-category of MD was added as a Technical Standard. On 21 December 2021, NOM-241-SSA1-2021 on Good Manufacturing Practices for Medical Devices ("NOM-241") was issued, which introduces the notion of Software as a Medical Device ("SaMD").

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 *Supplement on MDs* contains rules for the classification of SaMD.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

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 Mexican Data Protection Authority (the "INAI") 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 not particular regulations for health data. Instead, data protection is regulated by the laws mentioned herein, across all sectors and industries. In addition, it should be considered that other laws such as the federal consumer protection law 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.

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 same 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 has publicly recommended their implementation. 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 regulatory schemes apply to consumer healthcare devices or software in particular?

Our local health regulatory framework does not contain a regulatory category for "consumer products" or "consumer devices". This is rather a commercial term that can refer to a variety of regulatory categories, including (i) medicines, particularly over-the-counter drugs, (ii) medical devices, (iii) cosmetics, (iv) dietary supplements, and (v) food & beverages.

In the context of digital health, as mentioned before, the most relevant regulatory category would be that of MDs, which includes the sub-categories of medical equipment, prostheses, diagnostic tools, dental products, surgical & healing products and hygienic products. Furthermore, by recent addition, it also includes the sub-category of SaMD.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The Federal Commission for the Protection against Sanitary Risks ("COFEPRIS") is the federal authority in charge of health regulation, which includes drugs, medical devices and healthcare services.

The INAI is the data protection regulator in Mexico. The INAI has the purpose 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 INAI 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.

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. 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 in the protection and enforcement of IP rights.

2.5 What are the key areas of enforcement when it comes to digital health?

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 prior marketing authorisation be triggered, but also other regulatory requirements, including (i) product-related requirements, such as advertising rules, (ii) establishment-related requirements, such as the rule for good distribution practices, or (iii) company-wide requirements, such as operating a technovigilance 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 practice 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 is still a highly active regulator as is shown in its latest report for 2022, with 119 recorded proceedings and having concluded 78 of them, which derived in total $60 million in fines (approx. US$1,226,333.31). The INAI also began 249 Right Requests to confirm compliance with the law, from which 144 relate to the access right, five to rectification, 102 to cancellation and 35 to opposition.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

A new technical standard for medical devices recently entered into force, NOM-241. NOM-241 incorporated as a sub-category the notion of SaMD.

There is, however, another regulatory instrument missing. It is expected that the Supplement on Medical Devices of the Pharmacopeia will soon be amended to incorporate rules for the classification of SaMDs. To recall, medical devices are classified into classes I, II and III, according to the level of risk their use represents.

Apart from that, the whole regulatory framework for MDs would be applicable, including the GHL, the Secondary regulations for Medical Products, the technical standard NOM-137-SSA1-2008 on the labelling of MDs and NOM-240-SSA1-2012 on technovigilance.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

In 2018, Mexico issued an Artificial Intelligence ("AI") Strategy to create a framework for the development of an AI, becoming the 10th country to formalise an approach to AI. However, the current Administration of President Andrés Manuel López Obrador decided not to carry on with this strategy, therefore it is unlikely we will see any policy development on AI soon.

Since Mexico does not have a particular regulation addressing AI or machine learning, their health care applications are regulated only by the health regulatory framework. Depending on the application and business model of certain AI or machine learning, one or more regulatory schemes would be triggered.

The INAI has 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/machine learning 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/machine learning 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.

3 Digital Health Technologies

3.1 What are the core 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.
  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 subcategory of medical devices.
  Rather, challenges may exist in relation to intellectual property 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 medical devices, 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).
- **Software as a Medical Device**
  While SaMD has been recently recognised as a regulatory category in Mexico, specific regulations have not yet been issued, as mentioned in questions 2.1 and 2.6.
- **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.
  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 medical devices, thus the same challenges described above for other digital health applications would apply.
  At the same time, there are issues related to the collection of real-world data from patients. This kind of data is not yet 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 regulatory categories would include both medical devices and medicines, it is likely that in Mexico, they would be framed as a MD.
- **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 issues for digital platform providers?

From a health regulatory perspective, we often see that digital platform providers see the model of marketplaces as a means to avoid regulatory obligations, thinking that it would be the product or service provider who would bear alone the responsibility. We typically suggest for them instead to, first understand what the regulatory implications of their business model are, and second, identify more clearly in the agreements that will need to be executed with relevant parties in the model, what the obligations are and how compliance will be audited.

Also, digital platform providers frequently need to understand that some digital versions of business models, even if they are not regulated specifically, are likely to be caught by the regulation that was built for a physical version of a similar model. Thus, for example, the rules for brick-and-mortar pharmacies or medical consulting rooms typically apply to online pharmacies or telemedicine.

From an information technologies perspective, it is key for digital platform providers to comply with the requirements set forth by the corresponding data protection legal framework, depending on whether the data controller is a private or public entity, which include the delivery of a privacy notice and obtaining consent from the data subjects for the processing of their personal and particularly their sensitive personal data, as well as their consent for transferring the data to any third party that is not a data processor.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

In accordance with the information published by the INAI for 2022, 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) to deliver and comply 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.

4.2 How do such considerations change depending on the nature of the entities involved?

While both the public sector and private sector laws are omnisectorial, 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.

4.3 Which key regulatory requirements apply?

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.

4.4 Do the regulations define the scope of 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 What are the key contractual considerations?

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 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Under the Mexican Constitution and the Law, data subjects have the constitutional right to request access, rectification, cancellation, opposition and revocation of their personal data. After having received a request, the data controller has a particular period to analyse the request and provide confirmation; after having confirmed, there is another period for complying with the same. This must be detailed in the privacy notice that must be delivered to data subjects prior to the processing of their personal data.

It should be considered that in Mexico, data controllers may develop and implement self-regulation schemes to ensure compliance with privacy laws and to evidence proven accountability. Self-regulation schemes are a broad term which encompass Privacy Management Compliance Programs ("Privacy Programs"), Binding Corporate Rules ("BCRs") and compliance seals, among other self-regulation institutions. Data controllers who manage to have their privacy programs certified by the INAI are afforded regulatory benefits, such as lesser fines in case of infringements to the Law.

4.7 How are issues with 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 labor rights." This has also been quoted by the INAI in its Recommendations For the Processing Of Personal Data Arising From The Use of Artificial Intelligence.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Please see the answer to question 4.5.

5.2 How do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please see the answer to question 4.5.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patents protect inventions. 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 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).

Finally, it is important to mention that even though an invention meets the requirements of novelty, inventive activity and industrial application, it should not be found on the following list of items that will not be patentable (Art. 49 FLPIP):

- inventions whose commercial exploitation is contrary to public order or contravenes any legal provision, including those whose exploitation must be prevented to protect the health or life of people, animals or plants, or to avoid serious damage to the environment, such as: processes for cloning humans and products; procedures to modify the germline genetic identity of a human being and its products when they imply the possibility of developing a human being; the use of human embryos for industrial or commercial purposes; the procedures for modifying the genetic identity of animals, which involve sufferings without substantial medical or veterinary utility for man or animal, and animals resulting from said procedures;
- plant varieties and animal breeds, except in the case of microorganisms;
- the biological procedures for obtaining plants or animals and the products resulting from these procedures. This will not affect the patentability of inventions whose object is a microbiological procedure or any other technical procedure or a product obtained by said procedures;
- the methods of surgical or therapeutic treatment of the human or animal body and the methods of diagnosis applied to them; and
- the human body in the various stages of its constitution and development, as well as the simple discovery of one of its elements, including the total or partial sequence of a gene.

The initial term of protection of a patent is 20 years.

Regarding computer programs as such, these are excluded from patent protection; however, computer-implemented inventions, which 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 What is the scope of copyright protection?

Copyrights cover literary and artistic works. Computer programs as such 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 document 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, copyrights protect the software whether in source or object code.

6.3 What is the scope of trade secret protection?

The FLPIP defines trade secret as (Art. 163) any information of industrial or commercial application 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.

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 previous paragraphs, as well as a definition for misappropriation and misappropriation infringement and offenses. 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 academic technology transfers in your jurisdiction?

There is no general IP framework for academic technology transfer; general contractual laws apply. Each Higher Education Institution has its own regulation. When collaborating with a university or Institution, it is highly recommended to previously review and agree the conditions in which intellectual property will be developed and protected to avoid future conflicts.

6.5 What is the scope of intellectual property protection for software as a medical device?

There is no specific regulation for the protection of SaMD, so the general rules apply. In this way, the software, whether in source or object code, can be protected as Copyrights. 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?

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.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

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 program, 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.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

There needs to be a written agreement describing the scope of the collaboration and the obligations for each party. It must be agreed beforehand whether the resulting IP 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 IP. In addition, it must be considered that 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.

7.2 What considerations apply in 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.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning is at the heart of AI. However, its role in digital health, from a health regulatory perspective, represents important challenges. The problem is that, continuously using performance data generated by users in order to improve a product, quite closely resembles what constitutes "health-related research conducted in relation to a product", which is subject to both ethical and regulatory approval, in relation to a research protocol. However, having to obtain such approval would inhibit the process. If the data was obtained indirectly from data repositories and not directly from the users, one may argue that a privacy consent would suffice.

At the same time, attention must be paid to the fact that, from a health regulatory perspective, if the product improvement is such that (i) it creates a new functionality of the device, then it requires a new product approval, or (ii) it results in a significant software update, then a modification of the original product approval is required.

8.2 How is training data licensed?

It has not been discussed yet in Mexico whether health data should be licensed for AI training. At the same time, databases can be protected under copyright law, thus their licensing would have to abide to the copyright regime.

In addition, from a data protection perspective, one of the self-assessment questions to be asked, in connection with the Recommendations For The Processing Of Personal Data Arising From The Use Of Artificial Intelligence, is whether staff developing the AI product or service critically assess the quality, nature, source and quantity of personal data used, reducing unnecessary, redundant or marginal data during the development and training phases, and then monitor the accuracy of the model as it is fed with new data.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 considerations apply to licensing data for use in machine learning?

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.

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*.

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 civil code regime, unless it is demonstrated that the damage occurred due to fault of 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 of 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 12 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 where should the digital health care provider be licensed, in his/her place of residence or in the patient's place of residence? 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.

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 INAI 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 program, 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 to invest of venture capital and private equity firms may require a longer period to generate ROI.

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 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.

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 (CENETEC) has been proposed in draft law initiatives as a certifying body for digital health care providers, but it is not within its current scope which is to "*[c]ontribute to meet the needs of health technologies management and assessment through the generation, integration and dissemination of information, recommendations and advices based on the best available evidence, as well as the coordination of sectorial efforts that support decision making in order to facilitate effective access to healthcare services*".

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

The provision of public healthcare services in Mexico is provided by public health care institutions such as IMSS (the Mexican Institute of Social Security Services), ISSSTE (Institute for Social Security for State Workers), PEMEX (Mexican Oil Company) and the Ministries of Defence and Navy, who cater to affiliated workers and their families, with some restrictions. The INSABI Bienestar (the National Institute for Health and Wellness) caters to people with no affiliation to public healthcare services providers. These services attend to most of the Mexican population and must be provided at no cost, therefore the reimbursement scheme does not really apply in Mexico regarding public healthcare services. Rather, there is a system of public procurement of goods and services.

Only around 1.5% or so of the Mexican population has access to private medical insurance where the 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 do not cover medical experimental treatments in clinical phases or that are experimental. For instance, robotic surgery is considered experimental treatment and may not be covered, unless it is for brain surgery.

10.7 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.

There have been multiple draft law initiatives submitted in the Federal Congress in the last two years, which focus on different aspects of digital health. These include initiatives submitted on 20 January 2021, 24 March 2021, 7 November 2021, 25 November 2021, 5 April 2022 and 8 December 2022. The themes included have been telemedicine, electronic health records, e-prescription and medical apps.

Christian López Silva has more than 20 years of experience in the regulation of life sciences, pharmaceutical law and biotechnology matters, having worked in the private and public sectors and at the national and international level. For several consecutive years, Christian has led the rankings for Life Sciences in Mexico (*Chambers Latin America*, *The Legal 500 Latin America*). He holds a law degree from ITAM in Mexico and both a Master's degree in Biotech Law and Ethics and a Ph.D. in International Regulation of Life Sciences from the University of Sheffield in the United Kingdom.

Baker McKenzie
Edificio Virreyes, Pedregal 24, 12th Floor
Lomas Virreyes / Col. Molino del Rey
Mexico City, 11040
Mexico

Tel: +52 55 5351 4141
Email: christian.lopez-silva@bakermckenzie.com
URL: www.bakermckenzie.com

Carla Calderón is an experienced attorney in the regulation of life sciences, pharmaceutical law and biotechnology matters. She regularly advises on matters in the intersection of regulatory, data privacy and intellectual property for the manufacturing, import, distribution, advertising, labelling, commercialisation and post-market vigilance of medicines, medical devices, food and beverages, cosmetics, seeds, cannabis, veterinary products, chemicals, alcohol and tobacco. She has experience in consultancy, government relations, administrative proceedings, product registration and contractual work.

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
URL: www.bakermckenzie.com

Marina Hurtado Cruz leads Baker McKenzie's Patent Practice in Mexico. With more than a decade of experience handling sophisticated intellectual property matters, she advises on a broad range of areas including prosecution, licensing and litigation of patents, utility models, industrial designs and trademarks. In addition to this, Marina has extensive experience in the areas of Health, 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 intellectual property issues to collaborate in the development of IP public policies in 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
URL: www.bakermckenzie.com

Daniel Villanueva Plasencia is a technology partner of the Intellectual Property Practice Group at Baker McKenzie Guadalajara. He has extensive experience in: data privacy, information and cybersecurity matters; regulatory issues related to information technologies and consumer protection; and intellectual and industrial property, especially focused on digital environments, including the use and licensing of trademarks, patents and copyrights. Daniel is a Certified Information Privacy Administrator (CIPM) by the International Association of Privacy Professionals. Before joining the Firm, he was a founding partner of a local firm in Guadalajara.

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
URL: www.bakermckenzie.com

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. Additionally, as a full-service law firm, we have integrated advice in the fields of consumer law, transactional, M&A, foreign trade, antitrust, compliance, employment, tax and litigation.
The Firm works with the leading companies in both the healthcare sector and the information technologies market.

www.bakermckenzie.com

Portugal


Eduardo Nogueira Pinto


Ricardo Rocha

PLMJ

1 Digital Health

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

There is no specific definition of "digital health" under Portuguese law. However, the regulations for digital health matters – understood as the provision of healthcare using digital resources – are usually associated with the laws and regulations on medical devices and with the statutes and/or professional ethics codes of the associated professional associations.

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

1. Telemedicine

Telemedicine is not a recent phenomenon in Portugal. In 2006, an attempt was made to regulate teleconsultations by defining their concept and establishing price lists for telemedicine services in the *Serviço Nacional de Saúde* ("**SNS**") – the Portuguese national health service.

The COVID-19 pandemic increased the use of teleconsultations, with several advantages: greater efficiency; reduction of financial costs; and better accessibility to health services.

2. Medical Software

Medical software is progressively being used in healthcare to help doctors make clinical decisions and establish therapeutic programs. This software is under permanent development and its use is expected to increase exponentially in the future.

3. Health Apps

The SNS already offers some apps and this demonstrates the development of these technologies in the digital health sector in Portugal. One example of these applications is "SNS24", allowing access to digital health services on mobile devices, including teleconsultation, medicines history, prescriptions and therapeutical programs.

Private health companies also offer apps supporting their services allowing teleconsultations, test results, drug prescriptions and monitoring of health parameters.

4. Wearables

Wearable devices, which are products controlled by electronic components and software that can be incorporated into clothing or accessories, are also significant in terms of digital health.

These devices often include heart rate sensors, fitness trackers, sweat meters and oximeters. Technological advances have facilitated an explosion in the range of new devices that can gather data linked to the health of the wearer. Based on rapid consumer uptake so far, it is certain they will become a more integral part of human life in years to come.

1.3 What are the core legal issues in digital health for your jurisdiction?

The main legal issues arise in relation to safety, health literacy, privacy, information security and personal data protection.

The use of digital health resources can lead to self-diagnosis and self-medication by patients using the technology who do not have the knowledge necessary to decide the best treatment for their – alleged – disease. There are also risks associated with this kind of practice. The misinterpretation of the results provided by those devices can lead to unease and anxiety, and to the overburdening of health services due to false emergency episodes.

For matters relating to privacy, information security and data protection, see section 4 below.

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

Some forecasts project the revenue in the Portuguese digital health market will reach around €307 million in the current year. The market's largest sector is the digital fitness and wellbeing sector with a total revenue value of around €173 million in 2022.

The future of digital health in Portugal seems even more promising, as the projected market volume by 2027 is around €470 million.

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

This information is not publicly available even though some important companies are operating in Portugal in the digital health market.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

There are no specific regulations applicable to digital health. The legal framework arises from Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices ("**MDR**") and Regulation (EU) 2017/746 of

the European Parliament and of the Council of 5 April 2017 on *in-vitro* diagnostic medical devices ("**MDIVR**"). There are also the regulations of professional associations addressing professional ethics issues.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the General Data Protection Regulation ("**GDPR**").
- Decree-Law 7/2004 of 7 January on the legal framework for electronic commerce.
- Decree-Law 383/89 of 6 November on liability for defective products.
- Decree-Law 145/2009 of 17 June on the national provisions applicable to the advertisement of medical devices and governing the relationship between healthcare providers and medical device manufacturers.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Apart from the Regulations on medical devices and *in-vitro* medical devices mentioned above, the following consumer protection legislation is applicable:

- Law 24/96 of 31 July, the Portuguese Consumer Protection Law ("**Law 24/96**").
- Decree-Law 57/2008 of 26 March on Unfair Commercial Practices.
- Decree-Law 330/90 of 23 October, the Portuguese Advertising Code.
- Decree-Law 69/2005 of 17 March on the General Product Safety Law, transposing Directive 2001/95/EC into Portuguese law.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

- The Ministry of Health, as responsible for the definition of the national health policy and for the SNS.
- *Entidade Reguladora da Saúde*, which supervises all entities providing healthcare services, except pharmacies ("**ERS**").
- *Infarmed - Autoridade Nacional do Medicamento e Produtos de Saúde I.P.*, the regulatory body supervising medicines and health products ("**Infarmed**"), including pharmacies.
- *Comissão Nacional de Proteção de Dados*, the Portuguese Data Protection Agency ("**CNPD**").

2.5 What are the key areas of enforcement when it comes to digital health?

- The ERS ensures that healthcare providers comply with the requirements for engaging in licensed activities.
- Infarmed supervises the placing of medicines and medical devices on the market, and it enforces conformity with the applicable laws and regulations.
- The CNPD, if processing of personal data is required.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software classified as a medical device is subject to the MDR or MDIVR, as applicable.

From a domestic law point of view:

i) Decree-Law 145/2009 of 17 June, without prejudice to the MDR.

ii) Decree-Law 189/2000 of 12 August on *in-vitro* diagnostic medical devices, without prejudice to the MDIVR.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

There is currently no specific legislation regarding artificial intelligence in digital health devices.

There is a proposal from the European Commission to harmonise the legislation on artificial intelligence in the Member States.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  The main challenges in telemedicine and virtual care are obtaining resources and infrastructure to use telemedicine in the public health services and training health professionals to implement telemedicine as an effective method of consultation.
  The inclusion of digital health implies the redesign of working processes, as well as the integration of new technological systems with existing ones.
  Doctor–patient relationships can also suffer with the use of digital health tools. It is essential to preserve the relationship and the quality of the healthcare services provided to the patients.
  The confidentiality and security of patients and health professionals must always be preserved. All technological devices used must guarantee these matters.
- **Robotics**
  The main concern about the use of robotics in healthcare is the safety of patients and the quality of the healthcare provided. Questions regarding liability for accidents and/or medical negligence can also arise.
  Patient detachment due to the lack of health and digital literacy and the decrease in the improvision capacity of healthcare professionals are also relevant.
  The risk of technical errors and failures is also significant when it comes to the use of robotics in healthcare activities.
- **Wearables**
  Qualification and the requirements to put them on the market are probably the most important issues regarding wearables and mobile apps. Qualification as a medical device is highly important considering that the requirements for the placement on the market differ significantly. As the line between medical devices and non-medical or fitness apps is fine, it is important to ensure the safety of

the users without harming the innovation and development of new technological solutions.
These kinds of technologies can also induce misdiagnosis by users, with the associated danger to the health and safety of the patients.
There are also concerns about the security of patient data and privacy in this field.

- **Virtual Assistants (e.g. Alexa)**
  The safety and the possible illegal practice of health procedures by unqualified "entities" is a very significant risk when it comes to virtual assistants and healthcare.
- **Mobile Apps**
  Please see "Wearables" above.
- **Software as a Medical Device**
  Software can induce overconfidence in patients with the information provided, which may be subject to errors. As mentioned in "Wearables" above, the qualification of software as a medical device is complex, as it depends primarily on the purpose of the manufacturer. As such, it is essential to ensure that the use of software as a medical device is properly supervised by a healthcare professional to avoid risks and misinterpretation of results.
- **Clinical Decision Support Software**
  As support software, this kind of tool should be used to support decision-making by healthcare professionals and not as the final decision-maker. Healthcare professionals should critically analyse the results of software and evaluate whether the suggested decision is correct and suitable for the specific pathology.
  If not, technical errors can compromise the result and the health and safety of the patient. This could then lead to an error in the final diagnosis or in the choice of the most suitable treatment.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  As a technology based on algorithms, it is essential that the algorithm is tested to be fully reliable and safe. A validation system would be essential to ensure the safety and the suitability of those systems. Healthcare professionals need to be specifically trained and educated to apply those technologies to their healthcare activities.
  Another significant issue is the trust of the patients in those tools. It is necessary to provide accurate information on the benefits of AI in healthcare, and to adopt a fully transparent policy and communicate all the risks involved. The increase in use of AI can create a negative impact on the abilities and knowledge of healthcare professionals, which is why all digital tools used in healthcare should be decision-supporters for the professionals and not decision-makers.
- **IoT (Internet of Things) and Connected Devices**
  The privacy and safety of patients are the main issues in the IoT. There is a risk of cyber-attacks that compromise the privacy and safety of the patients and of a lack of trust in the results obtained by those tools.
- **3D Printing/Bioprinting**
  Quality, safety and suitability of these products are the main concerns regarding 3D printing and bioprinting when applied in the field of healthcare.
- **Digital Therapeutics**
  There is a high risk regarding patient data, especially because it may involve very sensitive data. It is also difficult to monitor quality and therapeutic compliance by the patient. The resistance of patients to those therapeutical methods is also an important factor.
- **Natural Language Processing**
  The main concerns are privacy and data protection and the capacity of the systems to correctly interpret messages which may lead to contradictory and meaningless communications. In turn, this could cause the unreliability of the system and risk the safety of patients.

3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are the need to (i) ensure that no illegal content is transferred to the digital platform, (ii) ensure the safety of the patients' data, (iii) ensure that the use of digital platforms is safe, efficient and improves the quality of the healthcare, (iv) design tools that enable a smooth transition to the use of digital platforms and, finally, (v) train and educate healthcare professionals to confidently use those digital tools in their practices.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The processing of personal data must consider the nature of the data, as information that relates to an identified or identifiable person, the process of anonymisation, in compliance with the principle of storage limitation, the process of pseudonymisation, to enhance data protection and authentication procedures. Article 9 of the GDPR prohibits the "processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" ("**Health Data**").

This prohibition may not apply under the exceptions in article 9(2), particularly when the data subject gives explicit consent, the processing relates to personal data which are manifestly made public by the data subject, or the processing is necessary for reasons of public interest in public health.

4.2 How do such considerations change depending on the nature of the entities involved?

Pursuant to article 7 of the GDPR, when processing is based on consent, the controller must be able to demonstrate that the data subject has consented to the processing of their personal data. The consent must be freely given, informed, specific and unambiguous, and the data subject must be able to withdraw it at any time.

Public authorities may process health data when this processing is necessary for reasons of public safety, regardless of consent. In these cases, the processing of health data must be properly justified to ensure the pursuit of a public interest that cannot otherwise be safeguarded. The processing of health data must be carried out by a person bound by duties of confidentiality, and appropriate security measures must be guaranteed to safeguard the security of the information, as defined in Law 58/2019 of 8 August.

4.3 Which key regulatory requirements apply?

Article 5 of the GDPR sets out the principles governing the processing of personal data: lawfulness; fairness and transparency; purpose limitation; data minimisation; data accuracy; storage limitation; integrity; and confidentiality. Exemptions or restrictions to these principles must be provided for by law, pursue a legitimate aim and be necessary and proportional.

Even in cases where the public interest allows for the processing of health data, confidentiality obligations, requirements of proportionality and appropriate security measures must be guaranteed.

4.4 Do the regulations define the scope of data use?

Law 12/2005 of 26 January ("**Law 12/2005**") defines health information as all types of information directly or indirectly linked to the present or future health of a person, whether living or deceased, as well as their medical and family history. Law 12/2005 stipulates that such information may only be used by the health system under the conditions expressed in the written authorisation of the data subject or their representative. Access to health information can be provided for research purposes on the condition that it is anonymised.

Article 6 of Decree-Law 131/2014 of 29 August provides that the processing of genetic information and the creation of genetic databases are allowed exclusively for the provision of healthcare or health research, including epidemiological and population studies.

4.5 What are the key contractual considerations?

Pursuant to article 24 of the GDPR, the controller must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Article 32 of the GDPR provides that such measures include (i) the pseudonymisation and encryption of personal data, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. The controller and the processor should also take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

When using or collecting personal data, it is vital that the data subject has the rights to be informed, to access the data, to rectify inaccurate data, to erase data, to be forgotten, to restrict the use of the data, to enjoy data portability and to object to the processing. In particular, Law 12/2005 defines a genetic database as any record, whether computerised or not, which contains genetic information about a set of persons or families. Regarding such databases, the law establishes that any person may request and have access to information about themselves contained in files containing personal data.

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

Under article 6(2) of Law 59/2019 of 8 August, profiling activities leading to discrimination of natural persons based on special categories of personal data, such as health data, should be prohibited.

Article 11 of Law 12/2005 establishes that (i) no one may be prejudiced in any way on the basis of a genetic disease or of their genetic heritage, (ii) no one may be discriminated against in any way on the basis of the results of a genetic test diagnostic, including for the purpose of obtaining or retaining employment, obtaining life and health insurance, access to education and for the purpose of adoption, (iii) no one may be discriminated against in any form, including in their right to medical and psychosocial follow-up and genetic counselling, for refusal to undergo a genetic test, and (iv) everyone is guaranteed equitable access to genetic counselling and genetic testing, with due safeguarding of the needs of the populations most severely affected by a given disease.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The GDPR provides for the free flow of data within the EU. There are specific requirements regarding the transfer of personal data to third countries outside the EU and international organisations, such as adequacy decisions, standard contractual clauses, binding corporate rules, certification mechanisms and codes of conduct. The primary purpose of these requirements is to offer the same level of protection when the personal data of EU citizens is transferred abroad.

5.2 How do such considerations change depending on the nature of the entities involved?

Pursuant to Directive 2016/680, competent authorities may exchange personal data within the EU. The exchange of personal data in these cases is neither restricted nor prohibited for data protection reasons.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Articles 45 and 46 of the GDPR provide for two ways of allowing the transfer of personal data to third countries and international organisations: an adequacy decision; or, in the absence of an adequacy decision, a controller or processor may transfer personal data by providing appropriate safeguards, including enforceable rights and legal remedies for the data subject.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patent protection confers an exclusive right on the holder to exploit an invention. An invention may be defined, broadly, as a new way of doing something, or a technical solution to a problem in the field of technology. Patent types may amount to a new product, may consist of a new process to obtain a new or an already known product, or to a new use/application of such product.

To be subject to patent protection, the invention must have a technical nature, and meet the standard requirements of novelty, inventive step and industrial application.

6.2 What is the scope of copyright protection?

In broad terms, copyright, referred to in Portugal as authors'

rights, grants protection over externalised expressive intellectual creations, designated as "works" or "artistic, scientific or literary works".

Originality and creativity are the general requirements for a work to be protected by copyright. This means that the work must be the author's own intellectual creation, and that at least some creative aspect is required.

Copyright protection is independent of the disclosure, publication, use or exploitation of the protected work.

6.3 What is the scope of trade secret protection?

The Portuguese Industrial Property Code ("**CPI**") provides that trade secrets are protected and that information will be considered as a trade secret if it meets the following requirements: (i) it is secret, in that it is not generally known or easily accessible to persons in the circles that normally deal with this type of information; (ii) it has commercial value by virtue of being secret; and (iii) it is subject to reasonable diligence in order to keep it secret. Articles 314 and 315 of the CPI identify the acts that constitute a legal or illegal use, acquisition or disclosure of the trade secret.

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

Pursuant to article 59 of the CPI, inventions made by employees or collaborators as a result of their research activities belong to the legal entity under whose statutory scope the research and development activities are carried out.

The inventor will, in any case, reserve the right to participate in the economic benefits arising from the exploitation or transfer of the patent rights.

The terms of this participation and further issues regarding academic technology transfers are defined in the articles of association and the intellectual property regulations of the legal entity in question.

6.5 What is the scope of intellectual property protection for software as a medical device?

Under the CPI, software *per se* cannot be subject to patent protection. However, patent protection may be granted to software which exhibits a technical effect. The EPO has held that computer software can be patented in certain circumstances: (i) when the software affects the execution of processes which take place outside the software or the computerised system; or (ii) when the software leads the computer/hardware to operate in a new manner. Furthermore, software can be protected by copyright under Decree-Law 252/94 of 20 October, which grants software protection analogous to that conferred on literary works.

The source code of a piece of software may also be protected under the trade secrets rules provided that the necessary requirements are met.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

There are no specific rules on AI devices being named as inventors in Portugal. When referencing the inventor and "*his/her successors in title*", article 57 of the CPI appears to be construed around the concept of the inventor being a natural person. Therefore, it seems to exclude legal persons and AI devices from being named as the inventor.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

There are no specific rules on Government-funded inventions. These are subject to the general principles of contractual freedom. The parties can draft the terms of ownership of any IP right and, in the absence of such terms, any supplementary rules will apply.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

There is no specific regulation on collaborative improvements in Portugal. However, these collaborations are accepted depending on the organisations and professionals involved. The regulatory and legal framework must be observed, particularly with regard to interactions between healthcare companies or pharmaceutical industry companies and healthcare professionals, healthcare organisations or patient associations. Under Portuguese law, an "interaction" includes granting benefits to any of the above professionals and organisations, supporting events, granting scholarships and any other interaction that results in the concession of a benefit.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

It is advisable for these agreements to be concluded in a written instrument where key issues are addressed. IP rights, data protection and confidentiality are the main issues to be considered. When concluding agreements with public healthcare entities, legal regulations should be considered to prevent distortions to competition and undue influence of healthcare professionals and organisations.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

As part of AI, machine learning can have a very important role in healthcare. However, this role must respect the patient, his/her safety and privacy.

8.2 How is training data licensed?

Training data may fall under the scope of Decree-Law 122/2000 of 4 July which incorporated into Portuguese law Directive 96/9/EC regarding the protection of database rights. In such cases, the licensing of training data is subject to the general provisions regarding the licensing of intellectual property rights. If it includes personal health data, the limitations imposed by the GDPR should also be considered in the context of licensing.

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

Pursuant to article 11 of the Portuguese Copyright and Related

Rights Code, copyright belongs to the intellectual creator of the work, unless expressly provided otherwise. To date, there are no specific rules for the IP rights resulting from machine learning improvements. Portuguese law does not recognise machine learning or AI as "authors" for copyright purposes. In Portugal, the creation of intellectual works is strictly associated with human beings.

8.4 What commercial considerations apply to licensing data for use in machine learning?

If the licensed data consists of health data, the commercialisation of sensitive information must always comply with the GDPR rules, in particular, the ones in articles 7, 9 and 32. Contractual provisions regarding indemnifications and liability for the use of data in violation of the GDPR should also be implemented by the parties, as should the customary representations and warranties regarding the ownership of the rights over the licensed data. Further issues regarding the definition of ownership of rights relating to that data should also be considered, including the ownership of any future works based on the licensed data, and the conditions and scope of use of that derivative data.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Depending on the specific service provided, contractual liability may be applicable. This liability is governed by the law chosen by the parties in the contract or the law where the service is provided. Moreover, non-contractual civil liability may be applicable if the legal criteria are met. Law 24/96 establishes an objective liability of the manufacturer for any damage caused by defects in the product or service placed on the market. Other bases of liability may be applicable depending on the nature of the event that led to the adverse outcome.

9.2 What cross-border considerations are there?

When it comes to liability in cross-border interactions, B2B relations must be distinguished from B2C relations. Concerning B2C relations, the parties' choice of the applicable law may not always be the prevalent criteria. Under the Rome Convention on the Law applicable to Contractual Obligations ("**Rome Convention**"), other criteria may be adopted to determine the applicable law depending on the specific circumstances of the case. In these cases, the parties may be able to choose the applicable law. However, if mandatory provisions exist in the country where the consumer has their habitual residency, these provisions will prevail. Under the Rome Convention, the applicable law is the law of the habitual residence of the consumer. As regards non-contractual liability, the Rome Convention determines, as a rule, that the applicable law is the one of the countries where the damage occurs, regardless of where the event giving rise to the damage occurred and the country where the indirect consequences of that event occur. However, there are other criteria depending on the specific circumstances of each case.

With special relevance to B2B relationships, under the Rome Convention, the law applicable to a non-contractual obligation arising from an infringement of an intellectual property right will be the law of the country where protection is claimed. In the case of a non-contractual obligation arising from an infringement of a unitary EU intellectual property right, the applicable law will be the law of the country where the infringement was committed, except for questions that are not governed by any relevant EU instrument.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Issues raised by Cloud-based services relate mainly to data protection, data transmission and privacy. It is essential to be aware that data treatment and data transfer by Cloud service providers raise additional legal issues.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The healthcare sector is a heavily regulated sector. EU instruments and national laws establish a framework that must be properly acknowledged by any company before entering the market. Other issues may be raised, particularly regarding intellectual property and data protection.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Considering the level of regulation of the health sector in Portugal, a compliance check is one of the most important requirements any firm should consider when approaching a target firm. The position of the target company in the relevant market, manufacturing costs and distribution channels, IP rights and commercial agreements are key issues to check when entering the market. Possible partnerships with governments in countries with public health systems as well as reimbursement agreements are also important issues that must be addressed before investing in a digital healthcare venture.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barriers are the legal frameworks, the lack of investment from governments in digital health technologies and the lack of adequate regulation regarding some specific technologies.

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?

Public entities such as the Central Administration of the Health Services, Health Authorities or the Shared Services of the Health Ministry perform an important role in this field. Depending on the type of technology, associations representing manufacturers and other stakeholders can influence clinical adoption of digital health solutions. Associations such as the Portuguese Association of Medical Devices, Portuguese Association of Health Engineering and Management and the Portuguese Telemedicine Association may be able to influence such decisions. Professional associations that regulate healthcare professions are also able to influence the clinical adoption of health solution from the perspective of the healthcare professionals.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Reimbursements by the Government depend on the product itself and are subject to specific regulation. Requirements for reimbursement are settled by law or administrative order. Solutions focused on efficiency are more likely to be subject to reimbursement rather than solutions focused on preventive health. Reimbursements by private insurers depend on the type of technology and the insurance policy.

10.7 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.

According to the Deloitte study "Shaping the future of European Healthcare" (2020), the current main challenges identified in the health digitalisation process in Portugal are bureaucracy, the choice of the most appropriate digital solution and training of healthcare workers. Moreover, adjustments in the regulatory framework are said to be needed to increase patient confidence in the use of digital solutions in healthcare. Inclusion of digital health in the education of healthcare professionals and patient literacy in digital health are also identified as key issues to be developed to allow the advancement of the digital transformation.

The Portuguese Government is engaged in the digital transformation of the healthcare sector and the Portuguese eHealth strategy has been referred to as exemplary by the WHO since 2015.

The Portuguese National Centre for Telehealth was launched in 2016 and was the first centre of this kind in the world. Its mission is to facilitate citizens' access to healthcare, ensure its fairness and increase the efficiency of national resources by taking advantage of information and communication technology. Furthermore, the National Strategic Telehealth Plan of 2019 demonstrates the engagement of the Portuguese Government in the digital transformation of the healthcare sector.

The National Strategy for the Health Information Ecosystem also performs an important role in fostering the digital transformation of the health sector in Portugal. The COVID-19 pandemic allowed some barriers to be broken down as it created an environment that was even more receptive to the implementation of digital solutions in the health sector in Portugal.

Eduardo Nogueira Pinto heads PLMJ's healthcare, life sciences and pharmaceutical practice. He has more than 20 years' experience in advising Portuguese and foreign companies, and he has worked on many projects in the areas of healthcare and pharmaceuticals.
He focuses on regulatory matters, licensing, compliance, advertising, prices and reimbursements, contracts and market access.
Eduardo has handled numerous licensing, public procurement and administrative offence proceedings, and he has also advised clients on M&A operations. Furthermore, Eduardo provides regular legal support and advice to the National Association of Pharmacies and to dozens of Portuguese and foreign companies from the pharmaceutical sector.
Eduardo won the M&A Lawyer of the Year in the *LMG Life Sciences Awards 2022 EMEA*.

PLMJ
Avenida Fontes Pereira de Melo, 43
1050-119 Lisbon
Portugal

Tel: +351 213 197 300
Email: eduardo.nogueirapinto@plmj.pt
URL: www.plmj.com/en

Ricardo Rocha is a senior associate with 10 years' experience who focuses on providing regulatory advice to Portuguese and international companies in the pharmaceutical industry. He assists his clients with all matters relating to the development and marketing of medicines, medical devices, food supplements and cosmetics.
Ricardo is building a strong track record and is advising various clients operating in the medical cannabis sector. He is also very active in writing opinion articles and giving conferences on this topic.
Ricardo has a Master's in legal-business sciences from the Faculty of Law of the University of Lisbon and completed a postgraduate course in healthcare law at the Faculty of Law of the *Universidade Católica Portuguesa* and attended the European Pharma Law Academy in Cambridge.
Before joining PLMJ, he was a lawyer at Glintt - Global Intelligent Technologies.

PLMJ
Avenida Fontes Pereira de Melo, 43
1050-119 Lisbon
Portugal

Tel: +351 213 197 300
Email: ricardo.rocha@plmj.pt
URL: www.plmj.com/en

PLMJ is a law firm based in Portugal that combines a full service with bespoke legal craftsmanship. For more than 50 years, the firm has taken an innovative and creative approach to produce tailor-made solutions to effectively defend the interests of its clients. The firm supports its clients in all areas of the law, often with multidisciplinary teams, and always acts as a business partner in the most strategic decision-making processes.
With the aim of being close to its clients, the firm created PLMJ Colab, its collaborative network of law firms spread across Portugal and other countries with which it has cultural and strategic ties. PLMJ Colab makes the best use of resources and provides a concerted response to the international challenges of its clients, wherever they are. International collaboration is ensured through firms specialising in the legal systems and local cultures of Angola, China/Macao, Guinea-Bissau, Mozambique, São Tome and Príncipe and Timor-Leste.

www.plmj.com/en

PLMJ Transformative Legal Experts

Saudi Arabia

Suhaib Hammad

Ebaa Tounesi

Hammad & Al-Mehdar Law Firm

1 Digital Health

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

The Health Sector Transformation Strategy issued by the Ministry of Health ("***MoH***") (the "***Strategy***"), defines digital health as "*the cost effective and secure use of information and communication technologies in support of health and health-related goals. This includes (without limitation) health surveillance, health education, healthcare services, health literature, knowledge and research*" in the Kingdom of Saudi Arabia (the "***Kingdom***" or "***KSA***").

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

The MoH aims to improve the efficiency and effectiveness of the healthcare sector through the use of information technology and digital transformation. The implementation of e-health and electronic information systems are evident in a number of hospitals and organisations in the Kingdom in which the MoH has further launched the Kingdom's SEHA Virtual Hospital, in line with the efforts to digitalise the healthcare industry.

Additionally, the recently implemented Strategy further aims to enhance the quality of healthcare delivery and explores the necessary sustainable services, policies and infrastructure. Some of the key technologies transforming the healthcare sector in the Kingdom include:

- Internet of Things ("***IoT***") and 5G which enables early interventions, serves healthcare providers in reducing costs and improving efficiency, and enhancing remote patient care.
- Artificial Intelligence ("***AI***") as it is utilised in health mobile applications, medical health records and telemedicine. Telemedicine is the technology that enables physicians to provide healthcare from a distance through advanced electronic communication systems. Treatment involves remote examination, automatic forwarding of examinations and analysts' results, exchanging expertise, conducting operations and other medical applications that make use of computer and communications systems in transferring medical information to other locations for remote diagnosis.

Furthermore, the key emerging technological systems in the Kingdom include, electronic medical records ("***EMR***"), picture archiving and communication systems ("***PACS***") and health portals.

- An EMR is an electronic healthcare information record that stores patient information with full interoperability within a health enterprise. It helps connect the work produced by different medical and technical departments. All services rendered to the patient will be stored in the patient record, which secures a more integrated and harmonious interaction between the hospital departments, with a view to providing an excellent health service.
- PACS aim to replace manual medical imaging systems that depend on radiological films with a digital system that enables more than one physician to examine digital images through a computer network. This overcomes the problem of lost images, which reduces the cost of taking images multiple times.

In addition, with the outbreak of COVID-19, Saudi Arabia deployed a number of strategies in the digital health sector to manage the spread of COVID-19. The MoH launched a number of essential tools and technology applications (as will be explained below) for the purpose of responding to COVID-19 while also promoting educational campaigns.

A few of the notable technologies launched during the pandemic include:

- "*Sehha*" application, which aims to virtually connect healthcare practitioners to patients by providing virtual medical consultations. Moreover, EMR have been implemented in all hospitals across the country in order for both patients and healthcare practitioners to access their data from the comfort of their homes.
- "*Sehaty*" is another application that has been introduced for the purpose of booking a slot at the nearest COVID-19 testing location. Upon taking the test, users are able to view their results on the same app within 24 hours.
- "*Tetamman*" was further launched by the MoH for the purpose of monitoring individuals who have been asked to isolate, either due to being infected with the virus, being in contact with an infected person or returning from travels. The application also includes services such as contacting healthcare practitioners in order to follow-up on their case, seek help or book another appointment to re-test where needed.
- "*Tabaud*" was developed by the Saudi Data and Artificial Intelligence Authority ("***SDAIA***") and is the latest application launched by the MoH in its efforts to combat the spread of COVID-19. The application provides three main services: (i) notifying its users if they have been in contact with an infected person during the past 14 days; (ii) providing aid to those who have tested positive or have been in contact with an infected person by sending their details to the MoH in order to provide them with the necessary guides and medical support according to the status of their case; and (iii) enabling individuals who tested positive to voluntarily share their test results with people they have contacted during the past 14 days.

Based on the introduction of such applications, the digital health solutions deployed by Saudi Arabia during the outbreak

of the virus are now being used for the purpose of revolutionising the healthcare system through mobile health applications, telemedicine and virtual/remote healthcare treatment. The hope is for Saudi Arabia to continue its digital growth and shift in the way the healthcare sector is working by introducing more innovative technological solutions in the country.

1.3 What are the core legal issues in digital health for your jurisdiction?

Considering the health industry is undergoing rapid development, there are a number of growing legal considerations regarding regulating the use of technology in healthcare. Along with confidentiality, privacy and security, other issues include changes to the standard of care regarding using electronic rather than paper medical records, user training and assuring accurate information is provided to users. These factors raise concerns for employers and product liability.

There are further legal considerations involved with the use of clinical diagnosis support tools, exchange of health information across institutions and the incorporation of genomic information into the clinical record. Informed consent for exchange of information as well as for the use of specialised tools will also be important to address. Given the sensitive nature of healthcare information, and the high degree of dependence from health professionals on reliable records, the issues of integrity, security, privacy and confidentiality are of particular significance and must be clearly and effectively addressed by health-related organisations and professionals.

Therefore, maintaining and safeguarding the integrity and physical protection of data and systems, privacy and confidentiality of individual health information, quality of content, and the protection of consumers and online health industry commercial interests against unethical practices, are the areas of greatest concern in the implementation and use of the Internet and other interactive applications in health and healthcare.

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

Generally, the digital health market in the Kingdom includes (i) online pharmacies, (ii) virtual doctor consultations, (iii) e-health devices, and (iv) e-health applications. Although there are no definitive figures regarding the market size in the Kingdom, there are, nevertheless, numerous emerging start-up companies and a range of technologies within the digital health sector.

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

Pursuant to question 1.4 above, there are no official records stipulating the largest digital health companies in the Kingdom. However, in recent years, the Kingdom's digital health market has seen a rise in digital health ventures with respect to diagnosis, teleconsultation and health information companies.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Strategy defines digital health governance as "*a system of policies, regulations and structures to instil appropriate behaviours, monitor performance, and optimize realization of health value to the population*". The core healthcare regulatory schemes include the following:

- The Private Health Institutions Law issued by Royal Decree No. M/40 dated 3/11/1423H (the "***PHI Law***").
- The Implementing Regulations of PHI Law, issued by Ministerial Decree 683151 dated 10/3/1436H.
- The Implementing Regulations of Health Practice Law issued by Royal Decree No. M/59 dated 4/11/1426H.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The Personal Data Protection Law issued by Royal Decree (M/19) dated 16/9/2021G (the "***PDPL***") is intended to provide regulatory guidance on data protection in the Kingdom, which will come into effect by March 2023. The PDPL aims to protect: the use of personal data, particularly with respect to patient data processed through digital devices; access to health data; and security related to personal and sensitive information.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The Medical Devices Interim Regulation ("***Interim Regulation***") issued by the Saudi Food and Drug Authority ("***SFDA***") together with the Implementing Rules govern consumer health devices in the Kingdom (the "***Interim Regulatory Scheme***"). The Interim Regulation specifies the regulatory approach whereby only those medical devices that have been authorised by the SFDA are permitted to be placed on the Saudi market; it ensures organisations involved in importation and distribution activities are registered with the SFDA and that authorised representatives are acting on behalf of overseas manufacturers; and further specifies appropriate post-marketing surveillance activities.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The MoH and the SFDA are the overseeing authorities of the healthcare industry in the Kingdom. The MoH is the authority responsible for the management, financing and regulation of the healthcare sector in the KSA. It also undertakes the supervision and follow-up of healthcare-related activities carried out by the private sector.

The SFDA seeks to regulate, oversee and control food, drugs and medical devices, as well as to set mandatory standard specifications thereof, whether they are imported or locally manufactured. Additionally, the SFDA oversees consumers' awareness on all matters related to food, drugs and medical devices and all other products and supplies.

2.5 What are the key areas of enforcement when it comes to digital health?

The Law of Practicing Healthcare Professionals issued on 6/12/2005 provides the rules regarding practicing healthcare professionals in Saudi Arabia. The law provides for the requirements for licensing, duties and professional responsibility. It further imposes the applicable penalties for violations, issuance of warnings, fines and civil liability in the case patients claim damages for malpractice or breach of duty by the healthcare provider.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

As discussed in question 2.3 above, the Interim Regulatory Scheme specifies the procedures applicable to software as a medical device. The SFDA requires a medical device marketing authorisation for most devices placed in the Saudi market in accordance with the Guidance on Software as a Medical Device. The SFDA have further launched the Medical Devices National Registry ("***MDNR***") for the purpose of obtaining details of the KSA medical device industry and establishing a database of all establishments, manufacturers, agents and suppliers working in the field of medical devices.

2.7 What regulations apply to artificial intelligence/ machine learning powered digital health devices or software solutions and their approval for clinical use?

The Guidance on the Review and Approval of AI- and Big Data-based Medical Devices published by the SFDA provides context on software medical devices to which AI technologies are applied to predict, analyse and diagnose medical conditions. The Guidelines are implemented in conjunction with the SFDA's Guidelines on Software as a Medical Device and further stipulates the market authorisation requirements relevant to AI medical devices.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Some of the key issues with telemedicine are payment, misdiagnosis and widespread implementation. It is challenging to reimburse telemedicine services compared to those of in-person services. There is no guarantee of payment consistency between telemedicine and in-person healthcare. This could therefore defeat the purpose of telemedicine to reduce healthcare costs and expand access to service as it may discourage providers from offering telehealth because there is no guarantee of comparable payment.
  The risk of misdiagnosis increases with telemedicine as there is no clear standard of care established by legislation. Misdiagnosis may increase the overall costs of healthcare, contrary to what telemedicine aims to achieve, because misdiagnosis leads to incorrect prescriptions and treatments. Some of the responsibility of implementation resides with the legal system and rests with the government. Some are institutional and rest with local hospitals and healthcare institutions; other challenges could be financial.
  The challenges for implementing and adopting telemedicine in Saudi Arabia range depending on the type of healthcare facility ("***HCF***") as there are different facilities in the Saudi healthcare system belonging to different sectors (i.e. the MoH sector, military sector, private sector). Additionally, HCFs are located in different areas: some in urban; others in rural areas. These changes make the challenges to implementing telemedicine different for each facility, seeing as each HCF will have its own challenges, motivations and expectations, business needs, etc.
- **Robotics**
  Medical robotics are beneficial because of their ability to perform complex surgical operations, whether directly or indirectly, such as brain, open-heart and nerve surgeries through a remote robotic control system. Robotics have been used for a variety of medical purposes in the KSA. The use of robotics impacts privacy, autonomy (e.g., isolation), the possibilities of human augmentation and creates technical dependencies that can have the opposite effect of fostering learning and personal development (e.g. medicine without doctors).
- **Wearables**
  Wearable technology in healthcare includes electronic devices that consumers can wear, such as Fitbits and smartwatches, and are designed to collect the data of users' personal health and exercise. The issue associated with wearables is the potential sabotage of the devices themselves and the use of devices as a backdoor into networks and patient data. If wearables that monitor patient health and data are broken or stop working, this may create major issues for the patient relying on the wearable device, as inaccurate data from the wearables can have a negative consequence on the patient's health. Furthermore, lack of proper security may jeopardise the patient or user's security and data protection as well.
- **Virtual Assistants (e.g. Alexa)**
  The issues here are similar to those in AI, where issues such as data privacy and security are to be considered, as well as errors and variation in the quality of the assistance provided. Error in dictation, high costs, challenges of adoption among healthcare professionals, variation in the quality and security issues are the major factors that may hamper the growth of virtual assistants to a certain extent.
- **Mobile Apps**
  As stated in question 1.2 above, mobile applications are being utilised in Saudi Arabia for a number of goals and increasing efficiency. Some of the challenges associated with medical mobile apps in Saudi Arabia are data privacy and security and successful user experience, as well as technical challenges such as managing large data on the platform. Cloud integration and compatibility with older medical systems are additional challenges.
  Cloud adoption is the main technical challenge for application development in Saudi Arabia because of security concerns about Cloud platforms. Some Cloud-based storage databases cannot be properly secured when it comes to maintaining patient data and information. The upcoming data protection regulations will certainly help regulate and address these issues related to storing personal data.
  Furthermore, modern applications face the challenges of incompatibility with old hospital systems. Old systems are not compatible with advanced healthcare applications, making it difficult for these applications to provide services to hospitals and medical centres that still operate using old technology.
- **Software as a Medical Device**
  The same challenges apply for software as medical devices as with mobile applications. The safety and security of medical devices driven by software, the software-development processes and the need for data collection and privacy, all offer challenges and opportunities for device regulation and clinical care.
- **Clinical Decision Support Software**
  Clinical Decision Support Software ("***CDSS***") has been implemented into a variety of healthcare facilities to improve clinicians' diagnoses. Challenges that have been hindering the implementation of CDSS include resistance from clinicians and patients due to confidentiality and

privacy concerns. There are high costs and standards of care associated with the adoption and contentious maintenance required after implementing CDSS.

- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  The benefits of AI are that it can predict and diagnose disease at a faster rate than most medical professionals. The issues related to AI powered digital health solutions are in areas such as data security, patient privacy, legal liability and the challenges of applying AI tools in new contexts. Another challenge is the regulation of AI which has been enhanced in the recent years; however, regulators must continue to refine their role in legitimising and approving AI-driven tools.
- **IoT (Internet of Things) and Connected Devices**
  The main issues concerning the IoT and connected devices in healthcare are easing security concerns, data integrity by keeping the IoT hardware updated, technical issues such as maintaining connectivity, and the government regulating this technology.
- **3D Printing/Bioprinting**
  While 3D printing technology has boomed in recent years, the reliance and full dependence on the technology remains far from being achieved. This is because 3D printing is currently facing both technological and regulatory challenges when attempting to utilise it. With respect to the technological challenges of 3D printing, the most common barriers include (without limitation): (i) error control during designing; (ii) error control during implementation and post-implementation; and (iii) pre-processing and post-processing requirements with respect to the maintenance of the printed product.
  With respect to regulatory challenges, a very limited number of 3D printing materials have obtained the approval of the SFDA. As such, while materials are being manufactured, very little of said manufactured materials make it to the market due to the difficulties entities are facing in obtaining SFDA approvals.
- **Digital Therapeutics**
  Similar to the above, digital therapeutics raise concerns related to privacy and data protection. Considering that digital therapeutics may transfer personal information online, there are risks of unauthorised access.
- **Natural Language Processing**
  Natural language processing ("***NLP***") can be used for comprehending human speech and extracting its meaning, as well as unlocking data in databases and documents by mapping out essential concepts and values and allowing physicians to use this information for decision-making and analytics. However, one of the challenges in the application of NLP is adapting existing systems to new clinical settings. This is both time-consuming and requires significant effort. The technical challenges included in adapting the NLP system are related to assembling study subjects and interpreting diverse linguistic content. Failure to interpret linguistic content properly can result in inaccurate results or unsatisfactory assistance from the NLP.

3.2 What are the key issues for digital platform providers?

Pursuant to question 3.1 above, there are several issues associated, depending on the platform or digital service provided. Generally, the liability of the digital platform provider is at risk when any infringements are committed through such digital platforms and devices.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The key issues to consider for the use of personal data are confidentiality and security. There are a number of provisions in different Saudi laws which relate to the protection of personal information. The concept is enshrined in the Saudi Basic Law of Governance issued by Royal Decree No. A/91 dated 27/8/1412H. Additionally, the concept of confidentiality is preserved under *Sharia*, the source from which Saudi laws derive. Saudi law and *Sharia* cannot contradict one another. Furthermore, the Saudi Anti-Cyber Crime Law, E-Commerce Law and the Telecommunications Law further protect confidentiality of personal information.

Moreover, individuals are prohibited from disclosing confidential information which would jeopardise the safety and security of the country, as stated in the Penal Law on Dissemination and Disclosure of Confidential Documents and Information issued by Royal Decree No. 16913/B dated 10/5/1433. The Cloud Computing Regulatory Framework further governs data protection with respect to customers using Cloud service providers.

The PDPL, upon its enforcement, shall further stipulate administrative and criminal sanctions for the disclosure of personal data and breaches of restrictions on cross-border data transfers.

4.2 How do such considerations change depending on the nature of the entities involved?

If the entity involved is a judicial or legislative authority, then considerations for the use of personal data may be compromised.

4.3 Which key regulatory requirements apply?

The Law of Practicing Healthcare Professions, issued under Royal Decree No. M/59 dated 4/11/1426H (corresponding to 04/12/2005G) and its implementing regulations (the "***PHP Law***") further imposed an obligation on all health practitioners to protect patients' data that they become aware of, except, *inter alia*, where patients' written approval is secured. Failure to commit to such provision and to the confidentiality provisions will subject the violator to disciplinary penalties and a fine, not exceeding SAR 20,000.

The applicable regulations governing private health institutions in the Kingdom are the PHI Law and its Implementing Regulations. The PHI Law does not impose restrictions on storage registration or export of data. That said, consent of the patient to use, store and re-distribute the data of individuals will suffice for the purpose of the PHI Law.

Additional regulations include the Electronic Transactions Law issued under Royal Decree No. M/8 dated 26/3/2007G which regulates the exchange of electronic communication and criminalises the use of an individual's personal information, for purposes other than certification, without obtaining the written or electronic consent of the subject person.

Once the PDPL comes into effect, it will cover and address key regulatory aspects such as data controller obligations, data consent, data minimisation, and registration and maintenance of data records.

4.4 Do the regulations define the scope of data use?

The PDPL defines processing of personal data as "*any operation*

carried out on personal data by any means, whether manual or automated, including (without limitation) collecting, recording, sabing, indexing, organising, formatting, storing, modifying data".

4.5 What are the key contractual considerations?

The emerging contractual considerations include compliance with the Saudi anti-fraud regulations to minimise abuse and fraud risk. Further, due to the sensitive nature of patient data and information, the protection of privacy and confidentiality must be maintained when dealing with patient data, particularly with respect to obtaining consent and notifying the relevant authorities in the event of a data breach. Another key consideration is product liability, as software developers and device manufacturers must ensure that product defects do not result in injuries or misdiagnosis to patients.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

As mentioned under questions 4.1 and 4.3 above, the absence of a law for the purpose of securing the collection of data specifically has raised several concerns with respect to data protection. However, the current general framework is that confidentiality of sensitive data must be preserved. Despite the absence of laws regulating the collection of data, the MoH, along with the relevant hospital (government hospitals more specifically), tend to impose heavy restrictions on the collection of data in practice by prohibiting the transfer and maintenance of data outside the hospital's servers – said servers are expected to be kept in the hospital's premises only.

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

The PDPL will impose obligations with respect to data accuracy, adequacy and completeness of personal data prior to processing any information. In addition, the PDPL applies procedures to ensure that automated systems operate without any bias or discrimination, and a review and audit is generally required periodically. As such, breaching data accuracy or operating systems with bias and/or discrimination aspects may result in penalties or imprisonment depending on the violation.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

As explained in question 4.1 above, privacy and security are the key issues to consider when sharing personal data, which are regulated by the laws mentioned above. The consent to obtain confidential information must be clear.

5.2 How do such considerations change depending on the nature of the entities involved?

Generally, if the entities involved are police or judiciary, then there are instances demonstrated in Article 21 of the PHP Law where confidentiality of personal data may be jeopardised.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please refer to the responses provided under questions 4.1 and 4.3.

6 Intellectual Property

6.1 What is the scope of patent protection?

The scope and protection of patent protection is governed by the Patents, Layout Designs and Integrated Circuits, Plant Varieties and Industrial Models Law, issued under Royal Decree No. M/27 dated 17/7/2004. The scope of patent protection relates to a single invention or to a group of integrated parts that form a single invention concept.

Invention can include any new article, method of manufacture or improvement in either of them. Therefore, the invention can be a product or process, or both. Patent protection generally extends for 20 years from the date of filing.

6.2 What is the scope of copyright protection?

The scope of copyright protection is governed by the Saudi Copyright Law promulgated in 2003 by Royal Decree No. M/41. The scope covers works of authorship published, produced, performed or displayed for the first time in Saudi Arabia. This also extends to protect the works of Saudi authors only if conducted outside Saudi Arabia for the first time.

In addition, works of broadcasting organisations and producers, i.e. sound recordings and performers, are copyright protected. The Copyright Law also extends its protection to copyrighted works pursuant to international agreements or treaties relating to copyright protection the Kingdom is a party to. Duration of copyright under Saudi law varies from 50 years' protection to life protection depending on the type and ownership of copyright.

6.3 What is the scope of trade secret protection?

The scope of protection of trade secrets is prescribed in the Regulations for the Protection of Confidential Commercial Information issued by the Ministry of Commerce and Industry Decision No. 3218, in 2005, which vaguely defines trade secrets as information not known in its final form or where information is not easily obtainable by those who deal in the same type of business.

Such regulation also extends to protect information of commercial value so long as the rightful owner takes reasonable measures to maintain its confidentiality. It is important to note that these regulations do not provide for a limit on protection duration, except for information submitted to an official body or competent authority for the purpose of approval, i.e. the marketing of drugs or for chemical substances used in chemical agricultural products; in which case, a minimum protection period of five years will apply (subject to limited exceptions).

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

The Kingdom has established a strong communication and information technology network infrastructure, capable of providing all modern services and accommodating the high data flow resulting

from the use of these services and application. The Ministry of Education ("***MoE***") has been introducing technology to the education system for health reasons to minimise the heavy weight of books to children. The MoE is also heavily encouraging innovation in schools and the use of machine learning.

6.5 What is the scope of intellectual property protection for software as a medical device?

The scope of software protection has not been mentioned in the current IP laws in the Kingdom, nor are there any specific restrictions or requirements to protect software as a medical device. That said, the general rule is that, in the absence of applicable legislation, *Sharia* principles would apply. Under *Sharia* principles, software components and any unique algorithms will be protected so long as it can be proven to the adequate court in case of dispute and is consistent with *Sharia* public order and/or public morals.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

No, only natural persons may be regarded as an inventor of a patent in the Kingdom.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

There are no current rules or laws related to government-funded inventions in the Kingdom. We expect that this will be addressed pursuant to the newly launched Strategy.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

This is not common in Saudi Arabia as most collaborative efforts in research and developments currently take place overseas. However, from a legal standpoint, the parties should set out clearly what intellectual property, know-how and expertise they are contributing. In addition, the collaborators must agree on the ownership of the newly developed efforts and solutions by licensing the use of their existing intellectual property to the new efforts, which they can also agree on how to divide the revenue generated through said efforts.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

These are mostly in the form of non-disclosure agreements, licensing agreements and/or development agreements.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Pursuant to the Strategy, the goal is to utilise AI to monitor patients virtually from their home devices, and further send alerts to be sent for abnormal readings and possible actions to be recommended. The benefits of AI are that it can predict and diagnose disease at a faster rate than most medical professionals. It can further assist in reducing workloads, lowering costs and bettering outcomes in the delivery of administrative work, diagnosis and treatment. AI already aids physicians in robotic-assisted procedures by providing a suggested road map and warnings throughout the process.

8.2 How is training data licensed?

Training data is usually licensed by means of licensing agreements, if the owner of such data is authorised to disclose it to a third party.

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

This is currently being reviewed under the new Saudi Intellectual Property Authority, which was established pursuant to a Royal Decree at the end of 2017, to promote the benefits of intellectual property and to build an advanced economy based on knowledge. In such absence of applicable laws, the Kingdom will adhere to international agreements or treaties to which it is a signatory to, as well as to the *Sharia* principles.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The rights to licensing data for use in machine learning belong solely to the data owner; and such rights can be assigned or licensed with or without consideration. However, the granting of a licence does not prevent the data owner from utilising the data or from granting a licence on the same data to another person, unless otherwise restricted in the original licence agreement. The licensee may not assign the rights and privileges conferred on him, unless his ability to do so is expressly stipulated in the licence agreement.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Some of the key principles of liability are penal obligations on the unfair use of the data, not obtaining consent of the data owner, or a leak or sharing of such data without the data subject's consent.

9.2 What cross-border considerations are there?

When dealing with digital health on a cross-border basis, special consideration needs to be sought in relation to the applicable regulations that permits cross-border transfers of personal data. Following the recent amendments to the PDPL, entities must comply with the requirements of data localisation. Personal data may only be transferred abroad to a jurisdiction which ensures appropriate protection of the rights of individuals and personal data. The current grounds which permit transferring data outside of the KSA include transferring information on the

basis of performing an obligation of the data subject which can be interpreted as a contractual obligation in accordance with Article 28 of the PDPL.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

There is no current regulation that tackles this issue in particular; however, we anticipate key issues to be: the level of protection over the data shared in the Cloud; and the obligation of the Cloud/service provider and the digital city to protect such data.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

There are no existing regulations or rules that discuss this issue; however, we anticipate the following issues for non-healthcare companies: ownership and control over the data; software licence and application ownership; and rights to amend over them.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Key issues for venture capital and private equity firms to invest in healthcare providers would be in relation to the stability of the digital platform, size of the clients and scope of services provided to healthcare. Some of the key elements that a digital health start-up must not violate are the licensing and compliance requirements for the health services they seek to work with.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

With the "newness" of digital tools and solutions in the healthcare sector, said solutions could be considered as burdensome. The reasons are attributable to regulatory and technological challenges facing the industry. As mentioned above, the SFDA applies strict regulations in order to approve the materials used for the production of digital solutions. As such, hospitals and healthcare practitioners face difficulties in safeguarding compatibility with the issued medical and SFDA guidelines and, therefore, in obtaining the authorities' necessary approvals.

Moreover, there are five key barriers that must be tackled in order to ensure the widespread adoption of digital health solutions:

(i) Usability in order to satisfy the patients' needs and safety.
(ii) Costs in order to ensure economic benefits on both the producers and consumers.
(iii) Data security and privacy with respect to the use and collection of patients' data and to further ensure compliance with the applicable laws and regulations in relation thereto.
(iv) Accessibility and usability by healthcare practitioners.
(v) Time consumption – ability to generate digital solutions in a timely manner.

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?

Based on the barriers mentioned under question 10.4, it is evident that the requirement for accreditation may aid in accelerating obtaining the necessary approvals (and possibly funding) in order to produce tools and solutions to be used in the digital healthcare sector. Accreditation programmes further improve the quality, process and extent of care provided by healthcare practitioners and services towards patients while also improving the outcome of healthcare services.

As such, due to the number of benefits that accredited centres have to offer, obtaining endorsement from said institutions should be considered as a critical requirement for licensing a healthcare entity or approving the production of the digital tools and solutions offered by the healthcare centres and practitioners.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

It is important to note that the MoH have highlighted the impact and importance of digitisation in the healthcare industry and is seeking to constantly update the regulatory framework. Currently, there are no official announcements with respect to reimbursement for digital health solutions. However, it is expected that e-health will be included in insurance coverage by private and public bodies in the Kingdom.

10.7 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 following trends are likely to grow and impact digital health in the Kingdom:

- **Telehealth**
  The COVID-19 pandemic and the reduction of physical consultations resulted in the use of digital health technologies such as tablets, mobile phones and laptops which have been developed to facilitate more efficient healthcare services. This will impact digital health by reducing contact and providing remote urgent care for a variety of conditions.
- **Virtual and Augmented Reality**
  Augmented and virtual reality is developing to offer practical uses within the healthcare sector beyond entertainment. Various healthcare providers are starting to use virtual reality ("***VR***") for healthcare learning purposes such as training simulations. Training simulations provide healthcare practitioners and students with new opportunities to practice complex procedures in a safe and controlled environment.
- **Disease Management**
  The outcome of COVID-19 formed a need for healthcare facilities to swiftly respond and develop innovations in the healthcare industry. This rapid change will facilitate and encourage healthcare providers to treat and monitor patients outside of the traditional healthcare premises.

Suhaib Hammad joined Hammad & Al-Mehdar Law Firm in 2009. He earned his LL.B. from IIU Malaysia and his LL.M. from the University of Miami, specialising in International Business Law.
As a Partner, Suhaib leads the Commercial and Intellectual Property practice, focusing on ICT, TMT and Life Sciences. In addition, Suhaib was placed on secondment with the corporate and commercial team at Simmons & Simmons in their Dubai and London offices, and has worked on leading cross-border transactions. His experience includes advising major international telecoms and healthcare companies on Saudi regulations in relation to formation and operation. Suhaib was also awarded a Client Choice Award by *Lexology* for the year 2019.

Hammad & Al-Mehdar Law Firm
Fakhry Tower, L 8
Prince Saud Al Faisal St- Al Rawdah District, Jeddah
Saudi Arabia

Tel: +966 920 004 626
Email: suhaib.hammad@hmco.com.sa
URL: www.hmco.com.sa

Ebaa Tounesi is an associate who completed his LL.B. with first-class distinction and obtained his LL.M. in Corporate and Commercial Law at the University of Southampton with merit. Ebaa is a qualified attorney in Saudi Arabia and has been part of the Corporate and Commercial team at Hammad & Al-Mehdar since July 2019. Ebaa's expertise includes working on various commercial agreements, advising on and implementing corporate restructuring, dealing with multinational joint ventures and shareholders' agreements, and working on several M&A transactions while further advising several healthcare companies in Saudi Arabia.

Hammad & Al-Mehdar Law Firm
Fakhry Tower, L 8
Prince Saud Al Faisal St- Al Rawdah District, Jeddah
Saudi Arabia

Tel: +966 920 004 626
Email: ebaa.tounesi@hmco.com.sa
URL: www.hmco.com.sa

Hammad & Al-Mehdar Law Firm was founded in 1983 in Jeddah, Saudi Arabia, and has grown to become a prominent private practice Saudi firm in the Kingdom and the GCC. The law firm boasts a leading local presence supported by international capabilities.
Hammad & Al-Mehdar provides a full suite of business and corporate legal services in all major areas of Saudi law, working on cutting-edge, complex and high-value transactions and disputes.
Headquartered in Jeddah, Hammad & Al-Mehdar's growth story is one of trade, innovation and technology in the Kingdom's private sector. Hammad & Al-Mehdar maintains a strong specialisation in servicing privately held businesses, with unrivalled expertise in business and transaction structuring, private construction works, commercial, intellectual property, corporate governance and regulatory advisory services.

The firm was recognised as the best Mergers & Acquisitions law firm for the years 2017 and 2018 by the IFN Law Awards, and has been honourably mentioned as a Tier 1 Firm in *The Legal 500 2017* for Banking & Finance Transactions.

www.hmco.com.sa

HAMMAD & AL-MEHDAR
LAW FIRM

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 technologies in your jurisdiction?

The key emerging digital health technologies in Singapore are presently in the areas of artificial intelligence ("**AI**"), telemedicine, mobile health, data analytics and digitised and integrated healthcare systems. The Ministry of Health ("**MOH**"), amongst others, has recognised that AI is increasingly being used throughout the healthcare continuum in training, research, administration, clinical decision support and direct patient care.

Additionally, with the onset of the COVID-19 pandemic, platforms for teleconsultation and telemonitoring have come to the fore. There is increased integration of telemedicine into the national health management system to allow for improved patient management and reduced hospital visits and re-admissions. Patients have also become more familiar and adept at using digital health services, for example, teleconsulting with private general practitioners for minor ailments to avoid overloading clinics and accident and emergency departments, or using health apps for booking appointments or vaccination slots.

In mobile health, mobile applications and wearable devices are used to monitor health statistics and wellbeing, and are used in conjunction with data analytic technology to identify trends and clusters based on proximity data (for example, the Trace Together mobile application / token developed for the COVID-19 pandemic).

Platforms for digitised and integrated health systems (such as the National Electronic Health Record and the Health Hub mobile application) are also being implemented to facilitate the consolidation, digital management and sharing of patient's information and records across both the public and private sectors, to increase individuals' ease of access to the healthcare system.

1.3 What are the core legal issues in digital health for your jurisdiction?

The emergence of telemedicine as an increasingly popular way of delivering healthcare creates a need for regulation. At this time, telemedicine is mainly regulated by the National Telemedicine Guidelines (January 2015), and the Singapore Medical Council's ("**SMC**") Ethical Code and Ethical Guidelines (2016) ("**ECEG**") (amongst other *ad hoc* guidelines / advisories by various regulatory and professional bodies). Following a "regulatory sandbox" period for telemedicine and mobile medicine in which the MOH sought to better understand the risks of these service delivery models and co-create corresponding risk mitigation measures with the healthcare industry, and with the Healthcare Services Act 2020 ("**HCSA**") recently coming into force on 3 January 2022, the MOH plans to expand the scope of healthcare services regulation under the HCSA in phases. A statutory scheme for regulation of telemedicine is presently anticipated to come into force at about the end of 2023, and the planned licensable providers will be independent doctors and / or dentists offering teleconsultations themselves, as well as organisations which have set up clinical and operational governance for their doctors and / or dentists to provide teleconsultations. At this time, telemedicine is not anticipated to be a separate category of licensable healthcare services, but regulatory requirements will be imposed on licensees approved to provide these services. Until then, the MOH has published a list of such direct telemedicine service providers who have demonstrated awareness of the risks and benefits of telemedicine, have put in place measures to address the risks, and agreed to comply with the practice guidelines set out by the MOH. Indirect telemedicine providers (i.e. those who do not provide direct medical care, and only offer technology support such as platforms offering software-as-a-service for teleconsultation, directory listings, and payment solutions) will not be licensed.

Increasing development and marketing of digital health products and standalone software (i.e. software that is intended to function by itself, rather than to control or affect the operation of other hardware medical devices, also commonly known as "Software as a Medical Device" or "SaMD" in the context of the International Medical Device Regulators Forum ("**IMDRF**")) is also likely to raise issues of registration and licensing, specifically, an increased need to determine if digital health products and associated dealer activities require registration and licensing as a medical device under the Health Products Act 2007 ("**HPA**"), as well as the applicable risk classification (which in turn determines the applicable registration requirements). At this time, not all

telehealth products are considered medical devices; for example, under the HSA's Regulatory Guideline for Telehealth Products (April 2019), wellness devices such as fitness trackers, with appropriate clarification statements as to the product's appropriate use, may be exempt from regulation as a medical device notwithstanding that their functions are in the nature of telemonitoring.

Within the existing regulatory regimes, there are also unique challenges posed by specific types of technology, such as AI / Machine Learning ("**ML**") and SaMD. The relevant regulators have begun to issue specialised guidelines, such as the Artificial Intelligence in Healthcare Guidelines (October 2021) ("**AIHGle**"), and the Guidelines on Risk Classification of Standalone Medical Mobile Applications and Qualification of Clinical Decision Support Software being issued (April 2022).

With increasing healthcare data stored and transmitted digitally, the security of patients' medical and health information is also of significant concern. Recent years have seen data breaches involving large amounts of confidential patient information, and fines totalling S$1 million being meted out by the Personal Data Protection Commission ("**PDPC**") to a healthcare provider and its information technology services provider.

Increased possibilities for healthcare to be delivered cross-jurisdictionally raises both jurisdictional and conflict of laws issues. The advent of electronic, consolidated patient information also raises questions as to the standards to which healthcare professions (in particular, public healthcare workers operating under time-poor conditions and in a team-based setting) ought to be held to when it comes to documentation.

1.4 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 reported that the revenue generated by the digital health market in Singapore in 2022 was US$525.70 million. Revenue in the digital health market in Singapore is projected to reach US$637.70 million in 2023.

1.5 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.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core healthcare regulatory schemes related to digital health in Singapore can be generally divided into regulation of digital health devices, healthcare service providers and healthcare professionals.

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 to regulate the import, manufacture, export and supply of medical devices in Singapore, and ensure 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.

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, providing health-related information and raising the general public's awareness on health issues. The regulatory regime for healthcare services is currently in a transitory state, moving from the incumbent premise-based system under the Private Hospitals and Medical Clinics Act 1980 ("**PHMCA**"), to the service-based system under the HCSA. The first phase of implementation under the HCSA commenced on 3 January 2022, and full implementation is currently expected by the end of 2023, likely alongside the repeal of the PHMCA. In addition, the national standards body, Enterprise Singapore, administers the Singapore Standardisation Programme through an industry-led Singapore Standards Council, whose standards cover new medical technologies, systems and processes, including telemedicine, personal care robots and medical devices.

For further details as to the regulatory regime for telemedicine in particular, please see the response to question 1.3.

Finally, the healthcare professionals involved in the supply of digital healthcare are each regulated by their respective professional bodies. To name a few: doctors are regulated by the SMC under the Medical Registration Act 1997; nurses are regulated by the Singapore Nursing Board ("**SNB**") under the Nurses and Midwives Act 1999; and allied health professionals (such as physiotherapists) are regulated by the Allied Health Professions Council ("**AHPC**") under the Allied Health Professions Act 2011. Each professional body also typically promulgates its own code of ethics and / or ethical guidelines.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Other applicable core regulatory schemes include the personal data protection regime administered by the PDPC under the Personal Data Protection Act 2012 ("**PDPA**") and its subsidiary legislation (including the PDPC's Advisory Guidelines for the Healthcare Sector).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Medical devices (including software) for use by consumers are regulated under the HPA regime (overseen by the HSA) described in the response to question 2.1. Whilst consumer devices are not subject to a special regime of their own, the specific registration requirements that apply to a medical device can vary depending on the risk classification assigned to the device. Medical devices meant for consumer use are generally expected to be of lower risk and would generally be subject to less stringent requirements. For example, consumer medical devices may be Class A (i.e. low-risk) devices and exempt from product registration.

There are also various general (non-health product-specific) regimes for the protection of consumers in Singapore, which would generally apply to consumers who purchase or use such consumer devices. For example, the Competition and Consumer Commission of Singapore administers the Consumer Protection (Fair Trading) Act 2003, which protects consumers from

unfair practices by commercial suppliers (which would include suppliers of digital health devices). Consumers also generally have recourse to civil remedies against such suppliers under contract and tort law, and legislation such as the Unfair Contract Terms Act 1977 grant certain special protections to consumers, such as requiring the commercial supplier's standard terms of business limiting liability for breach to be reasonable before such terms will be valid against consumers.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

Please see the response to question 2.1.

2.5 What are the key areas of enforcement when it comes to digital health?

The key areas of enforcement would generally mirror the areas of regulation in respect of medical devices, healthcare services and healthcare professionals, including registration, dealer's licensing, quality control, advertising, post-market obligations of record keeping and reporting, and the security of patients' medical and health information.

2.6 What regulations 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 described in the response to question 2.1. Such software includes software embedded in medical devices, standalone software (also known as 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, licensing 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 the Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (April 2022) and the Regulatory Guideline for Telehealth Products (April 2019). The HSA has also recently issued Guidelines for Classification of Standalone Medical Mobile Applications (SaMD) and Qualification of Clinical Decision Support Software ("**CDSS**") in April 2022, with the aims of harmonising the HSA's approach in determining the risk classification of SaMD with the IMDRF's guidance on SaMD and providing better clarity on the qualification of CDSS as medical devices.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Where AI / ML powered digital health devices or software solutions fall within the definition of a medical device, these are generally regulated under the HPA regime described in the response to question 2.1. Particular guidelines have also been promulgated by the HSA which are relevant to AI medical devices, including Part 8 of the Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (April 2022) and the AIHGle. Policymakers and regulators in Singapore have also articulated a technology- and sector-agnostic AI governance approach to the design, application and use of AI, known as the Model Artificial Intelligence Governance Framework (2nd ed., January 2020).

3 Digital Health Technologies

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

The following paragraph relates to the following technologies: robotics; wearables; virtual assistants (e.g. Alexa); mobile apps; SaMD; CDSS; AI / ML powered digital health solutions; Internet of Things ("**IoT**") and Connected Devices; 3D printing / bioprinting; digital therapeutics; 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 impact on registration and licensing requirements); (ii) data protection and security; and (iii) maintaining standards of healthcare that are comparable to traditional modes of delivery. Technologies which involve AI / ML and continuous learning capabilities, in particular, raise issues of post-market monitoring to ensure that learning does not compromise performance post-deployment.

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 issues for digital platform providers?

Please see the response to question 3.1.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Key issues to be considered 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 for which personal data of users will be put to (beyond providing the service or product to users), for example, whether the personal data will be used for health / clinical research by a third party.

4.2 How do such considerations change depending on the nature of the entities 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.

4.3 Which key regulatory requirements apply?

The collection, use and disclosure of personal data must be in accordance with the personal data protection regime in Singapore. The PDPA, its subsidiary legislation and guidelines (including Advisory Guidelines for the Healthcare Sector) issued by the PDPC, comprise the relevant regime for personal data protection in healthcare. The collection, use and disclosure of personal data must be with the consent of individuals (unless an exception applies) and for purposes that individuals have been notified of and a reasonable person would consider appropriate in the circumstances. Organisations must:

- permit individuals to obtain information on their personal data and the ways in which their personal data has been used within a year before the date of request and to correct their personal data;
- ensure that personal data of individuals is correct and complete;
- put reasonable security arrangements in place to protect personal data;
- ensure that personal data transferred outside of Singapore is subject to a standard of protection comparable under the PDPA; and
- notify the PDPC of data breaches in certain circumstances.

Under the Private Hospitals and Medical Clinics Regulations and the Revised Guidelines for Retention Periods of Medical Records (July 2022), there are also legal obligations regarding the retention of medical records.

The Healthcare Services (General Regulations) 2021 impose obligations on licensed healthcare service providers to:

- ensure that equipment used for the provision of licensed healthcare services that hold data are secured against unauthorised access, interference and tampering; the data held in the equipment is protected from unauthorised local or remote electronic access by implementing appropriate security measures; and data held in the equipment is securely transmitted to authorised recipients;
- maintain accurate, complete and up-to-date patient health records; and
- maintain the confidentiality, integrity and security of patient health records.

For digital health solutions that are regulated as medical devices, the Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (April 2022) include requirements for managing cybersecurity risks (where applicable).

4.4 Do the regulations define the scope of data use?

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 What are the key contractual considerations?

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, this should be considered when entering into / preparing the relevant contract.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Consent for purposes beyond that which is necessary to provide the service or product to users and which may not be considered appropriate by a reasonable person is one such key legal issue. Users need to be notified of these purposes and consent needs to be obtained (unless an exception applies) for these purposes, which may not be forthcoming from users. It is not permissible under the PDPA regime to require users to provide personal data beyond that which is reasonable for providing the service or product as a condition for providing the service or product. It bears noting that provided the above requirements are complied with, relying on consent for compliance with data protection requirements is fairly common.

4.7 How are issues with 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. 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.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 must be complied with. Please see the response to question 5.3.

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 do such considerations change depending on the nature of the entities involved?

The considerations change if an entity is a data intermediary. Please see the response to question 4.2.

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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The purposes for which the personal data is shared must be notified and consented to by individuals. If the personal data will be shared with a recipient outside of Singapore, the transferring entity must ensure that the recipient protects the personal data with a standard of protection comparable to that under the PDPA. Please see the response to question 4.5 on relying on contractual terms in transferring data overseas.

6 Intellectual Property

6.1 What is the scope of patent protection?

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 said computer (or other technical) features, as defined in the claims, is 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.

6.2 What is the scope of copyright protection?

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 What is the scope of trade secret protection?

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 which 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 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 What is 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?

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 are the core rules or laws related to government funded inventions in your jurisdiction?

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.

7 Commercial Agreements

7.1 What considerations apply to 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.

7.2 What considerations apply in 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).

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

ML (and AI, more generally), when incorporated successfully into clinical workflows, can play roles in:

- enhancing communications (e.g. through natural language processing with foreign patients);
- improving efficiency, accessibility, quality of diagnosis and triage (e.g. through pattern recognition of radiological images); and
- improving recommendations on interventions (e.g. through the accumulation and analysis of data tuned to the local population and context, which in turn enables more accurate prediction of health risks and outcomes).

8.2 How is training data licensed?

Training data is typically provided by one party to another under contract. The terms vary between parties and the nature of the projects or purposes for which the training data is licensed. Training data may be protectable by copyright as a compilation; however, no copyright subsists in the data itself. There is no *sui generis* database right in Singapore. Parties commonly rely on contractual obligations (including obligations of confidentiality) to control use of training data.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 considerations apply to licensing data for use in machine learning?

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.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

In Singapore, 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 amount to 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.

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 responses to question 3.1, and sections 4 and 5.

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, including as a response to the challenges posed by the

COVID-19 pandemic. 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.

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. This is more likely to be influenced by the prevailing government policies (and the work of bodies as such the Smart Nation and Digital Government Office, and its implementing arm, the Government Technology Agency), as well as sentiments of healthcare professionals and the public, and practical issues such as the costs of implementation.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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. For example, the MOH has published a Table of Surgical Procedures, which lists microsurgical reversal of sterilisation by robotic means as a procedure in respect of which claims under MediShield Life (a basic health insurance plan administered by the Central Provident Fund Board) may (up to certain maximum claim limits) be made. 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 for between the insured and insurer.

10.7 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.

Following the COVID-19 pandemic, apart from public and private hospitals, community healthcare providers including general practitioners, specialist clinics and nursing homes have been recognised as a critical pillar of the healthcare system. Given various trends, such as an ageing population, an increased focus will be shifted towards primary care to prevent illness, including increasing the support for private general practitioners. In order to facilitate greater integration of the healthcare ecosystem, the Health Information Bill is planned to be introduced this year, to require licensed healthcare providers (including private providers) to input patients' medical records into the National Electronic Health Record ("**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.

From a legal perspective, 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. Adequate safeguards will need to be considered and implemented. How the law attributes responsibility and liability for breaches will be closely examined. Patient preferences, including, for example, the choice and extent thereto to restrict the sharing of their data in the NEHR, will also have to be considered.

Acknowledgments

The authors would like to thank Claris Ng, Associate, and Sophia Eliza Rossman, Associate, at Allen & Gledhill LLP, for their valuable assistance in the preparation of this chapter.

Gloria Goh's areas of expertise are in intellectual property, technology and pharmaceuticals, health products, cosmetics and food regulation. Her practice involves 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 intellectual property due diligence in corporate transactions, conducting intellectual property audits for clients, advising clients on the acquisition of intellectual property and drafting and negotiating commercial agreements relating to the acquisition of intellectual property.

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7568
Email: gloria.goh@allenandgledhill.com
URL: www.allenandgledhill.com

Koh En Ying specialises in litigation and dispute resolution, with a focus on medical malpractice and construction disputes. In relation to the former, she regularly deals with medical negligence claims, disciplinary proceedings and coroner's inquiries, and has advised and represented a medico-legal defence organisation, insurers, healthcare professionals and hospitals in matters across a range of general and specialist medical practices. Her practice also includes advising on medical regulatory issues, such as the regulation of healthcare professionals, healthcare service providers and health products, including, where relevant, to operational matters and corporate transactions.

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7507
Email: koh.enying@allenandgledhill.com
URL: www.allenandgledhill.com

Tham Hsu Hsien's main areas of practice are in healthcare and professional indemnity, banking and employment litigation, and insolvency and restructuring. In the area of healthcare and professional indemnity, he advises professional indemnifiers, insurers and healthcare providers on regulatory and litigation matters. His contentious practice includes medical malpractice litigation and disciplinary proceedings. His non-contentious practice includes advising on regulatory and contractual issues, and on localisation of insurance policies.
He regularly contributes to healthcare industry education and healthcare legislation consultations. He is an appointed member of the Ministry of Health's National Transplant Ethics Panel of Laypersons and is a faculty member of the Singapore Medical Association's Centre for Medical Ethics and Professionalism.

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7820
Email: tham.hsuhsien@allenandgledhill.com
URL: www.allenandgledhill.com

Alexander Yap is Co-Head of the FinTech Practice at Allen & Gledhill. He focuses on the acquisition, divestiture, provision, sharing and receipt of technology and intellectual property-related assets, data and services. He also advises on intellectual property licensing, R&D and sponsorship arrangements, cybersecurity, collaboration agreements, outsourcing, distribution and franchising, online gaming, the Cloud and "as-a-service" platforms, and is a key contact for data protection and privacy compliance matters and data breach management. Alexander was recommended for his expertise in intellectual property work by *The Legal 500 Asia Pacific 2019* which notes him as "a key name for commercial transactions relating to intellectual property, information technology and the protection and management of data".

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989

Tel: +65 6890 7627
Email: alexander.yap@allenandgledhill.com
URL: www.allenandgledhill.com

Allen & Gledhill is an award-winning full-service South-east Asian law firm providing legal services to a wide range of premier clients, including local and multinational corporations and financial institutions. The Firm is consistently ranked as a market leader in Singapore and South-east Asia, 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 strong rankings in leading publications, and by various awards and accolades. With a growing network of associate firms and offices, it is well-placed to advise clients on their business interests in Singapore and beyond, on matters involving South-east Asia and the Asian region. With its offices in Singapore, Myanmar and Vietnam, as well as its associate firm in Malaysia (Rahmat Lim & Partners), and its network firm in Indonesia, Soemadipradja & Taher, Allen & Gledhill has over 650 lawyers in its network across the region, making it one of the largest law firms in South-east Asia.

www.allenandgledhill.com

ALLEN & GLEDHILL

Spain


Montserrat Llopart Vidal


Javier Saladich Nebot

Baker McKenzie

1 Digital Health

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

There is no formal or legal definition of digital health in Spain. According to the *Fundación Tecnología y Salud*, a foundation set up by the Spanish Federation of Healthcare Technology Companies (FENIN), digital health refers to the set of Information and Communication Technologies used in a medical setting in areas related to the prevention, diagnosis, treatment, monitoring and management of health, acting as an agent of change that enables cost savings and improves efficiency.

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

Telehealth is increasingly taking hold and making interactive, real-time communication between patients and healthcare professionals commonplace, avoiding the need for face-to-face medical visits. In Spain, all interested stakeholders are investing in this area: the national health service, private insurance companies and telecommunications companies that partner with established telehealth providers.

Furthermore, the shift from treatment to prevention in healthcare and the rise of patient-centric solutions has boosted innovation in the field of digital health and wellness monitoring, with the development of a wide array of health apps and mobile and wearable devices.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues are data privacy, quality of data, cybersecurity and the interoperability of IT systems as well as IP rights. Regulatory issues (product classification as medical device) and financing are also key for the development of digital health.

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

The pharmaceutical industry in Spain exceeded 17,000 million euros in medicines exports in 2021. There is no data on the digital health market size for Spain.

The SEIS index, created by the Spanish Society of Health Informatics in collaboration with the Ministry of Health and the public entity Red.Es, evaluates and quantifies the implementation of Information and Communication Technologies (ICTs) in the Spanish public health system. Data from 2021 shows that the overall expenditure on technology platforms and information systems increased by 7.69% and 10.29% respectively in comparison to 2020. It also shows that tele-dermatology, tele-ictus and tele-ophthalmology are among those telemedicine specialities with the most initiatives. Finally, some of the most prioritised ICT projects undergoing implementation relate to data analysis and knowledge generation, health personnel channels, electronic health records, health portals and production of population-based information to support clinical decision making.

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

The Spanish digital healthcare market is characterised by a high fragmentation of its operators, consisting of three main groups: start-ups; pharmaceutical companies with digital health initiatives; and ICT/technology companies investing in digital health or partnering with healthcare players.

The market is rapidly changing with the entrance of new start-ups. The most relevant private equity funding company in digital health for 2021 was Koa Health (which closed a 30-million-euro financing round), which is a start-up that offers digital solutions for mental wellbeing based on scientific evidence around behavioural therapy.

Other start-ups and pharmaceutical companies, such as MedLumics, Inbrain Neuroelectronics, Top Doctors or Overture Life, have also closed financing rounds of between 12.5 million euros and 18 million euros to further develop and implement digital health solutions.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Spain does not have specific legislation relating to digital health, but the following schemes apply:

- Royal Legislative Decree 1/2015, approving the revised text of Law 29/2006 on Guarantees and the Rational Use of Medicines and Medical Devices.
- Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices.
- Royal Decree 1591/2009 on medical devices; Royal Decree 1616/2009 on active implantable medical devices; Royal

Decree 1662/2000 on *in vitro* diagnostic medical devices (currently all of these are under review to adapt them to the above EU Regulations).
- Law 34/1988 on Advertising.
- Law 3/1991 on Unfair Competition.
- Guide for Advertising of Medical Devices to the General Public of the Catalonia region – January 2017, fourth edition.
- Code of Ethics of the Spanish Board of Medical Associations (OMC).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The following regulatory schemes apply to digital health in Spain:
- The General Data Protection Regulation (EU) 2016/679 (GDPR).
- Organic Law 3/2018 of 5 December on Data Protection and Guarantee of Digital Rights.
- Law 34/2002 on Information society services and electronic commerce.
- Royal Decree 3/2010 regulating the National Security Framework in the field of e-government.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The following regulatory schemes apply to consumer healthcare devices/software in Spain:
- Royal Legislative Decree 1/2007 approving the revised text of the general law for the protection of consumers and users (GLPCU).
- Royal Decree 1801/2003 on general product safety.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The Ministry of Health is responsible for the financing of medical devices and establishes the framework for the provision of health services. It is also responsible for consumer protection legislation. The Spanish Agency for Medicines and Medical Devices, attached to the Ministry of Health, supervises the whole lifecycle of medical devices.

The regional authorities are responsible for the provision of healthcare services, supervision of promotional activities, enforcement of consumer protection and market surveillance in general.

The Spanish Data Protection Agency is the national supervisory authority under the GDPR and ensures that data privacy principles and regulations are respected.

The OMC is responsible for supervising doctors, including telemedicine practices.

2.5 What are the key areas of enforcement when it comes to digital health?

The key areas of enforcement for digital health in Spain are the following:
- Regulatory authorities' actions against digital health and healthcare IT that meet the definition of medical devices but have not obtained the CE mark.
- The Spanish Data Protection Agency's actions in the event of breaches of data protection legislation and data security.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software that qualifies as a medical device must follow the provisions relating to medical devices, which vary depending on the kind of medical device.

EU Regulation 2017/745 and EU Regulation 2017/746 apply. At Spanish level: Royal Decree 1591/2009; Royal Decree 1616/2009; and Royal Decree 1662/2000 apply (currently all of them are under review to adapt them to the above EU Regulations).

The European Commission has issued guidelines on the classification of medical devices and, in particular, on the Qualification and Classification of stand-alone software used in healthcare (MDCG 2019-11).

Digital solutions to be adopted by the national health service are checked to ensure that the security standards required for the public administration are met.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Artificial Intelligence (AI) in healthcare is mainly regulated by the EU Medical Devices Regulation 2017/745 (MDR) and *In-vitro* Diagnostic Medical Devices Regulation 2017/746 (IVDR) in combination with the GDPR. Medical devices are often either developed using AI or they have an AI component. The GDPR applies since the application of AI implies the collection or treatment of data, and, specifically health data, which is considered as special-category data and is subject to strict privacy and data protection obligations. The MDR and IVDR contain both *ex ante* and *ex post* requirements for AI in healthcare to be safe and performant throughout their entire lifecycle.

Moreover, Ethics Guidelines for Trustworthy AI, published by the European Commission (2019) highlighted that AI applications should not only be consistent with the law, but they must also adhere to ethical principles and ensure their implementations avoid unintended harm.

On a European level, the EU has presented a Proposal for Regulation, laying down harmonised rules on AI (the AI Act), that will impact medical device and diagnostic companies. Regulation classifies medical devices and *in vitro* diagnostics as high-risk AI systems, therefore those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the EU market. Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle. The importance of this Regulation also lies in the fines for non-compliance, some of them up to 30 million euros or up to 6% of the total worldwide annual turnover for the preceding financial year.

In Spain, following the European scheme, the applicable legislation would be the Royal Decrees regulating medical devices, implantable medical devices and *in vitro* diagnostic medical devices, as well as Organic Law 3/2018 on the Protection of Personal Data.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  There is no specific telemedicine regulation in Spain. The regulatory loophole was a problem in itself because the legislation governing healthcare professions refers this issue to the medical profession's deontological rules and the Code of Ethics of the OMC does not allow telemedicine, unless ancillary to face-to-face medical consultation. Privacy is another important concern, especially consent, data minimisation and data security.
  As for virtual care, covering both clinical and non-clinical applications, key issues relate to privacy and cybersecurity.
- **Robotics**
  The core issues are product qualification, security, cross-border remote control and liability. Avoiding the risk of hacking is critical. Cross-border remote control raises issues relating to differences in the qualifications of the persons located outside of Spain controlling robotic devices. Finally, it may become difficult to determine whether product defects or incorrect use are to blame when loss or damage occurs.
- **Wearables**
  The core issues are the reliability of data, privacy concerns and data security. To the extent that an app tracks medical conditions, product qualification and liability issues may also arise.
- **Virtual Assistants (e.g. Alexa)**
  The core issues are first data security and the risk of cyber-attacks and then the reliability of data, together with privacy concerns. Additional concerns relate to the illegal non-licensed practice of medicine if enforcement authorities consider that the virtual assistant is giving medical advice.
- **Mobile Apps**
  The same issues apply as for wearables – see above.
- **Software as a Medical Device**
  Software that will meet the definition of medical devices needs to be developed according to the requirements set out in medical device regulations in order to obtain the CE mark.
- **Clinical Decision Support Software**
  The core issues are lack of interoperability between different systems and the difficulty to pool information from many and diverse clinical sources. Moreover, product classification and privacy issues.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Product qualification and liability issues in the event that the algorithm fails and triggers a faulty clinical decision. In addition, in contradictory situations or where there is a lack of interpretation, an algorithm may not work properly. As long as the product liability framework is not amended, the chances to find a developer of a standalone software liable for a defective product are limited. In this regard, the new European Commission Proposal for regulating the liability of AI systems is still at a premature stage.
- **IoT (Internet of Things) and Connected Devices**
  The core issues are cyberattacks, data security, the value and reliability of the data obtained and privacy issues. Interoperability with healthcare providers' IT systems also needs to be addressed.
  Virtual reality, augmented reality and mixed reality, with their potential for treating patients and affecting their behaviour, may pose additional security and regulatory issues.
- **3D Printing/Bioprinting**
  The core issue is product qualification of the resulting product. The collection of biological samples intended to be used for 3D printing/bioprinting in the framework of biomedical research is subject to Law 14/2007, especially with regard to informed consent, confidentiality and personal data protection. In addition, liability issues could arise with regard to implanted bio-artificial organs or tissues.
- **Digital Therapeutics**
  Sound evidence of performance and clinical evidence is key for digital therapeutics (DTx) to receive conformity assessment under the MDR. Furthermore, risks pertaining to data protection refer to the profiling of patients and the serious security threats and major consequences in the event of a data breach.
- **Natural Language Processing**
  The core issue is the existence of various official languages in Spain, some spoken by small populations. Availability of digital health technologies in several of those languages may be key to their adoption by Spanish regional healthcare authorities.

3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are as follows:

- Interoperability of digital platforms with apps, wearables, Internet of Things (IoT), medical devices and other digital healthcare technologies without compromising the integrity of the platforms.
- Market access issues due to the need for validation before connecting with public healthcare IT systems.
- Business models that favour the creation of value and potential savings for healthcare providers and sustainable financing models.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The main issue to consider is that genetic data, biometric data uniquely identifying natural persons, and health data are considered to be special categories of personal data (art. 9 of the GDPR) and that the GPDR prohibits the processing of special categories of personal data. However, there are some exceptions, such as the explicit consent of the data subject.

The first step when using personal health-related data is to clearly define for which purposes the personal data will be used, in order to check if any of the exceptions foreseen in art. 9 of the GDPR apply and to be compliant with the transparency principle. In this regard, the most commonly used exception is to obtain the explicit consent of the data subject to process personal data concerning health, without such personal data being collected for a purpose other than that for which the data subject gave their consent.

Operators shall limit the purposes for which personal data is collected and provide transparent and granular information on how and by whom personal data is going to be processed.

Extending the types of processing in the future to purposes not foreseen at the outset or that could have appeared with the evolution of the market may not be compliant with the transparency principles of the GDPR, and the obligations of privacy by design and should be avoided.

4.2 How do such considerations change depending on the nature of the entities involved?

When the controller is a private entity, the legal basis required to process personal data relating to health is usually the consent of the data subject. In case of public authorities, there are certain circumstances under which they do not need the consent of the data subject in order to process his or her personal data.

In this regard, the Spanish Data Protection Agency has recognised that public authorities, unlike individuals, may process personal health data without the consent of the data subjects, if it is necessary for the performance of a task carried out in the public interest or in the exercise of public authority and as long as it has a competence conferred by law.

However, personal data protection regulations must be complied with at all times and the data must be limited to that which is strictly necessary for the intended purpose.

4.3 Which key regulatory requirements apply?

When using personal health-related data, appropriate safeguards are required. These include, for example: (i) correctly identifying the purposes for which the personal data is going to be processed and only processing personal data that is strictly necessary for the identified purposes (data minimisation); (ii) applying the privacy-by-default and privacy-by-design principles; (iii) conducting a privacy impact assessment and analysis of the risks for the rights and freedoms of the data subjects prior to the processing of data; (iv) guaranteeing the confidentiality, integrity and availability of the personal data processed; (v) anonymising personal data or, at least, pseudonymising the same and prohibiting third parties with whom personal data may be shared from reverting the pseudonymised data; (vi) obtaining separate consent for each purpose; (vii) providing clear information to data subjects, using plain language and providing information about the identity of the data controller, and specifying whether personal data is shared and with whom and if it will be re-used and for which purposes; (viii) designing user-friendly settings options, so that data subjects can easily decide whether they want to share personal data or not; and lastly (ix) taking into account that profiling is only permitted under very specific circumstances and, if done, explicit consent of the data subject needs to be obtained.

Pursuant to art. 37 of the GDPR, the controller and the processor shall designate a data protection officer in the following events, *inter alia*: if the processing is carried out by a public authority or body; or if core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to art. 9 (e.g. data concerning health). Under Spanish data protection legislation (art. 34), in addition to the circumstances foreseen in the GDPR, there are some entities that shall designate in any case a data protection officer, such as: entities operating networks and providing communications services when dealing with habitual and systematically personal data on a large scale; or healthcare centres legally required to maintain patients. Digital health providers should generally process personal health data on a large scale, and therefore they will be obliged to designate a data protection officer.

In addition to the above, other regulatory requirements which stem from the treatment of personal health data are the following: (i) regardless of the size of the entity, the controller, or, if applicable, the processor who processes health data on behalf of the controller, shall keep a record of processing activities pursuant to art. 30 of the GDPR; and (ii) by default, when there is large-scale processing of health data, the controller shall carry out a data protection impact assessment pursuant to art. 35.3 of the GDPR.

4.4 Do the regulations define the scope of data use?

Yes, they do. The scope varies depending on the purpose of the processing:

(a) Public health and biomedical research: the data subject may give their consent to the processing of their personal data for purposes of biomedical research. Personal data for health and biomedical research purposes can be reused when, having obtained consent for a specific purpose, the data is used for related research. In this case, controllers shall provide the information regarding the processing of personal data under art. 13 of the GDPR, in an easily accessible place on the corporate website of the centre where the research or clinical study is being carried out, and, where appropriate, on the website of the sponsor, and notify the parties concerned of the existence of this information by electronic means. A prior favourable report from the Research Ethics Committee is required.

(b) The processing of pseudonymised personal data: it is considered lawful to use pseudonymised personal data for health research, and in particular for biomedical research. However, the following requirements shall be fulfilled:
   (i) a technical and functional separation shall be made between the research team and those who perform the pseudonymisation and keep the information that makes reidentification possible; and
   (ii) the pseudonymised data may be accessible to the research team only when there is an express commitment to confidentiality and not to carry out any reidentification activity, and specific security measures are adopted to prevent reidentification and access by unauthorised third parties.

   There is an exception in which reidentification of the data at the source may take place. This is when, in the course of an investigation using pseudonymised data, it becomes apparent that there is a real and specific danger to the safety or health of a person or group of persons, or a serious threat to their rights, or reidentification is required to ensure proper healthcare.

(c) Situations of exceptional relevance and seriousness for public health: health authorities and public institutions with responsibilities for public health surveillance may carry out scientific studies without the consent of those concerned in situations of exceptional public health relevance and seriousness.

4.5 What are the key contractual considerations?

(a) Privacy contractual considerations with data subjects (users): according to the Spanish Data Protection Agency's guidelines, information with regard to the processing of personal data (privacy policy) must be available both in the application itself and in the application store, so that the user can consult it before installing the application or at

any time during its use. The language used in the privacy policies must be clear, taking into account the target user of the application. For example, applications available in Spanish and therefore aimed at Spanish-speaking users must provide the privacy policy in Spanish. In addition, the permissions that the application can request for access to data and resources should be indicated in the privacy policy. For example, it must explain if the application will process personal data only when it is being used by the user in the foreground or also when it is running in the background.

(b) Privacy contractual considerations with data processors: the processing by the processor shall be governed by a binding contract that sets out the subject matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects and the obligations and rights of the controller. The contract must ensure that processing only takes place in accordance with the instructions of the data controller and prohibit the processor from reverting to pseudonymised data in order to reveal the identity of the data subjects.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Health data is categorised as a special category of data according to the GDPR, and it is important to secure comprehensive rights to data because any processing activities regarding health data that does not comply with the purposes in art. 9.2 of the GDPR will be unlawful. If explicit consent of the data subject is the legal basis for lawful processing, the controller/processor shall ensure that the data subject has consented for the "one or more specific purposes" that they are interested in. As a general rule, and according to the purpose limitation principle under art. 5 of the GDPR, personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

Public interest sometimes overrides consent as a legal ground for health data processing in some instances, as explained in question 4.2. Key legal issues relating to personal data protection are outlined in question 4.3.

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

It is worth highlighting the role of the Spanish Data Protection Agency, which is responsible for publishing guides, reports and other documents on how personal data should be processed by companies and public administrations.

In both cases, guidelines are offered that provide support and enable the needs of the public and private sectors to be met with regard to the correct processing of data. It also provides resources and tools to facilitate compliance with the GDPR. Finally, it is also possible to consult the Agency on the application of the data protection regulation.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The main issue when sharing personal data in the context of digital health is that it is a market with many different players (app developers, device manufacturers, app stores, etc.). As the European Data Protection Supervisor established in its Opinion 1/2015 on Mobile Health, this makes it difficult to identify which parties act as data controllers or processors and to ensure an appropriate allocation of responsibilities, as well as ensuring user empowerment.

Therefore, it is important to respect the principle of transparency and accountability and the information requirements of art. 13 of the GDPR.

Moreover, in order to meet the obligations of privacy-by-design, it is important to clearly identify the different operators that will take part in the processing and to design the structure of all data processing activities accordingly. The above-mentioned Opinion states that data subjects should be given the option to freely allow the sharing/transfer of personal data to a third party, which is linked to the obligation of privacy-by-default, i.e. that the default features of the applications limit the types of processing to what is strictly necessary for the purposes of the application and/or device.

5.2 How do such considerations change depending on the nature of the entities involved?

Public authorities, unlike individuals, may transfer personal data concerning health without the consent of the data subjects, if it is necessary for the performance of a task carried out in the public interest or in the exercise of public authority and as long as it has a competence conferred by law.

According to the Spanish Data Protection Agency, if a certain processing is not "necessary" for the fulfilment of the mission carried out in the public interest or in the exercise of public powers conferred by law, such processing would lack a sufficient legal basis and would also infringe the principle of minimisation of data, which is also applicable to data processing carried out by public authorities.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Private entities may only share personal data if the data subject has provided their consent. There is also a legal obligation to transfer personal data that is essential for making decisions in public health to the health authorities. Transfers of data directed to territories outside of the EEA seem very likely in the field of digital health services; the provider may need to obtain an authorisation or alternatively to prove that the country of destination has been subject to a decision of adequacy by the European Commission or establish adequate safeguards conferring legal rights and remedies, such as conducting a risk assessment and enter into Standard Contractual Clauses with the data importer or relying on binding corporate rules, among other options.

Public authorities may transfer data subjects' health data without their consent to other public health authorities when this is strictly necessary for the protection of the population's health.

For purposes of biomedical research, it is necessary to collect the express written consent of the person concerned for the transfer of personal data to third parties not involved in medical care or biomedical research, even if the data is pseudonymised. In addition, if the data obtained from the source subject may reveal information of a personal nature about their relatives, the transfer to third parties shall require the express written consent of all the parties concerned.

6 Intellectual Property

6.1 What is the scope of patent protection?

The technologies involved in digital health may include medical devices, software and algorithms. AI and machine learning technologies are based on computational models and algorithms.

According to art. 4.4 of Law 24/2015 of 24 July 2015 on patents (Spanish Patent Act), computer programs, mathematical methods, plans, rules and methods for the pursuit of intellectual activities, for games or for economic and commercial activities and ways of presenting information, may not be patentable.

Therefore, the AI and machine learning solutions *per se*, which are essentially software, i.e. a mathematical method, are not patentable. However, AI-related inventions having a technical character would be patentable, since the patent would not relate to a mathematical method as such.

6.2 What is the scope of copyright protection?

According to the Spanish Copyright Act, the intellectual property of a literary, artistic or scientific work belongs to the author by the mere fact of its creation. Therefore, protection is granted without requiring the fulfilment of any kind of formality, i.e. it is not necessary to register the work before any office. In Spain, the registration is merely for evidentiary purposes.

Copyright is the most common way to protect software. In this regard, art. 10(1)(i) of the Spanish Intellectual Property Act expressly foresees that computer programs are protected by copyright.

With regard to AI solutions, which allow operators to process, analyse and extract useful information from huge data sets, according to art. 12 of the Spanish Copyright Act, these data sets could be copyright protected as data compilations.

6.3 What is the scope of trade secret protection?

Law 1/2019, of 20 February 2019 on Trade Secrets defines trade secrets as any information relating to any area of the company, including technological, scientific, industrial, commercial, organisational or financial, which is secret in the sense that it is not generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question, its secrecy has commercial value and it has been subject to reasonable steps to keep it secret.

Trade secrets protection may be the only current existing option for protecting algorithms that are not patentable.

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

The Spanish Organic Law 6/2001 on Universities regards technology transfer as one of the main functions of universities. This law also facilitates the involvement of professors in university spin-offs, e.g. temporary leaves of absence. In turn, the Spanish Law 14/2011 on Science, Technology and Innovation governs basic aspects of the technology transfer process, e.g., the application of private law to transactions between universities and companies.

Results of academic technology are generally transferred or licensed to third parties through invention assignments or licence agreements, respectively, or as a result of the creation of a spin-off company. Universities and public research centres need to follow specific state regulations providing protection regarding the ownership of the creations, and are required to follow internal protocols that set out the terms for cooperation between university personnel and private entities. According to Law 14/2011, researchers shall in any case be entitled to share in the profits from the exploitation or assignment of their rights to such inventions obtained by the entities for which they provide their services.

On 6 September 2022, the new Law 17/2022, of 5 September, amending Law 14/2011, of 1 June, on Science, Technology and Innovation was published. This law regulates further incentives for academics to bring their research to market, or to create start-up companies building on research outcomes. In this sense, Communication 2022/C 414/01 of the European Commission provides guidelines for ensuring adequate compensation for public universities and public research organisations in their contracts with companies, which has a direct impact on the criteria for the preparation of budgets and intellectual and industrial property rights.

6.5 What is the scope of intellectual property protection for software as a medical device?

Although the Spanish Patent Act expressly excludes the patentability of "computer programs", it seems to admit the possibility of patenting computer applications incorporated in patented hardware.

Another alternative to protect software would be through the Spanish Copyright Act, which expressly foresees the protection of computer programs. However, the protection granted by copyright is not as strong as patent protection, since the software will not be protected against the development of other programs meeting similar needs.

Other potential ways of protecting software are using trade secrets as well as trademarks legislation. However, regarding trade secrets, competitors may try to reverse engineer the software and it is key that reasonable steps are taken to keep it secret (such as signing non-disclosure agreements and prohibiting reverse engineering in licensing agreements).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

The Spanish Patent Act does not mention the condition that the inventor must be a natural person. However, the Guidelines published and followed by the Spanish Patent and Trademark Office for the examination of Spanish patent applications specifically establish that "only natural persons can be designated as inventors, and never, legal persons". Taking also into account that the understanding of the term inventor as referring to a natural person appears to be an internationally applicable standard, at this moment it is not possible for an AI device to be named as an inventor of a patent since the inventor must be a natural person in Spain.

The same is applicable at European level. Although there is no express provision in the European Patent Convention (EPC) which states that the inventor must be a natural person, it recognises moral rights to the inventor and contains references to the inventor being a natural person. In that regard, in 2018 two patent applications in which the inventor was an AI system, referred to as DABUS, were filed before the European Patent Office (EPO). It rejected the application on the grounds that they do not meet the legal requirement of the EPC that an

inventor designated in the application has to be a human being, and not a machine. The decision has been confirmed by the Board of Appeal of the EPO.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

Government-funded inventions in Spain fall within the general regime for inventions, which includes the Spanish Patent Act, Royal Decree 316/2017 approving Regulations for the implementation of the Spanish Patent Act, and Orders ETU/296/2017 and ETU/320/2018. In addition, Royal Decree 55/2002 on the exploitation and transfer of inventions made in public research bodies sets, specifically, the ownership regime that must rule the inventions created by research staff working for several Spanish research agencies, such as the Spanish National Research Council and the Carlos III Health Institute.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The FENIN has a Code of Ethics which includes minimum principles to which its members must adhere when entering into collaboration agreements with healthcare professionals. The main requirements are that a legitimate need for the services must have been identified beforehand, that the agreements have to be documented in writing, all conditions should be agreed on market terms and be transparent, which means that the agreement should be notified in advance to the employer and that any publication or presentation of results will need to mention the collaboration.

Collaboration agreements should address confidentiality, ownership of the results, publication rights and adherence to ethical rules.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

Any agreement with non-healthcare companies needs to include an express commitment by the non-healthcare company to adhere to the ethical rules to which the healthcare company adheres, in addition to the usual provisions regarding ownership of results, confidentiality and publication rights.

In the event that the digital health solution under development will need to be approved as a medical device, the agreement should address regulatory matters in order not to jeopardise approval.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning can be used for the prediction of population health risks, enhancing health information management, quick and accurate diagnosis of conditions that are difficult to uncover or, for example, providing early health information to patients.

8.2 How is training data licensed?

Before licensing training data, it is vital to determine if healthcare data is involved, in which case the enhanced data protection principles apply. If anonymised, or at least pseudonymised, the data can be used for training purposes, and these should be referred.

Before licensing any data, the machine learning providers should obtain sufficient information about the provenance of the data, ascertain whether the data controller has collected the data in compliance with the law, and whether they have sufficient permissions to apply the data in the training.

The agreement should further foresee the scope of permitted use of the licensed data and allocation of developed and derived data.

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

The automatic learning algorithms learn from the information provided by their programmers and from there, they generate new works through a series of independent decisions, which may result in learning new methods or the creation of new algorithms and models.

In Europe, the European Court of Justice has stated on several occasions, notably in its landmark Infopaq decision (case C-5/08, *Infopaq International A/S v. Danske Dagblades Forening*), that copyright only applies to original works and that originality must reflect the "author's own intellectual creation". This expression is generally understood to mean that an original work must reflect the author's personality. This can be interpreted to mean that there must be a human author for a copyright work to exist. In this case, it could be the programmer who owns the intellectual property rights.

If the machine learning process can be sufficiently described and put into use in a technical context, the subject matter could also fall within the patentable domain.

In this context, it is of vital importance that the parties involved in the machine learning process, generally at least the AI/machine learning provider and the provider of the data set used to teach the algorithm, must foresee beforehand in their contractual terms not only how the data input and resulting data can be used, but also how these data are going to be allocated and who will own the IP rights, such as trade secrets and patents, to the developed, clinical or derived data.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The foremost consideration in the licensing of data for their use in machine learning is the protection of personal data, due to the sensitivity of the data involved. The parties should address the provenance of the data and check that the necessary permissions to use such data are in place.

The correct allocation of IP rights under licensing contracts is also of the utmost importance in order to protect the parties and to secure the commercial viability of the project. Typically, it should be considered and foreseen beforehand who owns the background IP and the IP developed based (in part) on the other

party's data, who owns and under what conditions the results and derived data may be used, and if there are any specific allocations, for example, for specific categories of data or assets.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

The GLPCU imposes strict liability for personal injury or material damage that is caused by a defective product. The manufacturer of a product or an "own brander" (i.e. someone who, by putting their name, trademark or brand on a product, holds themselves out as the manufacturer) are primarily liable for defective products under the GLPCU.

The GLPCU will only apply to an algorithm or a solution if they are considered to be "products". In this regard, there are precedents of the Spanish High Court declaring that a software is considered a product.

This area is under review by the EU regarding AI. The European Commission has adopted a Proposal on adapting non-contractual civil liability rules to AI, published on 28 September 2022. This Proposal highlights the establishment of common rules on the disclosure of evidence on high-risk AI systems so that plaintiffs can substantiate their fault-based liability claims; it also eases the burden of proof for damage caused by an AI system and establishes a presumption of causation for cases where there is a causal link between the AI system and the damage.

9.2 What cross-border considerations are there?

Suppliers (if they were aware of the defect) and importers of the defective product in the EU can also be liable. Liability is joint and several in the event that there are different potential liable parties. In the specific case of medical devices, Spanish Royal Decree 1591/2009 regulating medical devices rules that manufacturers who are not established within the EU shall designate a single authorised representative within the EU, both the manufacturer and the EU representative may be liable.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Hospitals and healthcare professionals are increasingly relying on Cloud-based services to store information related to patients and to make it accessible. Challenges in this area are the protection of personal data and prevention of cyberattacks.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Regulation remains an important issue. Whether the digital health solution will require approval as a medical device has to be assessed from the outset through a risk classification of the product and this will affect the product development cycle. Non-healthcare companies will need to factor in longer product development cycles than for non-healthcare digital offerings.

Reimbursement strategies and developing a sustainable business model are becoming increasingly important. Non-healthcare companies need to understand the clinical problems they want to address and whether payers will see a value in it.

The healthcare provided in Spain is predominantly public. Therefore, the importance in gaining acceptance by public healthcare authorities also needs to be considered, in particular, when the digital health solution satisfies an unmet and clearly identified need.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

The key issues are understanding the business model, clarifying the regulatory and market access issues and the positioning of the product, and the specific revenue model, including potential reimbursement.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Key barriers preventing widespread clinical adoption of digital health are not so much regulatory as they relate to organisational, budgetary or cultural reasons. The COVID-19 pandemic has been a turning point. The Digital Spain Plan 2025 identifies the following fields of action to increase the efficiency and quality of public healthcare services in Spain: (i) research to measure and improve health outcomes and to design preventive systems; (ii) support to patients in order to automatise and provide them with tools to be better informed in making health decisions; (iii) patient empowerment with telemedicine, self-diagnostic or enhanced accessibility tools; and (iv) streamlining of information systems to enable better data sharing and interoperability.

Leaving aside the prevailing attention to digitalisation of information, digital health solutions such as mHealth are not generally present in the clinical practice because they have not been generally incorporated in the public National Health System and therefore are not financed.

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?

Certification initiatives are mainly coming from the public sector rather than physician associations. We are not aware of any formal requirement of endorsement by physician certification bodies in Spain in order to introduce digital health solutions into clinical practice. Note, however, that some regional health authorities have accreditation and/or certification systems in place for mobile applications (mHealth). They award accreditations and/or include them in repositories of accredited apps for use in the regional public health system (Healthcare Quality Agency of Andalusia with the Distintivo AppSaludable (seal of quality) and Catalonia's TIC Salut Social and iSYS Score). Such accreditations are a driver for clinical adoption.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

There is no specific reimbursement process for digital health solutions within the Spanish health system. Spanish patients,

when treated by the National Health System, receive all healthcare products and treatments included in the list of health benefits of the National Health System (Royal Decree 63/1995). Digital health solutions can be incorporated by the National Health System or by regional authorities, so that patients can benefit from them without charge. In this regard, each autonomous community may decide to incorporate digital health solutions that qualify as medical devices to their healthcare services. Regarding telemedicine, within the National Health System, it is provided by the National Health System professionals and, therefore, does not need a reimbursement process.

Any medical consultations outside of the National Health System are not reimbursed, whether in person or via telemedicine, unless they are provided under an agreement between the services provider and the National Health System.

10.7 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 Ministry of Health approved in December 2021 the Digital Health Strategy of the National Health System. This strategy seeks to maintain a good level of citizens' health along with the improvement of the public health system by adapting it to the digital world.

The following objectives may be highlighted: the empowerment and involvement of people in their health care; the generation of valuable processes to improve the public health system; the adoption of data management policies to have interoperable and quality information; and the application of innovation and focus on 5P healthcare policies (People, Prevention, Predictable, Personalised, Participative) to adapt the National Health System to current needs.

Montserrat Llopart Vidal is a Partner in the International Commercial & Trade department and leads the Healthcare and Compliance Law practices in the Baker McKenzie Barcelona office.
She is a regular speaker and contributor to specialist conferences and publications, and she is recognised by the leading legal directories such as *Chambers and Partners*, *The Legal 500* and *Best Lawyers* and in the *InspiraLaw* Top 50 Women's List for Spain and Portugal.
Montserrat is the former head of Baker McKenzie's Barcelona office and the Firm's pharmaceutical law group in the EMEA region.

Practice Focus

Montserrat assists healthcare companies throughout the lifecycle of healthcare products, from R&D to commercialisation and more specifically in the areas of clinical trials (agreements, regulatory procedures, processing of personal data), market access (pricing and reimbursement), products and companies regulations, commercial relations between healthcare industries (distribution, (co)promotion, manufacturing, supply, licensing, partnership agreements), relations with healthcare professionals and/or patients including compliance communication & advertising, e-health (connected devices, telemedicine, hosting of health data) and product liability. Her practice encompasses both advisory and litigation matters.

Baker McKenzie
Av. Diagonal, 652
Edif. D, 8th Floor
Barcelona 08034
Spain

Tel: +34 93 206 0820
Email: montserrat.llopart@bakermckenzie.com
URL: www.bakermckenzie.com

Javier Saladich Nebot is an Associate with the International Commercial & Trade department of the Baker McKenzie Barcelona office.
Javier advises life sciences companies on regulatory law issues related to authorisations, marketing and promotion of their products and compliance with industry codes. He drafts and reviews industry-specific agreements between life sciences companies and their stakeholders including HCOs and patient associations. Javier also works on matters related to compliance with personal data protection legislation and corporate compliance, including the implementation of compliance programs and internal investigations. Finally, Javier is the co-coordinator of the Pro Bono Committee of the Baker McKenzie Barcelona office.

Baker McKenzie
Av. Diagonal, 652
Edif. D, 8th Floor
Barcelona 08034
Spain

Tel: +34 93 206 0820
Email: javier.saladich@bakermckenzie.com
URL: www.bakermckenzie.com

Baker McKenzie is the first global law firm and operates from 78 offices in 46 countries around the world.
Baker McKenzie helps clients overcome the challenges of competing in the global economy. We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instil confidence in our clients.

www.bakermckenzie.com

Taiwan


Hsiu-Ru Chien


Eddie Hsiung


Shih-I Wu

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 Taiwan law. In general, "digital health" should cover areas such as mobile medicine (mHealth), medical health information (Health IT), wearable devices, telehealth and telemedicine, personalised medicine, and other applications of information and communication technology (ICT) in the medical and health fields.

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

Based on Taiwan's complete semiconductor and ICT industry supply chain, cross-border integration of medical technologies, as well as innovative digital health technologies such as healthcare big data, Internet of Things (IoT), artificial intelligence (AI) and 5G technology, biomedical chip technology, sensors, wearable devices, biobanks, telehealth and telemedicine are being invested, created, and developed in various fields and industries, and also by government organisations.

1.3 What are the core legal issues in digital health for your jurisdiction?

With respect to digital health in the context of a medical device, it is subject to regulations under the Medical Devices Act, which took effect on May 1, 2021. The term "medical device", as defined in the Medical Devices Act, shall refer 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 Taiwan legal perspective, the manufacturing or importation of medical devices may be conducted only after a medical device permit licence that grants registration and market approval is issued by the government authority.

Personal data protection is also a critical issue where any personal data is to be collected, used, or processed in the course of providing any digital health products or services.

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

There are no official statistics concerning the digital health market size in Taiwan. Nonetheless, according to the estimated data of the Industrial Technology Research Institute, Taiwan's precision health market was estimated to be about NT$8.75 billion (around US$300 million) in 2020 and to reach NT$14.2 billion (around US$490 million) in 2025, with a compound annual growth rate of 10.2%; the growth rates for digital health, precision medicine, and regenerative and immunomedicine composites were estimated to be about 11%, 11.5%, and 4.8%, respectively.

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

In Taiwan, the digital health market is mostly invested in by major electronic technology companies. The revenue of these companies is calculated on the basis of the overall enterprise, so it is difficult to distinguish their revenue or rank with respect to the digital health field.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Medical Devices Act provides for core regulations governing medical devices.

As indicated under question 1.3, the manufacturing or importation of medical devices is only allowed after a medical device permit licence that grants registration and market approval is issued by the Ministry of Health and Welfare (MOHW).

Medical device manufacturing must comply with the guidelines set forth in the Good Manufacturing Practice (GMP) under the Pharmaceutical GMP Regulations.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Depending on the issues involved, the following laws and their related regulations apply:

- The Personal Data Protection Act (PDPA).
- The Physicians Act.
- The Consumer Protection Act.
- The Civil Code.
- The Telecommunications Act.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The Consumer Protection Act and the Civil Code are the main laws providing for the relevant consumer rights and product liabilities. The manufacturing and sale of consumer devices should also follow the regulations under the Commodity Labelling Act and the Commodity Inspection Act.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The MOHW is the competent authority responsible for supervising healthcare-related matters, products, and industries. The MOHW has a broad mandate to improve the quality of healthcare.

Under the MOHW, the Food and Drug Administration (TFDA) is responsible for regulating the system for the safety and quality of food, drugs, medical devices, and cosmetics. The TFDA grants product registration and clinical trial approvals, monitors manufacturing and importation, and conducts safety surveillance activities on health-related products.

2.5 What are the key areas of enforcement when it comes to digital health?

The Medical Devices Act outlines a three-tier risk-based classification system for medical devices: Class I products with low risk; Class II products with medium risk; and Class III products with high risk.

Additionally, any person who manufactures or imports medical devices without the required prior approval may be subject to imprisonment for not more than three years and may, in addition thereto, be imposed with an administrative fine of not more than NT$10,000,000.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

In addition to the regulations mentioned in our answer to question 2.1, the Guidance for Medical Software Classification, as announced by the TFDA, also applies to Software as a Medical Device. On December 24, 2020, the TFDA announced the revision of the Guidance for Medical Software Classification, which excludes medical software used to measure heart rate and blood oxygen (including wearables) for daily health management of the general public within the scope of a medical device, if they are not related to the diagnosis or treatment of diseases. Recognition of classification is still subject to the judgment of the competent authorities.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

No specific regulations are enacted specifically for AI/Machine Learning (ML) powered digital health devices or software solutions. Medical devices are all governed by the Medical Devices Act; Chapter IV of the Medical Devices Act provides for regulations concerning management of medical device clinical trials.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - Service provider – Pursuant to the Physicians Act, a physician may not treat, issue a prescription, or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances. Therefore, physicians are not allowed to provide telemedicine services under current laws in general.
  - Regulations for medical devices – The regulations mentioned in our answer to question 2.1 should be complied with if the equipment/devices involved are considered as medical devices.
  - Personal data protection – Taiwan's personal data protection law should also be followed if any personal data is to be collected, used, or processed.
  - Product liability – Manufacturers and sellers of products are subject to the duties and liabilities under the Consumer Protection Act and the Civil Code.
  - Attribution of responsibility – Provision of the service of telemedicine may involve the user (patient), the healthcare service provider (physician) and the manufacturer/seller of the product. The attribution of responsibility of the relevant parties should be determined generally based on the contracts as well as the tort law (Civil Code and Consumer Protection Act).
- **Robotics**
  Similar issues as for Telemedicine/Virtual Care regarding regulations for medical devices, personal data protection, product liability, and attribution of responsibility.
- **Wearables**
  Similar issues as for Telemedicine/Virtual Care regarding regulations for medical devices, personal data protection, and product liability.
- **Virtual Assistants (e.g. Alexa)**
  Similar issues as for Wearables.
- **Mobile Apps**
  Similar issues as for Wearables.
- **Software as a Medical Device**
  Similar issues as for Wearables.
- **Clinical Decision Support Software**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Similar issues as 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**
  Similar issues as for Wearables.

- **3D Printing/Bioprinting**
  Similar issues as for Wearables.
- **Digital Therapeutics**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **Natural Language Processing**
  No special regulations for Natural Language Processing.

3.2 What are the key issues for digital platform providers?

The PDPA is the main law governing the collection, processing, and use of personal data so as to prevent harm to personality rights and to facilitate the proper use of personal data. Digital platform providers should follow the requirements under this Act if any personal data is involved in the products or services provided by digital platform providers.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

Under Taiwan law, the PDPA is the main law governing personal data protection. The key issues to consider for use of personal data under the PDPA include, among others, the following:

- Whether the data is considered "personal data" under the PDPA.
- Whether the "personal data" is considered "sensitive personal data" under the PDPA. Please see our response to question 4.4 for the definition of "sensitive personal data".
- Whether the use of personal data complies with relevant requirements under the PDPA, such as the requirement to obtain the necessary informed consent from the data subject as required by the PDPA, etc. (or whether any exemption from the requirement applies).

4.2 How do such considerations change depending on the nature of the entities involved?

The considerations indicated in our response to question 4.1 above would not change regardless of the nature of the entities involved; however, the available types of exemptions from the requirement to obtain informed consent from the data subject are different between non-government entities and government entities.

4.3 Which key regulatory requirements apply?

Under the PDPA, unless otherwise specified by law, a company is generally required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing, or using any of said individual's personal information (i.e., the "informed consent" requirement), subject to certain exemptions. To satisfy the notice requirement, certain matters must be communicated to the individual, such as the purposes for which his or her data is collected, the type of the personal data and the term, area, and persons authorised to use the data, etc.

In case the personal data is regarded as "sensitive personal data" (please see our response to question 4.4), the consent must be made in writing, and the following must be complied with: (i) the collection, processing, or use must not exceed the necessary scope of the specific purpose(s); (ii) the collection, processing, or use based solely on the consent of the data subject is not otherwise prohibited by law; and (iii) such consent is not given by the data subject out of his/her free will.

4.4 Do the regulations define the scope of data use?

Pursuant to the PDPA, "personal data" is defined broadly to include: name; date of birth; I.D. card number; passport number; characteristics; fingerprints; marital status; family information; education; occupation; medical record, medical treatment and health examination information; genetic information; sexual life information; criminal record; contact information; financial conditions; social activities; and other information which may directly or indirectly identify an individual. Additionally, personal data pertaining to a natural person's medical records, healthcare, genetic information, sexual life information, physical examination, and criminal records are known as "sensitive personal data", and thus are generally subject to stricter regulations under the PDPA.

4.5 What are the key contractual considerations?

In case any collection, use, or processing of personal data is contemplated under a contract, it is suggested that the above-mentioned "informed consent" requirement be fully complied with, unless any of the available exemptions are satisfied. Additionally, it may be arranged to have the parties (or, at least for the party who will actually collect, use, or process personal data) agree to the "compliance clause" to ensure a party's compliance with the PDPA throughout the contract period.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Compliance with the PDPA, in particular, obtaining required "informed consent" for collection, use, and processing of personal data and using and processing the collected personal data within the necessary scope of the specific purpose(s), is the key legal issue; as any violation of the PDPA (e.g., unlawful collection, use, or processing of personal data) may be subject to civil, criminal, and/or administrative liabilities. For example:

- Civil liability: A company would be liable for the damages caused by any unlawful collection, processing, or use of personal data due to its violation of the PDPA (Article 29 of the PDPA).
- Criminal liability: Any unlawful collection, processing, or use of personal data in violation of the PDPA with the intention of obtaining unlawful gains and thereby causing damage to others would be subject to imprisonment for no more than five years and may, in addition thereto, be imposed with a criminal fine of not more than NT$1,000,000 (Article 41 of the PDPA).
- Administrative liability: Any unlawful collection, processing, or use of personal data in violation of the PDPA may be required to be corrected, and any failure to correct such violation within a specified period of time would be subject to an administrative fine (Articles 47 and 58).

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

With respect to data inaccuracy, pursuant to the PDPA, a data subject has the right to correct or supplement his/her personal data, as well as the right to request the deletion of the data.

As for data bias and discrimination, currently no specific laws or regulations have been promulgated or amended to address the issues regarding data bias or discrimination. In this regard, we believe that more and more discussions will emerge in legal fields such as labour/employment law (with respect to sex, race, religion or belief, political views, etc.), privacy law, anti-trust, and any other area where "equality" or "fairness" would be an important factor with respect to social life and economic activity, especially from the viewpoint of issues that may be caused by the use of AI algorithms and big data analytics.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Please see our response to question 4.1 above, as sharing personal data would be considered to fall within the definition of "processing" and/or "use" of personal data under the PDPA.

5.2 How do such considerations change depending on the nature of the entities involved?

Please see our response to question 4.2 above.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please see our response to question 4.3 above.

Please also note that, in case the personal data is regarded as "sensitive personal data" (please see our response to question 4.4), an exemption from the "informed consent" requirement for collection, use, and processing of personal data (including data sharing) is "where it is necessary for statistics gathering or academic research by a government entity or an academic institution for the purpose of healthcare, public health, or crime prevention, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject".

6 Intellectual Property

6.1 What is the scope of patent protection?

According to the Patent Act, the subject of a patent right may be an invention, a utility model, or a design:

- Invention – the creation of technical ideas, utilising the laws of nature.
- Utility model – the creation of technical ideas relating to the shape or structure of an article or combination of articles, utilising the laws of nature.
- Design – the creation made in respect of the shape, pattern, colour, or any combination thereof, of an article as a whole or in part by visual appeal. For computer-generated icons (Icons) and a graphic user interface (GUI) applied to an article, an application may also be filed for obtaining a design patent.

Under the Patent Act, any invention/utility model/design is patentable provided it complies with the requirements for patentability, such as novelty, inventive step, and enablement. However, please note that diagnostic, therapeutic, and surgical methods for the treatment of humans shall not be granted a patent under the Patent Act. Thus, if a concerned "digital health" invention or technology involves diagnostic, therapeutic, and surgical methods for the treatment of humans, it may be deemed an unpatentable subject matter.

Moreover, a digital health invention or technology may relate to the creation of a software or an algorithm. "The Examination Guidelines for Computer-related Inventions" provide rules for deciding whether such invention can be granted a patent. The Guidelines classify statutory subject matters for software patents: process; product; and computer-readable storage media. "Process" is defined as a series of specific operational steps to be performed on or with the aid of a computer. "Product" encompasses a computer or other programmable apparatus whose actions are directed by a computer program or another form of software. "A computer-readable storage medium" is an article of manufacture that, when used with a computer, directs the computer to perform a particular function. Software patents are patentable if the data format interacts with computer software or hardware to produce technical effects (such as enhancing data processing, storage performance, security, etc.).

6.2 What is the scope of copyright protection?

A "work" under the Copyright Act means a creation that is within a literary, scientific, artistic, or other intellectual domain, which includes oral and literary works, musical works, dramatic and choreographic works, artistic works, photographic works, pictorial and graphical works, audio-visual works, sound recordings, architectural works, and computer programs. There are no registration or filing requirements for a copyright; however, there are certain features that qualify for being copyrighted, such as "originality" and "expression".

Software designed for "digital health" can be protected through copyright.

6.3 What is the scope of trade secret protection?

Trade secrets are protected if they satisfy the following constituent elements: information that may be used in the course of production, sales, or operations; has the nature of secrecy; has economic value; and its owner has taken reasonable measures to protect the secrecy. There are no registration or filing requirements for a trade secret to be protected by law.

To keep trade secrets confidential during court proceedings, the court trial may be held in private if the court deems it appropriate or it is otherwise agreed upon by the parties. In an intellectual property-related lawsuit, the parties may apply to the court to issue a "protective order", and the person subject to such protective order should not use the trade secrets for purposes other than those related to the court trial and should not disclose the trade secrets to those who are not subject to the order.

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

In general, academic institutions have specific internal policies to regulate the ownership and management of the technologies

created by their scholars, researchers, graduate students, and employees. Academic institutions may license or assign their IPs to a third party for commercial purposes.

6.5 What is the scope of intellectual property protection for software as a medical device?

Software can be protected by intellectual property rights such as patents, copyrights, or trade secrets. For software-implemented inventions such as a medical device, if it coordinates software and hardware to process information, and there is a technical effect in its operation, it might become patentable.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

In judicial practice, an artificial intelligence device cannot be named as an inventor of a patent. Judgments from the Taiwan Intellectual Property and Commercial Court hold that a patent invention is the creative output of the human spirit, and cannot be created by an artificial intelligence device; from the perspective of Taiwan laws, only natural or legal persons can enjoy such rights.

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

For projects in scientific and technological research and development (R&D) to be subsidised, commissioned, or funded by the government, or to be conducted under scientific and technological R&D budgets prepared by public research institutions (organisations) pursuant to the law, the "management and utilisation of the R&D results" should comply with the Fundamental Science and Technology Act and the Government Scientific and Technological Research and Development Results Ownership and Utilisation Regulations. Specifically:

- The R&D results and the income from such a project may be conferred, in whole or in part, to the executing R&D units for ownership or licensing for use, and are not subject to the National Property Act.
- The ownership and utilisation of the R&D results and the income therefrom should be determined based on the principles of fairness and effectiveness by assessing the percentage contribution of capital and labour, the nature of the R&D results, potential uses, societal benefits, national security, and impact on the market.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Issues in relation to the rights (especially the IP ownership), obligations and division of responsibilities are critical for collaborative improvements. The applicable laws and agreements between the parties would need to be carefully analysed and arranged for in this regard.

For a collaborative improvement involving a fund provider and an inventor/developer, the IP laws adopt similar rules to govern the ownership of the said improvement. With respect to patent rights and trade secrets, the agreement between the parties shall prevail, or such rights will be vested in the inventor or developer in the absence of such agreement, and the fund provider may use such invention.

With respect to copyright, the person who actually creates the work is the author of the work unless otherwise agreed upon by the parties; the economic rights arising from the work should be agreed upon by the parties, or the author owns such rights in the absence of such agreement. However, the commissioning party (fund provider) may use the work.

For improvements that are jointly made by several parties, attention shall be paid to the issue of co-ownership. The Patent Act clearly provides the following provisions for co-owned patents:

- Where a right to apply for a patent is jointly owned, the patent application related thereto shall be filed by all the joint owners. If a co-owner contravenes the provision for "joint-application" by individually filing an application and obtains a patent as a result thereof, other co-owners may file a cancellation action with respect to such patent and seek revocation of the patent right.
- Where the right to apply for a patent is jointly owned, the right to apply for the patent shall not be assigned or abandoned without the consent of all joint owners. Where the right to apply for a patent is jointly owned by two or more persons, none of the joint owners shall assign his/her own share therein to a third party without the consent of other joint owners. Where one of the owners of the right to apply for a patent abandons his/her own share, this share shall be vested in other joint owner(s).
- Where a patent right is jointly owned, except for exploitation by each of the joint owners, it shall not be assigned, entrusted, licensed, pledged, or abandoned without the consent of all the joint owners. Where a patent right is jointly owned, no joint owner may assign, entrust, or establish a pledge on his/her own share without the consent of all the other joint owners. Where a joint owner of a patent right has abandoned his/her own share, this share shall be vested in other joint owner(s).

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

As indicated in our answer to question 2.1 above, the manufacturing or importation of medical devices is only allowed after a medical device permit licence granting registration and market approval is issued. Given that, whether the company has or is required to obtain the permit licence would be a critical issue.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

According to our understanding of the practice, the current applications of machine learning include, among others: (i) clinical decision support: for example, analysing medical images with machine learning to improve the accuracy of diagnosis results; and (ii) big data forecasting: by analysing large amounts of data, tracking, or forecasting the relationships between different medicines and side effects.

Please note, however, that although an AI might be able to make decisions by itself, under current Taiwan law, only a licensed physician may practice as a physician. Thus, AI and machine learning are merely "technologies" or "tools" to assist physicians.

8.2 How is training data licensed?

If any personal data would be collected, used, or processed with respect to training data/data licensing, the PDPA regulatory regime (e.g., our response to sections 4 and 5) would apply – for example, it should be arranged to have the data collector obtain the necessary "informed consent" unless any exemption applies. If any intellectual property is involved in the licensing, it is suggested that the customary licensing practice (e.g., IP licensing agreement to be entered into by the licensor and licensee) be followed.

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

Determining the owner of the intellectual property of an AI-created work is expected to be a legal issue that will be widely discussed as AI use develops and becomes more widespread. According to the views of many experts and scholars, AI development can be generally divided into the following three phases, and we are currently in phase 2:

(i) Phase 1: all intrinsic knowledge/information of AI is given by humans, and AI simply functions as a tool to respond to human query inputs. AI does not have the ability to learn or think.

(ii) Phase 2: AI learns through computer software designed by humans, which is called "deep learning". In addition to responding to human query inputs, AI is able to use its limited intrinsic perception and logic to help its users make decisions.

(iii) Phase 3: AI has evolved to have the ability to think for itself and act sufficiently like a human (i.e., it may have perceptions and emotions). That is, AI has a self-training ability, and the ability to evaluate, determine, and solve problems.

With respect to phase 1, as the AI merely functions as a tool utilised by humans to create a work or invention, the human (user of the AI) should be the owner of the intellectual property (copyright or patent).

In phase 2, AI already has the ability of deep learning, and it is not merely a tool for humans. However, there would be issues as to whether AI has the ability to create an "original expression" under copyright law or to be an "inventor" under patent law, and if not, whether the human using the AI can be considered as the one who actually creates the "expression" or the invention. Such issues would be more important and cannot be ignored in phase 3, when AI has evolved to have the ability of independent thinking and can create an "expression" and make an invention like a human.

We believe that the above view is also generally supported by a letter of interpretation issued by Taiwan's Intellectual Property Office (IPO) dated April 20, 2018 (Ref. No.: 1070420), which provides that as AI is not a "person" from a legal perspective, any AI-created work cannot be protected by copyright.

In general, our preliminary view is that such issues might not be solved under the current IP regime in Taiwan; it is a real challenge faced by, and needs to be addressed by, the government, legislators, representatives of the court system, and other legal practitioners in the future, along with the development of AI.

8.4 What commercial considerations apply to licensing data for use in machine learning?

As indicated in our response to question 8.2, if any "personal data" would be collected, used, or processed with respect to training data/data licensing, the PDPA regulatory regime (e.g., our responses to sections 4 and 5) would apply. Specifically, in case of any "sensitive personal data", more restrictions would apply – such as the requirement that the "informed consent" be in writing (see question 4.3). We believe PDPA compliance as indicated should be carefully considered with respect to data licensing.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

The theories of liability applying to adverse outcomes are mainly as follows:

- Civil liability – breach of contract, torts, and product liability: the Civil Code; and the Consumer Protection Act would apply.
- Criminal liability – injury (intentional act or negligence) or carrying out activities of manufacturing or importation without the required permit or approval: the Criminal Code; the Physicians Act; and the Medical Devices Act would apply.
- Administrative liability – carrying out activities of manufacturing or importation without the required permit or approval; the Medical Devices Act would apply.

9.2 What cross-border considerations are there?

In case any digital health-related services are provided to Taiwanese persons from offshore, there may be an issue as to whether such offshore entity would be required to comply with the Taiwan regulatory requirements regarding licensing (e.g., prior approval/permit/licence required for running a medical device company or carrying out healthcare-related activities) as healthcare is a regulated industry in Taiwan. Please also see our response to question 10.2 for such regulatory requirements.

From a contract perspective, even if the governing law of the contract for the digital health-related service is foreign law (i.e., non-Taiwan law) and a foreign court is agreed in the contract for dispute resolution, we still cannot completely rule out the possibility that in case of any dispute where the Taiwan persons file the suit in a Taiwan court, the Taiwan court would still review the matter and rule that the Taiwan laws (such as the Taiwan Consumer Protection Act) would apply in order to protect said Taiwanese persons.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

With respect to Cloud-based services for digital health, the PDPA will be applicable, as an organisation using the Cloud-based service may carry out the activities of collecting data from the data subjects, which would then be passed to a service provider for processing and use. Therefore, from a Taiwan legal viewpoint, the key issue in Cloud-based services for digital health is PDPA compliance. Please see our responses to sections 4 and 5, specifically, where personal data is considered "sensitive personal data", the requirement for the informed consent be in writing (see question 4.3), and an exemption from the "informed consent" requirement for use by non-government entities or academic institutions under certain circumstances (see question 5.3).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Please note that healthcare is a regulated industry in Taiwan. For example, running a medical device company, as well as the manufacturing and sale of medical devices, would require prior approval/permits under current regulations. Additionally, pursuant to the Physicians Act, a person may not practice medicine as a physician without a required licence, and, in the context of telemedicine, a physician may not treat, issue a prescription, or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances (please also see question 3.1 above).

Given the above, it is advisable for non-healthcare companies to consider the above licensing/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 perspective, it is suggested that venture capital and private equity firms analyse in depth whether the target digital healthcare venture's business model is in line with Taiwan's regulatory regime at the due diligence stage – most importantly, the compliance with licensing/regulatory requirements as indicated under question 10.2 above as well as the PDPA compliance, especially if the personal data collected by the target company would involve "sensitive personal data".

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

According to our observation, the current legal obstacles in Taiwan that would hinder the developments of digital health solutions may include, for example: (i) as indicated in question 3.1, a physician may not treat, issue a prescription, or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances. Therefore, providing telemedicine services by physicians is generally not permitted under current laws in Taiwan; or (ii) there are generally more restrictions on collection, use, and processing of "sensitive personal data", which should be normally involved as to 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 (e.g., Taiwan Surgical Association) do not play an important role in the clinical adoption of digital health solutions. Compliance with existing regulatory requirements is of the greatest importance. Please see our response to question 10.2 for the licensing/regulatory requirements that need to be followed from a Taiwan regulatory perspective.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

To our knowledge, there are no private insurers that specifically exclude patients who utilise digital health solutions from filing insurance claims when an insured matter occurs and no additional documentation is required, unless it is specified in the insurance policy. Regarding the reimbursement by the government, we notice that there is a pilot plan announced by the National Health Insurance Administration in 2020 aiming to include virtual care for remote areas in the coverage of our National Health Insurance. Under the said pilot plan, patients who are seen through medical institutions that are approved to conduct virtual care may only need to pay for registration fees, subject to certain exceptions specified in relevant regulations.

10.7 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.

Taiwan's Constitutional Court announced a judgment in August 2022 (Ref. no.: Xian-Pan No.13) regarding the PDPA, holding that relevant laws should be promulgated or amended within three years, so that there would be: (i) an independent supervision mechanism for personal data protection under the PDPA; and (ii) clear provisions regarding protection of personal data stored, processed, transmitted, and used in the National Health Insurance Research Database (NHIRD), which contains the public's personal data collected through Taiwan's national health insurance system. Therefore, it is suggested to closely follow any amendments to the PDPA and related laws and regulations in the near future.

Hsiu-Ru Chien has an educational background in science, management and law, and is a certified attorney-at-law and patent attorney in Taiwan. She passed the Chinese Patent Bar in 2013. Her practice focuses on patent prosecution, enforcement, licensing, and transactions as well as other IP-related matters. She is serving as the Deputy Secretary of General of the Taiwan Patent Attorney Association. As a partner at Lee and Li, she periodically publishes IP-related articles in international journals such as the *World Intellectual Property Report* and *International Law Office Newsletter*. She has been honoured as Patent Lawyer of the Year 2021 in Taiwan by the 2021 *Corporate Intl Magazine Global Award*, Best Patent Prosecution Attorney (Taiwan) by *APAC Insider Legal Awards*, and Top 100 Women in Litigation 2020 by *Benchmark Litigation Asia-Pacific*.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2806
Email: hrchien@leeandli.com
URL: www.leeandli.com

Eddie Hsiung is licensed to practise law in Taiwan and New York. His practice focuses on M&A, securities, financial services, general corporate and commercial, start-ups, etc. He has participated in many corporate transactions (M&A, IPO, JV, cross-border investments) spanning a broad range of industries and areas, including TMT, bio-tech, big data, digital financial services, etc. In addition to the above-mentioned traditional practice areas, he is familiar with legal issues regarding digital economy, digital transformation and the application of new technologies such as fintech, blockchain, virtual assets, AI, and data protection, and is often invited to participate in public hearings, seminars, and panel discussions to provide advice to the government, regulators, legislators, and university/research institutions in these areas on regulatory policies.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2162
Email: eddiehsiung@leeandli.com
URL: www.leeandli.com

Shih-I Wu has a dual background in biological engineering and law and specialises in handling intellectual property and civil disputes. Shih-I has a wealth of experience in litigation and administrative remedy procedures for patent applications, patent infringement and patent cancellation, as well as in civil and criminal litigation regarding trade secrets, copyrights, and trademark rights. She has undertaken significant trade secret cases and a landmark case concerning protection of computer software. She is also familiar with reviewing intellectual property contracts and consulting on related disputes, and has experience in intellectual property transaction negotiations, royalty audits, and tax exemption applications, as well as civil disputes, product liability and consumer protection, fair trade disputes, environmental law disputes, and labour disputes. Shih-I's writings on the practice of intellectual property rights have been published in both domestic and foreign journals.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2515
Email: shihiwu@leeandli.com
URL: www.leeandli.com

Lee and Li, founded more than half a century ago, is the largest law firm in Taiwan providing legal services in the Greater China area by collaborating with law firms and intellectual property agencies in Mainland China. Besides our headquarters in Taipei, we have offices in Hsinchu, Taichung, and Kaohsiung, as well as strategic alliances in Beijing and Shanghai. Our services are performed by a total of around 860 employees, including nearly 200 Taiwan-qualified lawyers, 50 foreign lawyers, over 100 Taiwan patent agents/patent attorneys, more than 100 technology experts, and specialists in other fields such as Taiwan- and U.S.-certified public accountants, as well as the PRC patent attorneys and PRC-qualified lawyers of our strategic alliances.

www.leeandli.com

理律法律事務所
LEE AND LI
SINCE 1965 ATTORNEYS-AT-LAW
關懷・服務・卓越
we care・we serve・we excel

United Kingdom


Sally Shorthose


Toby Bond


Emma Drake


Pieter Erasmus

Bird & Bird LLP

1 Digital Health

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

Apps, programmes and software used in the health and care system – either standalone or combined with other products such as medical devices or diagnostic tests.

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

The key emerging digital health technologies in the United Kingdom (**UK**) are as follows:

- 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 distance support to patients either through healthcare practitioners or AI; the integration of telemedicine services with digitised health systems.
- Health data analytics – the digital collation, analysis and distribution (including on a commercial basis).
- Personalised medicine – using genomics to get a faster diagnosis of a condition and being given personalised treatments based on that diagnosis.

1.3 What are the core legal issues in digital health for your jurisdiction?

The two core legal issues are:

- compliance, in the digital collation and handling of patient data, with the requirements of the UK's General Data Protection Regulation (**UK GDPR**) and the UK Data Protection Act 2018 (**DPA**); and
- compliance, in delivering digital health services, with the relevant UK healthcare regulatory regime. For example, in the case of telemedicine services, the regulatory regime is not yet fully updated to deal with the issues arising from the delivery of telemedicine services.

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

Certain sources estimate that the UK healthcare IT and digital market is currently valued at around £5 billion, although this is likely to grow significantly.

1.5 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 in the UK include:

- Babylon Health;
- Teladoc;
- Cera;
- Huma;
- DnaNudge; and
- Lumeon.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

England, Scotland, Wales and Northern Ireland each have their own regulatory regime and competent authority. In England (approximately 85% of the UK population), the relevant legislation is the UK Health and Social Care Act 2008. Broadly equivalent legislation and regulators are in place in the other UK nations. All national regimes require all providers of regulated healthcare services (including e.g. telemedicine) to meet the requirements of the applicable legislation and to register with the relevant national regulatory body in order to be able to legally undertake those services.

Medicines and healthcare products (including software as a medical device (**SaMD**)) are governed across the UK by the UK Human Medicines Regulations 2012 and the UK Medical Device Regulations 2002 (**MDR 2002**), as amended.

General legislation such as the Electronic Commerce Regulations 2002, the Consumer Rights Act 2015 and the Consumer Protection from Unfair Trading Regulations 2008 may also be relevant to digital health.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health 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 (England, Northern Ireland, Scotland and Wales).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Consumer health devices are, to the extent they are "medical devices", covered by the MDR 2002, as amended. All medical devices need to meet the applicable UK Conformity Assessed (UKCA) marking requirements in these regulations and must be registered. However, as part of the guidance regarding transitional arrangements published by the Medicines and Healthcare products Regulatory Agency (**MHRA**) in October 2022, manufacturers will be able to continue to place CE marked medical devices on the Great Britain market until the end of June 2024. There will be separate requirements for certain medical devices placed on the Northern Ireland market, which is currently aligned with the EU regime.

All consumer devices that are not regulated as medical devices under the MDR 2002 are regulated by the UK General Product Safety Regulations 2005 and those other CE/UKCA marking regulations which apply to the specific product, e.g. UK Electrical Equipment (Safety) Regulations 2016, etc. Evidence of compliance with applicable CE/UKCA marking laws and regulations must be compiled and maintained by a nominated responsible person in the UK where the manufacturer is based outside the UK. Based on recent guidance, manufacturers of the aforesaid consumer devices that are not regulated as medical devices may continue to use the CE marking on the Great Britain market until 31 December 2024.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

For the healthcare regulatory regimes in the four nations, the relevant regulatory authorities are:

- England – Care Quality Commission.
- Scotland – Healthcare Improvement Scotland.
- Wales – Care Inspectorate Wales.
- Northern Ireland – The Regulation and Quality Improvement Authority.

The MHRA is the competent regulatory authority for medical devices and maintains the register of such devices. Various regulatory bodies have responsibility for particular UKCA marking regulations.

2.5 What are the key areas of enforcement when it comes to digital health?

Primary areas of concern:

- Telemedicine service providers: Loss of registration (and thus loss of ability to legally provide healthcare services) for failing to comply with the relevant standards. Serious criminal conduct may result in prosecution and significant fines.
- Medical devices (including software): Failure to comply with the relevant regulations can result in the product being recalled and withdrawn from market by the MHRA, and, if there is serious failure to comply with the regulations, an unlimited fine and/or six months imprisonment on conviction.
- In general: Privacy and data security.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

SaMD is governed by the MDR 2002, as amended. In 2022, the MHRA published a "roadmap" for its *Software and AI as a Medical Device Change Programme* published the previous year. Though, the roadmap provides that the changes will primarily come in the form of guidance, some secondary legislation is expected. For example, the MHRA intends to develop secondary legislation to account for cybersecurity and IT risks relating to the large amount of personal data generated in the field of SaMD. The MHRA have further indicated that their aim is to bring new regulations into force by July 2024. The exact outcome of the programme and roadmap on the regulatory landscape in the UK is not yet clear but should become so in the coming years. It will also be interesting to see if any aspects of the EU Medical Devices Regulation are reflected in the new UK legislation.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

See question 2.6 above.

3 Digital Health Technologies

3.1 What are the core 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 (**WEEE**).
  - 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.
- **Natural Language Processing**
    - No particular issues.

3.2 What are the key issues for digital platform providers?

Data protection and especially the lawful transmission, storing processing and use of data – and ensuring adequate consent to such use has been obtained. International data transfers remain a compliance hot topic.

The digital platform provider must ensure, to the extent it is responsible, 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.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

- 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.
- 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 (e.g. step counts, sporting performance, etc.).
- Identifying the appropriate legal basis for processing data and obtaining any necessary consent.
- Carrying out a Data Protection Impact Assessment (**DPIA**), if required (as is likely) 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.
- Ensuring that any overlapping requirements related to rules on patient confidentiality are met.

4.2 How do such considerations change depending on the nature of the entities 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.

4.3 Which key regulatory requirements apply?

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 (**PECR**) restricts 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 misuse of private information (**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.
- Organisations should be aware that the UK Government has recently laid draft legislation to review UK data protection law, including provisions that will alter requirements on accountability, further processing and definitions of consent. A stated aim of the Government is the lessening of the burden on organisations carrying out research. A close eye should be kept on these developments throughout 2023.

4.4 Do the regulations define the scope of 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 question 4.3 above, there are overlapping restrictions under contract, soft law and confidentiality/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 What are the key contractual considerations?

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 preapproved 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).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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).

4.7 How are issues with 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. It further requires controllers to ensure that any individuals are not subject to substantial and entirely automated decision-making without explicit consent, contractual necessity or legal obligation.

The UK's data protection regulator, 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.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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.

5.2 How do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The preceding answers, in particular for questions 4.1, 4.3, 4.5, 5.1 and 5.2, have covered the key regulatory requirements applicable to the sharing of personal data in a digital health context.

6 Intellectual Property

6.1 What is the scope of patent protection?

Monopoly patent protection is available for novel, non-obvious products or processes which have industrial application. Fees are payable on application and renewal. Protection lasts 20 years from the date of application once the patent is granted (see UK Patents Act 1977).

6.2 What is the scope of copyright protection?

The right to prevent copying, dealing in copies, issuance of copies to the public, performance, broadcast, or adaptation for (relevant works only):

- Literary, musical, artistic works (including software) – life of author plus 70 years.
- Published sound recordings – 70 years from date of publishing.
- Broadcasts – 50 years from date of broadcast.

Copyright (generally) arises on creation and fixation of the work, with no requirement for registration. (See UK Copyright, Designs and Patents Act 1988 (**CDPA**).)

6.3 What is the scope of trade secret protection?

Common law of confidence protects trade secrets. It 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. However, the common law of confidence provides stronger and more comprehensive protection.

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

IP rights in technology developed in academic institutions usually vests in the academic institution. The institution will typically seek to license the technology either to existing businesses or via the creation of a spin-out company to commercialise the technology.

There are no specific laws governing academic technology transfer.

6.5 What is the scope of intellectual property protection for software as a medical device?

Software is only patentable in the UK to the extent that it meets the requirements in the UK Patents Act 1977. These requirements are stringent and difficult to meet for software. Generally, however, software will be protected as a literary work under the CDPA (see question 6.2).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

Following the decision *in Stephen L Thaler v The Comptroller- General of Patents, Designs And Trade Marks* [2021] EWCA 1374, an AI device cannot be named as an inventor of a patent in the UK. In October 2021, the UKIPO issued a public consultation on whether the Patents Act 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 which 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 are the core rules or laws related to government funded inventions in your jurisdiction?

Government funding for innovation is available in the UK. This funding is classed as a subsidy and therefore must be consistent with WTO rules, the EU-UK Trade and Cooperation agreement and other bilateral UK Free Trade Agreements.

7 Commercial Agreements

7.1 What considerations apply to 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, so the joint owner might find themself in an invidious situation if complete clarity is set out regarding the permitted uses a joint owner may have over the IP.

There may be better ways of approaching this – have ownership following the ownership of background on which the improvement is made or assign it in accordance with predetermined fields of use. Royalty payments and licences to background technology should also be provided for.

7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

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.

Public sector healthcare providers often have very strict rules (even to the extent of bureaucracy) which can mean that negotiation of IP rights, for example, can be difficult to deviate from the norm.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

The statistical and pattern recognition capabilities of machine

learning have a wide range of possible applications in the digital health context. These encompass activities which are trivial for any human to complete but challenging for traditional computer systems (e.g. converting handwritten medical records into text) and those which require many years of human expertise (e.g. detecting breast cancer in mammograms). Their use also covers the full range of potential medical purposes from diagnosis, prevention, monitoring, prediction and prognosis of disease to its treatment and alleviation. Applications currently receiving particular attention are the use of pattern recognition techniques to detect abnormalities in medical imaging data. Olfactory AI is also emerging as a new potential diagnostic technique for certain diseases.

However, any digital health problem which involves the identification of signals in a noisy environment is potentially susceptible to the use of machine learning.

Machine learning can also be applied to the manner in which digital health services are delivered. Natural language processing can, for example, be used to facilitate human interaction with systems which are themselves based on machine learning techniques. Potential applications include "chat bots" combined with expert diagnostic systems to replicate a doctor's consultation. Current systems are limited to diagnosing specific conditions in tightly controlled situations. Future systems will generalise this approach to broader diagnostic platforms with general application. Recent advances in language models and generative AI may also open new possibilities for synthesising and communicating information in a healthcare setting.

8.2 How is training data licensed?

Under English law there is no single property right which applies to data *per se* and there is a general reluctance to treat information as a form of property. There may, however, be legal rights which may, depending on the nature/source of the data, be used to control access to, use and disclosure of training data. These include rights in confidential information along with IP rights in the data elements (e.g. copyright, where applicable) or in an aggregation of data (e.g. copyright in original databases or EU database rights).

Where these rights exist, they can form the subject matter for a contractual licence to training data, e.g. an IP licence and/or knowhow licence. The English courts have also recognised that it is possible to impose contractual restrictions on access to, use and disclosure of data even where that data is not protected by other rights. Training data can therefore also be licensed on a purely contractual basis under English law. The possibility of granting a purely contractual licence does not, however, give rise to some general right of "ownership" in the data being licensed.

Unless they refer to intellectual property rights in the data, reference to "ownership" of data in licences may give rise to confusion as this term has no clear legal meaning under English law.

Well-drafted data licences will commonly focus on the rights and restrictions regarding access, use and disclosure of the data and will only refer to ownership in the context of intellectual property rights in the data. They will also address (often complex) issues relating to access, use and disclosure of derived data which is created by the licensee using the licensed data. Data provisions in AI service agreements should also consider the status of meta-data which may be generated through customer interactions with the system.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 which underly 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 machine learning 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 machine learning 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 machine learning 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.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Many machine learning projects often involve collaboration between a party with expertise in deploying machine learning and another party with access to the data required to train a machine learning system to solve a particular problem. Common commercial issues which 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 which 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 which 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 intellectual property 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 which is used to provide the service, or potentially to develop new AI models for use in a different context.

Customers may resist contractual terms which 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.

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 (**CPA**) 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 GDPR might create joint and several liability between partnering organisations if GDPR noncompliance 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, Scottish 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 post-Brexit, at least in the short term.

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 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, and these regulations can vary from jurisdiction to jurisdiction – no broad-brush approach will be applicable. It is also a fast-moving market and keeping up with the changes in regulation is 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, MDR and WEEE.
- Consider competition – are they first, second or third to market?
- Consider patent protection – has this been secured where applicable and have they taken steps to protect and exploit unregistrable IP, such as trade secrets?
- Do they own all necessary IP?
- Do they have good supply and service contracts in place, and secure sources of hardware?

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 aforementioned reform plans in the field of medical device regulation indicate that the regulatory environment is undergoing significant change to "catch up".

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* (**ABHI**) plays a key role in representing the industry to stakeholders, such as the Government, NHS and regulators.

Lobbying in the UK is less formalised, although ensuring that the particular digital health solutions meet certain criteria such as the NICE Evidence standards framework for digital health technologies would improve the likelihood of widespread adoption.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

This would depend on the product in question. From an England perspective, while there may not yet be specific publicly funded provision of general health apps *per se* direct to patients, the provision of, e.g. telemedicine may, under certain circumstances, be funded via the NHS. This would be an area to keep a close watch on since the recent launch of the NICE Office for Digital Health, which intends to, amongst other things, work with strategic partners to improve digital health approval pathways and reimbursement policy.

10.7 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.

A trend to watch in 2023 is the increased use of genomic data and the resulting growth of precision diagnostics. As part of the Genome UK: 2022 to 2025 implementation plan, the UK Government is investing a total of £178 million for the research and implementation of genomic medicine. While the regulatory and data concerns highlighted above are sure to apply as genomic data is harnessed at scale, other concerns may develop as the regulatory landscape struggles to cope with such rapid developments in genomic technologies.

We can expect to see further disruption to the medical device and life science sectors, as the use of smartphones and social media continue to transform the way that people manage their health. The practice of medicine has already been transformed by software and we expect this trend to continue, whilst interactions between patients and providers are fundamentally altered and boundaries blurred.

Acknowledgment

The authors would like to thank Hadrien Espiard for his invaluable assistance in the writing of this chapter. Hadrien is a trainee solicitor at Bird & Bird LLP, based in London.

Sally Shorthose is a Partner in the Life Sciences and Intellectual Property Group at Bird & Bird LLP, based in London and Dublin, and is the joint head of the International Life Sciences Regulatory Group. Before her return to private practice in 2001, she had spent 11 years working in-house in senior roles in the Life Sciences industry, including several years as Legal Director of the Novartis Group in the UK. She now specialises in transactional IP work and life sciences regulatory and commercial work and regularly undertakes due diligence and freedom-to-operate projects. She is the editor of the Kluwer Law publication, the *EU and UK Guide to Pharmaceutical Regulatory Law*, the latest edition of which was released at the beginning of 2023, and is a regular speaker internationally on all types of IP and regulatory issues. She has spent much of the last three years leading the Brexit advisory team at Bird & Bird.
Solicitor – England & Wales, 1988.
Solicitor – Ireland, 2017.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7982 6540
Email: sally.shorthose@twobirds.com
URL: www.twobirds.com

Toby Bond is a Partner in Bird & Bird's Intellectual Property Group, based in London. Much of his work focuses on helping clients navigate issues relating to the protection and commercialisation of data as they take advantage of the power of big data analytics and AI. He has a particular interest in the wider intellectual property issues arising from the development and deployment of AI systems. Toby also advises clients on medical devices legislation and his broader experience covers CE marking, EU batteries legislation, REACH/CLP, RoHS, WEEE and Electromagnetic Compatibility, with a particular focus on emerging technologies including IoT and AI.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6718
Email: toby.bond@twobirds.com
URL: www.twobirds.com

Emma Drake is a Legal Director in Bird & Bird's Privacy and Data Protection Group. She works with a variety of healthcare and life science clients, from traditional pharmaceutical companies to health informatics providers to new entrants handling personal data in the context of wellness apps or new technology. She has helped clients on diverse topics spanning application of research exemptions, anonymisation, assessing the compliance of new medical technologies, patient support programmes and the processing of data for pharmaceutical regulations such as pharmacovigilance or restrictions under the ABPI code.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6728
Email: emma.drake@twobirds.com
URL: www.twobirds.com

Pieter Erasmus is a Senior Associate in the Intellectual Property Group in London, with a focus on regulatory and commercial 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 advice in relation to a broad range of matters in these fields, including pharmaceuticals, medical devices, general healthcare, clinical trials, marketing and advertising of health products, etc. Pieter's experience further includes corporate and commercial work, including transactional work and the drafting of a wide range of general and bespoke commercial agreements in the life sciences and healthcare sectors. He is a co-author of the Kluwer Law publication, the *EU and UK Guide to Pharmaceutical Regulatory Law*, the latest edition of which was released at the beginning of 2023. Before joining Bird & Bird in 2019, he spent over six years working at the Johannesburg offices of Africa's largest law firm.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7905 6217
Email: pieter.erasmus@twobirds.com
URL: www.twobirds.com

USA


Roger Kuan


Jason Novak


Susan Linda Ross

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 technologies in your jurisdiction?

The key technology areas in digital health 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 (IoMT), 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).

1.3 What are the core legal issues in digital health for your jurisdiction?

Some core legal issues in digital health are:

- Patentability of digital health technologies, especially with respect to innovations in software and diagnostics.
- Data privacy and compliance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Consumer Privacy Act (CCPA) as amended recently by the California Privacy Rights Act (CPRA), the California Genetic Information Privacy Act (GIPA), the Virginia Consumer Data Protection Act (CDPA), and the federal Health Information Technology for Economic and Clinical Health Act (HITECH Act).
- The Federal Food, Drug and Cosmetic Act (FFDCA, FDCA or FD&C Act), which regulates food, drugs and medical devices. The FFDCA is enforced by the US Food and Drug Administration (FDA) which is a federal agency under the US Department of Health and Human Services (DHHS). Relevant FDA regulations and programs related to digital health include 510(k) certification, Premarket Approval (PMA), Software as a Medical Device (SaMD), Digital Health Software Pre-Certification Program (Pre-Cert Program) and Laboratory Developed Test (LDT) regulated under the Clinical Laboratory Improvement Amendments (CLIA) program.
- Practice of Medicine Laws that relate to licensure of physicians who work for telemedicine and virtual health companies. These can be state-specific or part of the Interstate Medical Licensure Compact Commission (IMLCC), which regulates the licensure of physicians to practice telemedicine in the list of member states.
- Stark Law and Anti-Kickback Statutes that apply to telemedicine and virtual health providers who enter into business arrangements with third parties that incentivise care coordination and patient engagement.

1.4 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 2020 range from a low of $39.4 billion to a high of $181.8 billion.

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

- Optum.
- Cerner Corporation.

- Cognizant Technology Solutions.
- Change Healthcare.
- Epic.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

In the US, the Federal Food, Drug and Cosmetic Act and subsequent amending statutes (FFDCA, FDCA or FD&C Act) is the principal legislation by which digital health products that meet the definition of medical devices are regulated.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The HIPAA, as amended by the HITECH Act, is a core healthcare regulation related to digital health. The HIPAA sets forth the federal privacy and security requirements for how certain entities must safeguard protected health information (PHI) (inclusive of electronic PHI or ePHI) and how to handle security breaches of PHI or ePHI. In the US, individual states may also have state-specific healthcare privacy laws that pertain to their state residents that might apply to digital health offerings in a particular state and that may also be more strict than the HIPAA. For example, in California, there is the GIPA that was enacted in 2022 and the recently enacted CPRA which amends the CCPA of 2018. The GIPA 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 CPRA amends the CCPA to allow California residents to ask businesses to correct inaccurate personal information that the business has about them and the right to limit the use and disclosure of the sensitive personal information they have collected about them. In Virginia, the CDPA came into effect in 2023 and is the most recent new 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.

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; federal Civil Monetary Penalties Law; and state-law equivalents of each of the foregoing.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Consumer devices are regulated under the statutory and regulatory framework of the FDCA as applies to all products that are labelled, promoted or used in a manner that meets the definition of a "device" under the FDCA. Additionally, the regulations that apply to a given device differ depending on the regulatory class to which the device is assigned and is based on the level of control necessary to ensure safety and effectiveness – Class I (general controls), Class II (general contracts and special controls) and Class III (general controls and PMA). The level of risk that the device poses to the patient/user is a substantial factor in determining its class assignment.

From a consumer standpoint, digital health devices and offerings are also subject to laws and regulations that protect consumers from unfair and deceptive trade practices as enforced on a federal level by the Federal Trade Commission (FTC).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In the US, the DHHS regulates the general health and safety of Americans through various programs and divisions, including the FDA, Centers for Medicare and Medicaid Services (CMS), Office of Inspector General (OIG) and Office for Civil Rights (OCR), among many others.

The FDA is the principle regulatory body charged with administering and enforcing the provisions of the FDCA, including those that relate to medical devices and 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 US.

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, providing the FDA with regulatory advice and support to assist the FDA 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.

2.5 What are the key 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.

2.6 What regulations 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 functionality 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*.

2.7 What regulations apply to artificial intelligence/machine learning 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 of 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 optimize 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:

i. 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.
ii. Strengthen the FDA's encouragement of the harmonised development of Good Machine Learning Practice (GMLP) through additional FDA participation in collaborative communities and consensus standards-development efforts.
iii. Support a patient-centered 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 (PEAC) 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.
iv. 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.
v. Advance real-world performance pilots in coordination with stakeholders and other FDA programs to provide additional clarity on what a real-world evidence generation program 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.

3 Digital Health Technologies

3.1 What are the core 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 the 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 the 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 the HIPAA, CCPA and HITECH Act with regards 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 the HIPAA, CCPA and HITECH Act with regards to voice and WIFI signal data that is collected by the virtual assistant.
  - Data rights to the voice and WIFI 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 the HIPAA, CCPA and HITECH Act with regards 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 therapeutic 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 the HIPAA, CCPA and HITECH Act with regards 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 therapeutic claims for the AI/ML-powered software. Unique issues with evaluating the 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 the HIPAA, CCPA and HITECH Act with regards 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 the HIPAA, CCPA and HITECH Act with regard to the handling of patient imaging data used as 3D printing templates.
  - FDA regulatory issues such as SaMD, 510k, PMA and Biologics License Application (BLA) 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 the HIPAA, CCPA and HITECH Act with regards 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.
- **Natural Language Processing**
  - FDA regulatory issues if the natural language processing (NLP) software is used as part of a medical device or SaMD used for 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 issues for digital platform providers?

The key issues for digital platform providers are:

- Compliance with data privacy laws including the HIPAA, CCPA and HITECH Act with regards 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 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 issues to consider for use of personal data?

Some of the key issues to consider for the use of personal data are:

- What type of personal data is it? If it is PHI, it would thereby be subject to the HIPAA. Contrast this with wellness data, for example, which would appear to be health-related, however, in reality, is separate and distinct and, therefore, not regulated by the HIPAA. Of course, personal data in general is subject to various, state, federal and international data privacy laws.
- 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.
- What are potential secondary uses of the data? Defining secondary uses upfront 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.

- 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 do such considerations change depending on the nature of the entities involved?

Assuming the data under consideration is PHI, in dealing with the HIPAA, a threshold determination is whether one is an entity subject to the 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 (HMOs), 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.

4.3 Which key regulatory requirements apply?

The HIPAA is the primary and fundamental US federal law related to protecting PHI. In relation to the HIPAA, the HITECH, signed into law in 2009, further increased patient rights by financially incentivising the adoption of electronic health records (EHR) 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 US 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.

4.4 Do the regulations define the scope of data use?

Generally, yes, and particularly, the regulations concerning PHI, HIPAA and HITECH define the allowable scope of data use.

4.5 What are the key contractual considerations?

Key contractual considerations depend on what is being contracted. For example, for a data transaction involving entities as part of collaborative research, intellectual property (IP) rights arising out of the research, as well as primary and secondary uses of the data, should be clearly defined. 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 the 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.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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.

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

The US currently has no federal requirements relating to algorithmic "fairness", though that is almost sure to change.

For example, in July 2022, the House Energy and Commerce Committee approved the proposed American Data Privacy and Protection Act (ADPPA) by a vote of 53–2. The bill will create national standards and safeguards for collected personal information, the safeguards also including protections aiming to address potentially discriminatory impacts of algorithms. Although other federal legislation addressing algorithmic decision-making has been introduced in recent years, the ADPPA is the first with overwhelming support and the first to bundle provisions targeting algorithmic accountability and bias with provisions addressing data privacy and security issues. In particular, Section 207 of the ADPPA specifically states that covered entities and service providers cannot "collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on

the basis of race, color, national origin, sex, or disability". In terms of enforcement, the ADPPA will put in place a Bureau of Privacy at the FTC to enforce.

In another example, in 2021, the US Equal Employment Opportunity Commission launched an agency-wide initiative to ensure that the use of software, including AI, ML and other emerging technologies used in hiring and other employment decisions comply with the federal civil rights laws that the EEOC enforces. The EEOC stated that it will be providing guidance to employers, such as this guidance relating to the use of AI and discrimination against people with federally recognised disabilities.

On the other hand, at the state level, municipalities and state legislatures recently began taking steps directed toward preventing AI-induced bias. Illinois enacted the Artificial Intelligence Video Interview Act. Under the Act, effective January 2020, employers are required to notify applicants in writing and obtain their consent if AI may be used to analyse facial expressions during a job interview. Employers must also provide applicants with detailed information about the AI application and how it will be used to evaluate them. In 2021, the New York City Council passed an ordinance (Local law 144) requiring that employers provide notice of the use of AI 10 business days prior to its use, and that the AI tool has been subject to a bias audit within the preceding year. The employer must make the results of the bias audit publicly available on its website.

Somewhat similar to the EEOC, the California Fair Employment and Housing Council (FEHC), on March 15, 2022, published the *Draft Modifications to Employment Regulations Regarding Automated-Decision Systems*, which specifically incorporate the use of "automated-decision systems" in existing rules regulating employment and hiring practices in California. The draft regulations seek to make unlawful the use of automated-decision systems that "screen out or tend to screen out" applicants or employees (or classes of applicants or employees) on the basis of a protected characteristic, unless shown to be job-related and consistent with business necessity.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Key issues include data privacy and security generally, regardless of whether the information is PHI or not. For personal data in general, as discussed herein, entities dealing in data must consider the regulatory requirements across different jurisdictions. For US data sharing, federal and state laws must be considered. For international data sharing, ex-US 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 the HIPAA and HITECH to consider.

From a personal standpoint, each individual must recognise their own personal right to their own 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 may desire.

5.2 How do such considerations change depending on the nature of the entities involved?

As discussed herein and previously, when data is PHI and subject to federal regulations such as the HIPAA and HITECH, 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please see Sections 2 and 4.

6 Intellectual Property

6.1 What is the scope of patent protection?

As relevant to digital health, current US 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 US 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.

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 What is the scope of copyright protection?

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 US 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 establishes *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 US 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 What is the scope of trade secret protection?

Trade secret protection can be used to protect formulas, practices, processes, designs, instruments, patterns or compilations of information that are not generally known to the public and have inherent economic value. Trade secrets have no fixed term; however, 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 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 What is 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 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). An SaMD can also be protectable by patents if it meets US 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?

In the US, both the courts (in *Stephen Thaler v. Andrew Hirshfeld*, E.D.Va., 2021) and the US Patent and Trademark Office (USPTO) have ruled that an AI machine cannot be an "inventor" for purposes of the US Patent Act (35 U.S.C.).

6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

In the US, 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 US industry that is found in all technology transfer programs 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" permits 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 US industry-preference provision before licensing.

7 Commercial Agreements

7.1 What considerations apply to 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 in 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 US 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 considerations apply in 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 the HIPAA and patient-informed-consent requirements. Failure to properly develop and/or execute processes that are compliant with the 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.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

AI, particularly ML, is used in a variety of ways to enable a myriad of digital health solutions. It has transformed the way healthcare data is processed and analysed to arrive at predictive insights that are used in applications as diverse as new drug discovery, drug repurposing, drug dosing and toxicology, clinical decision support, clinical cohort selection, diagnostics, therapeutics, lifestyle modifications, etc.

Precision medicine models that are powered by Big Data analytics and AI/ML can ensure that an individual's uniqueness (e.g., genome, microbiome, exposome, lifestyle, etc.) factors into the prevention and treatment (e.g., therapeutics, surgical procedures, etc.) of disease condition(s) that the individual is suffering from. An example of this would be companion diagnostic tests that are used to predict an individual's response to therapeutics based on whether they exhibit one or more biomarkers.

AI/ML algorithms trained to predict biological target response and toxicity can also 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 promises 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 and will likely lead to drugs that have greater efficacy and fewer side effects for larger groups of patients.

8.2 How is training data licensed?

The rights to training data sets are typically specified in the agreements between the parties sharing the data. Data rights can be licensed in the same manner as other types of IP rights. That is, it can be treated as a property right (either under copyrights, trade secrets or as proprietary information) that can be limited by use, field, jurisdiction, consideration (monetary or in kind), etc. As a result, training data licence agreements can be structured with terms that can apportion ownership and rights (e.g., IP, use, etc.) to the trained ML algorithm and any insights that it generates.

Some representative examples are:

- A healthcare system gives an ML drug-discovery company access to its data set (i.e., patient medical records) and requires a non-exclusive licence to use the ML algorithm that was trained with its data set for any purpose and joint ownership of any IP rights on clinical insights generated by the ML algorithm.
- A pharmaceutical company gives its data set (i.e., clinical trial data) to an ML data analytics company as part of a collaboration and limits the use of the data for the field of hypertension and asks for an option to exclusively license any IP rights arising from insights generated by the ML algorithm trained with its data set.
- Two pharmaceutical companies agree to combine their data sets (i.e., Car-T research data) with one another and carve out specific fields (e.g., leukemia, lymphoma, breast cancer, etc.) that each of them can use the combined data set for.

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

Current US 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 (MPEP) and recent Federal Circuit cases (*Beech Aircraft Corp. v. EDO Corp.*, 990 F.3d 1237, 1248 (Fed. Cir. 1993); *Univ. of Utah v. Max-Planck-Gesellschaft 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 US Copyright Office Practice states that "(t)he US Copyright Office will register an original work of authorship, provided that the work was created by a human being".

8.4 What commercial considerations apply to licensing data for use in machine learning?

A variety of different commercial considerations must be addressed when licensing data for use in ML for digital health solutions.

They are as follows:

- Data Set Definition.
- The contents of the data (e.g., genomic, proteomic, EHR, etc.) being shared.
- The type of data (e.g., PHI, de-identified, 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.

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 US federal, US state, and ex-US 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 US 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 analogs in ex-US 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.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

As discussed herein and previously, digital health (regardless of whether it is Cloud-based), brings 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 US, in several US 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 previously, digital health is a convergence of typically disparate industries: tech; and healthcare. Each industry encounters issues unique to their industry. 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, the FDA, HIPAA/HITECH, 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.

When it comes to data-rights strategy, investors should ensure that these companies have mapped their data from cradle to grave; from where it originates, through upstream handling by other entities, and to downstream deployment. Investors should ensure companies secure the necessary consents and data rights to use and deploy the data as it sees fit. If any of the data lines are broken by bad data-rights agreements or lack of (or proper) consent agreements, the static and dynamic models trained by the data will be in peril.

For IP strategy in this arena, investors should ensure companies demonstrate a strong IP strategy centred around a product road map. Rather than filing patent applications for filing sake, IP strategy timed on product development aligns investors with the company's underlying motivations. This includes Freedom to Operate (FTO) analyses, which often should not be properly conducted until the product is substantially developed. Investors often pressure companies for FTOs, but early analyses on uncompleted products do not adequately protect the final product and incur additional costs for additional analyses in the future.

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 two 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 US, one that may continue for a substantial period of time, 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 US include the: American College of Radiology; American Board of Medical Specialties; American Medical Association; and American Board of Professional Psychology.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

From a US industry standpoint, payors continue to observe inconsistency in regard to the reimbursement of digital health-related therapies and treatments. Further, from a government payor program perspective, government review of proposed regulations continues in an effort to ascertain how best to determine if a particular digital health-related device is clinically beneficial to, or reasonable and necessary for, a government healthcare program 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 programs (whether government or private based) that are currently available and that vary by payor program. 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 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.

Moving forward, there are both existing challenges and new emerging issues that need to be overcome in order for Digital Health Technologies to fully realise its promise to take healthcare into the 21st century.

Most of the remaining challenges relate to industry-wide coordination and standard setting around health data interoperability and clinical adoption of digital health tools. Interoperability of EHR continues to be an industry-wide issue that poses a significant barrier to efficient and effective EHR data exchanges and sharing between Digital Health Ecosystem constituents. This significantly hampers agile aggregation of the EHR data that is the lifeblood of the many AI/ML-powered digital health tools. The lack of a standardised EHR data format in the US is one of the root causes of the EHR interoperability issue and it has somewhat nullified the advantage that the US holds in being domicile to a large volume of heterogenous population EHR data over other countries in the world.

This same lack of industry coordination and standard setting has also played a part in slowing the wide-spread clinical adoption of Digital Health Technologies by clinicians. Until recently, physician certification bodies have not routinely published clinical algorithms that outline how digital health tools should be utilised to help in diagnosing and treating patients. In fact, the American College of Radiology has only recently started releasing formalised use cases for how AI software tools can be reliably used in the clinic.

On the horizon, there are a number of emerging concerns that have only begun to surface and take on more prominence. A sample of those are:

1. Data bias: In digital health, this refers to the systematic error or prejudice in the data and algorithms used to develop Digital Health Technologies. This can lead to discriminatory outcomes and affect patient care, particularly for underrepresented or marginalised populations. For example, if the training data used to develop a predictive algorithm for a certain medical condition is mostly comprised of patients from a single demographic group, the algorithm may not accurately predict the outcomes for patients from other demographic groups, leading to biased results.
2. Evidence-based efficacy: There is a growing need for rigorous, evidence-based research to demonstrate the effectiveness of digital health products and to guide their clinical adoption.
3. Equity and access: Ensuring that digital health tools are accessible and affordable to all populations, regardless of socioeconomic status, is becoming increasingly important.
4. Workforce development: The digital health industry is facing a shortage of trained professionals, including clinicians, data scientists and software engineers, who can effectively utilise and develop digital health tools.

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 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, California 94104-1609
USA

Tel: +1 628 231 6810
Email: roger.kuan@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

Jason Novak's practice was specifically created to focus on advising entities, both large and small, on the various legal issues that can arise with emerging technologies in the healthcare, food and life sciences industries, with a particular and targeted focus on "convergence" technologies (e.g., digital health, personalised/precision medicine, alternative protein) that operate at the intersection of multiple industries.
Jason has extensive experience in IP and data rights strategy. For data rights, Jason advises clients on transactions, protection and general strategy. On the IP front, Jason's experience extends to patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in- and out-licensing, freedom-to-operate, various types of due diligence, IP training, risk recognition and management and dispute resolution.

Norton Rose Fulbright
555 California Street, Suite 3300
San Francisco, California 94104-1609
USA

Tel: +1 628 231 6811
Email: jason.novak@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

Susan Linda Ross is based in Norton Rose Fulbright's New York office with a practice focused on technology and US privacy matters.
Sue has extensive experience with negotiating, drafting and interpreting computer hardware and software, SaaS, consulting, outsourcing, Internet, electronic signatures, web hosting, application service providers and non-disclosure agreements. She is also experienced with preparing website terms and conditions and privacy policies.
Sue also handles US privacy matters, including security breach laws, as well as assisting clients with their questions and compliance efforts relating to Red Flag Rule, HIPAA Privacy and Security Rules, Gramm-Leach-Bliley, Telephone Consumer Protection Act, CAN-SPAM, CCPA and FACTA. Sue has assisted clients with privacy and information security questions relating to the PCI-DSS, provided counselling on a wide variety of matters that raised privacy issues and created privacy policies for corporations, as well as for web sites.

Norton Rose Fulbright
1301 Avenue of the Americas
New York, New York 10019-6022
USA

Tel: +1 212 318 3280
Email: susan.ross@nortonrosefulbright.com
URL: www.nortonrosefulbright.com

Predicting Risk and Examining the Intersection of Traditional Principles of Product Liability Laws with Digital Health


Eric Alexander


Gerard Stegmaier


Jamie Lanphear


Michael Rubayo

Reed Smith LLP

Introduction

There is a somewhat old saw in product liability law that "law lags science; it does not lead it."[1] In the rapidly changing field of digital health, including the increasing use of software in a wide range of medical devices, law definitely lags science. While the United States Food and Drug Administration ("FDA") has issued a range of guidance documents intended to help fit digital health and software within the larger regulatory scheme for medical devices, technological advances, including artificial intelligence ("AI"), are setting a brutal pace – with product liability law changing at a comparatively glacial pace. The resulting gap is creating an exponential increase in technical, legal, and regulatory debt – some of which will most likely end up rooted in novel product liability concerns.

At its core, product liability law applies to *products* and software has generally been considered a service or intangible, not a product.[2] One consequence has been that companies that develop and sell software to the public, or companies that use software in a product that is sold to the public, have managed their possible liability for injuries or loss primarily through contractual provisions. Software is typically licensed (rarely sold) and under particular terms that include limit or cap liability, disclaim most, if not all, warranties, prevent third party beneficiaries, and contain aggressive *force majeure* provisions in efforts that have mostly shielded software developers from liability arising out of or relating to the performance (or non-performance) of their code.

Further, software is increasingly distributed and licensed in a form that does not represent its final version and often the purveyors expressly disclaim that they are not selling software at all but rather providing access to a "service." Software is often updated and changed during its lifecycle and the ability to license and distribute non-finalised programming allows for software developers to take on "technical debt." Technical debt refers to a practice of prioritising delivery of a software program or feature as quickly as possible instead of as perfectly as possible.[3] When developing software for digital health companies or for use in or as a medical device, the technical debt may compound into regulatory or legal risks as the relationship between product liability law and the law of software licensing and development, as practised, seem increasingly at odds with software being recently recognised as a product by more than one court, including in connection with electronic health records software.

Because of the significance of these issues, we seek to explain the basics of product liability law, FDA's regulation of medical devices, and recent legal developments in the context of traditional software development and risk allocation. We aim to aid software developers in digital health and those that advise them in anticipating, preparing for, and responding to this potentially rapidly changing liability landscape.

Digital Health: FDA Regulation of Medical Devices Including Software

Software has been used in medical devices since at least the 1960s. Devices containing both hardware and software components, such as MRI systems, required FDA to review not only the hardware components of the device, but also its software. In 1989, FDA issued its first draft policy on how it planned to regulate computer-based or software-based devices. As the use of computer and software devices grew and the types of devices became more complex, however, FDA determined that the draft policy had become obsolete and withdrew it in 2005. Since then, FDA has issued several guidance documents to aid manufacturers in the design, development, marketing, and servicing of safe and effective software devices.

The current framework for determining whether and how software used for medical purposes is considered a medical device, subject to FDA regulation, is complex. The Food Drug and Cosmetic Act ("FDCA") defines a device as "an instrument, apparatus, implement, machine, contrivance, implant, *in vitro* reagent, or other similar or related article, including any component, part, or accessory" intended to prevent, diagnose, mitigate, treat, or cure a disease without achieving its intended purpose through chemical action.[4] This definition excludes drugs and biologic agents, such as vaccines, but includes a full range of products, from a simple tongue depressor to AI-based devices used to alert providers of a potential stroke in patients. In 2016, Congress amended the definition of device to exclude certain types of software, including those intended to display, store, transfer, or convert formats of medical device data and results. Software intended to maintain or encourage a healthy lifestyle that are unrelated to the prevention, diagnosis, mitigation, treatment, and cure of a disease or condition are also excluded.[5]

FDA has provided details about the types of software that meet the definition of device.[6] Generally speaking, FDA considers software intended to diagnose, prevent, mitigate, treat, or cure a disease, or one intended to affect the structure of the human body, as meeting the definition of device.[7] Examples include software that can detect and diagnose a stroke in patients by analysing MRI images and software that can process images to aid in the detection of breast cancer. Certain medical mobile applications, such as apps designed to measure a patient's glucose level, are also classified as medical devices subject to FDA regulation. It is important to note that when determining whether software or a mobile app meets the definition of device, the focus is

on the software's function, not its platform. Software intended to interpret EKG waveforms to detect heart function irregularities, for example, meets the definition of device, regardless of whether it runs on an EKG machine or mobile app.[8]

Despite the fundamental differences between hardware devices and software devices, FDA has not instituted a specific approach for regulating software devices outside of its normal review process based on their risk classification. Class I devices, such as software that solely displays readings from a continuous glucose monitor, are considered low-risk and are subject to the lowest degree of regulation. Class II devices are those of moderate risk, and may include software that analyses medical images, such as mammograms. Most Class II devices require FDA clearance of a 510(k) premarket submission before they can be marketed. Alternatively, for novel medical devices that are low-to-moderate risk, manufacturers may submit a *De Novo* request for FDA to classify its device as Class I or Class II. Class III devices, such as an implantable defibrillator, pose the greatest risk to patients and are subject to the greatest degree of regulatory oversight. Such devices must obtain premarket approval ("PMA") from FDA before they can be marketed. For all classes of devices, FDA's review process focuses on safety and efficacy. FDA does not evaluate premarket submissions with an eye toward issues related to privacy and security, unless those considerations pose a potential risk to patient safety.

With the increased risk of cyber vulnerabilities inherent in software devices, cybersecurity has become a critical focus of FDA. FDA's concerns about cybersecurity relate to the impact cybersecurity threats pose to device functionality and patient safety, not privacy. FDA expects device manufacturers to identify cybersecurity vulnerabilities that increase the potential risk of patient harm and put mitigations in place, such as limiting unauthorised access to device software and using design approaches that will maintain the device's functionality, even after its security has been breached.[9] Manufacturers are expected to manage cybersecurity risks throughout the device's lifecycle by, for example, issuing regular software updates and patches and reporting to FDA any suspected cyber attack that impacted the device's performance. Information concerning how a manufacturer has addressed cybersecurity risks and how it intends to monitor and manage those risks throughout a device's lifecycle is a critical component of a PMA and 510(k) for medical device software.[10]

As healthcare continues to become more digital, the prevalence of devices reliant on software continues to grow. Modern-day devices are increasingly connected and rely on data analysis from many sources and over time to perform their functions. Ranging from smart watches tracking your steps, heart rate, and oxygen levels, to insulin pumps automatically managing an individual's blood sugar levels, devices use software to collect and use data. However, as demonstrated in recent guidance regarding Device Software Functions and Mobile Medical Applications, FDA has been careful to not imply that *all* software utilised for medical purposes satisfies the definition of device or will be subject to its regulatory authority. Some of the software functions FDA has announced it considers to be a device, subject to its regulatory authority, include:

- functions that control or analyse data from the device;[11]
- functions that transform a mobile platform into a regulated medical device by using attachments, display screens, or sensors;[12] and
- functions that perform patient-specific analysis and provide specific outputs or directives for use in the diagnosis, treatment, mitigation, cure, or prevention of a disease or condition.[13]

FDA's recent guidance illustrates the role software increasingly plays in digital health and determinations regarding whether a medical product meets the definition of device and/or is subject to FDA regulation. The guidance does not demonstrate a specific concern by FDA to protect personal data collected, analysed, and stored by the software, but rather to ensure no physical harm will be done to patients because of software malfunctions.[14] This is demonstrated by the lack of regulation for software focused only on recording or tracking health information, providing access to patient health information, or transferring health information from one healthcare professional to another, among other functions.

Product Liability

Historically

Devices

Traditional United States ("U.S.") product liability law, including as it applies to medical devices, can be hard to reconcile with existing legal models for software licensing and emerging AI and machine learning developments. First of all, unlike in the European Union or other parts of the world, there is no single source of U.S. authority that can be consulted to determine the law. Each state has its own law on product liability. Some have fairly comprehensive Product Liability Acts, but most have law shaped by the decisions of mostly state appellate courts that address the issues before them. Federal court decisions predicting state law consistent with *Erie Railroad Co. v. Tompkins*,[15] may be persuasive or they may be rejected by a subsequent state appellate court decision or legislative act. There may be issues addressed definitively by most states, but not at all by others. The resulting patchwork makes it difficult to characterise what "the law" is on a number of product liability issues. Even the Restatements of Torts have limited authority, do not address all product liability issues, and are updated infrequently.

Generally speaking, subject to variability in the defences available because of the regulatory status of the device and state law at issue, product liability for medical devices has largely resembled product liability law for other products. Liability for medical devices is most often predicated on an inadequacy in the disclosure of the device's risks, an issue with the device's design that makes it unduly risky, or a deviation from specifications in the manufacture of the particular device used by or implanted in the plaintiff.[16] A warnings claim requires proof that an adequate warning would have changed the outcome in the case, as by making the prescribing physician choose a different device that would not have produced the same outcome. A design claim often requires proof that the design was unreasonable in comparison to the alternative designs and knowledge at the time and that a device with an adequate design (i.e., without the alleged design defect) would have avoided the plaintiff's injuries. A manufacturing claim requires proof that the particular device caused harm to the plaintiff because it deviated from how it was supposed to be when it left the manufacturer's control. Each of these liability theories requires proof that the device caused the plaintiff's injuries and alleged damages. These theories do not make a manufacturer an insurer of all harms caused by its products, but require some showing of unreasonable conduct by the manufacturer or unreasonable risks attendant to the design of its product.

Three of the most significant issues determining the potential liability for a medical device manufacturer are whether the device requires a prescription, the device's regulatory status, and whether the applicable state law imposes duties beyond those

described above. The first issue is typically referred to as the "learned intermediary doctrine," which means that the duty of the manufacturer of a prescription device or other medical product runs to the physician who prescribes it, not the patient or general public. There is widespread near-national acceptance of the learned intermediary doctrine for prescription medical devices. This makes sense not just because prescription medical devices cannot be obtained legally without a prescription, but because FDA requires specific physician-facing labeling for prescription medical devices. Moreover, a manufacturer would rarely have a practical ability to ensure that any patient-facing labeling was seen by a patient before the prescription/implant/use of the device.

As discussed above, FDA's risk-classification system divides devices into three classes based on FDA's assessment of risk. This system not only affects the required route to market, but the availability of preemption pursuant to the Supremacy Clause in the U.S. Constitution. The Medical Device Amendments of 1976 ("MDA") include an express provision for preemption of state law claims that are "different from, or in addition to" a federal requirement that relates "to the safety or effectiveness" of a medical device.[17] Since the U.S. Supreme Court decision in *Riegel v. Medtronic, Inc.*,[18] most warnings and design claims against FDA-approved Class III devices are preempted and thus not viable.[19] This is not the case with regard to Class I or Class II devices, which have more limited preemption defences available. *Medtronic, Inc. v. Lohr*,[20] focused on the regulatory requirements of a device cleared before the Safe Medical Device Act of 1990, but has had a lasting impact on preemption for a wider range of Class II devices. Implied preemption under *Buckman Co. v. Plaintiffs Legal Committee*,[21] for claims predicated on violating FDA requirements, applies across classes of devices; however, treatment varies greatly from case to case. Even without preemption, evidence that a device was compliant with the terms of its market authorisation and that the manufacturer complied with all of its obligations can be powerful evidence.

Because of the power of express preemption for Class III devices, some judges have created new duties to impose liability on device manufacturers that are not "different from or in addition to" the requirements imposed by FDA approval. The path is narrow for these purported "parallel claims" because of the interplay with *Buckman's* requirement that liability not be predicated on a violation of a federal requirement. The result is that some courts have found that what might otherwise seem are purely federal requirements, like reporting adverse events to FDA, are also independent requirements of state law. There is wide variation between and within states on the endorsement of novel parallel claims to impose liability on manufacturers.

Some issues relevant to liability for software have less state variability. In general, consistent with the requirement that the product was not changed after leaving a manufacturer's control to impose liability on the manufacturer, product liability generally does not apply to another entity that merely distributed or re-sold the product.[22] In terms of a prescription medical device, the company that designed, manufactured, and sold the device into commerce may be liable under the theories discussed above, but the hospital that purchased it and charged a patient for its use will not be, absent an alteration of the device. Similarly, entities involved with the design or manufacture of the device before it leaves the manufacturer's control, like the manufacturer of a component, will not be liable under product liability principles.

Additionally, courts rarely allow an inference of a "malfunction" to suffice. It may be easy to assume that any medical complication in the anatomic vicinity of a device is due to some device failure. The concept of *res ipsa loquitur* allows a similar inference of negligence in circumstances where the defendant has sole control of the alleged instrument of injury and the injury/accident would not be expected otherwise, such as, where a sponge is found in the abdomen after a surgery, it can inferred that a negligent act or omission by the surgeon or staff in the operating suite left it there. For product liability claims regarding a medical device, however, a doctor's or patient's use of the device is not within the manufacturer's sole control and the injuries at issue are typically not something that occur only when the device fails. As such, a "malfunction" is not assumed even when some injury follows the use of a medical device.

Moreover, while the consideration of causation in medical device product liability cases can be involved, the plaintiff must typically connect a tangible physical injury to the device to recover any damages, including for mental anguish or economic loss. Asymptomatic injuries, fear of a possible injury, or the need for medical screening or possible future medical intervention are typically not compensable. Similarly, care occasioned by the recall of a device because of a potential risk of injury typically will not give rise to liability absent the device actually causing that injury in the plaintiff.

With this background in mind, there are a number of areas where the application of traditional U.S. product liability principles could differ with patient-facing digital health and software-driven medical devices. This is particularly so because software is often updated over time as weaknesses or issues become known or areas for potential improvement are identified. In today's wireless world, the ability to issue software updates and patches is largely expected[23] and whether and how affirmative consent and additional licensing provisions may apply represent on-going issues for many software developers.

The role of updates for patient-facing software-driven medical devices greatly complicates the product liability and risk-prevention analysis. For instance, a defect in design or manufacture is typically measured at the time that the product left the manufacturer's control. If a manufacturer can update software post-sale on its own, then has the product ever left its control? Does the design of a software-driven product become defective at the point updates become available to address a safety issue, but the updates are not made to the plaintiff's particular product for one reason or another? In most states, the duty to warn of risks is also measured as of the time of the sale of the product, with a minority of states recognising a post-sale duty to warn under special circumstances. This makes sense for prescription medical devices, like most products. The manufacturer can provide warnings with its device, but will typically have no mechanism to warn the prescribing physician, subsequent health care providers, and/or the patient (whose identity will almost always be unknown to the manufacturer) of subsequently attained information relevant to the device's risks. Again, this works differently with digital health and software-driven devices, where the relationship with the end-user may often continue post-sale and the ability to update software may go hand-in-hand with the ability to notify an end-user of a post-sale issue. While these issues are not unique to digital health applications of software, the consequences may be more severe and the responsibility for "users" to patch and update the software, therefore, may be much more legally complicated. Moreover, even though devices may only be available by prescription, the learned intermediary doctrine may not apply in some cases where the level of direct and/or continuing interaction between the manufacturer and patient undercuts the rationale for the doctrine. When the doctrine does not apply, the duty to warn runs to the plaintiff/patient directly, which increases the risk of product liability exposure.

Preemption of design or warnings claims involving Class III medical devices could also operate differently for software-driven

devices. For express preemption under the MDA to apply, the plaintiff's theory of liability must be "different than or in addition to" the federal requirements imposed in connection with PMA approval. In the case of a device with software that will be updated over time or where the device utilises AI or machine learning, some courts may doubt that the device at the time of the alleged injury was the same as what FDA had approved. In an arguably analogous situation, the off-label use of FDA-approved Class III devices has generally not defeated preemption of design and warnings claims that would otherwise exist.[24]

Given that product liability law has generally not applied to software, any imposition of product liability would entail making new state law. The dynamic described above in terms of purported parallel claims for Class III medical devices would likely apply with devices utilising software, machine learning, or AI. As noted above, most states do not impose post-sale duties to warn and, when they do, require there to be new information on the risk of the product, so any liability for when and how post-sale software updates are rolled out would require significant expansion. Similarly, detailed requirements for PMA are unlikely to have true parallels in duties imposed by state tort law.

Lawsuits over injuries allegedly due to a failure of software in a medical device might also name entities that contracted with the device manufacturer to develop or update that software. A parallel may be seen in the history of suing manufacturers of raw materials and component parts used in connection with the manufacture of breast implants and other implantable devices. This led to the enactment of the federal Biomaterials Access Assurance Act of 1998, as it was considered to be a matter of "national interest" to protect suppliers of raw materials and components against litigation[25] "to safeguard the availability of a wide variety of lifesaving and life-enhancing medical devices."[26] Should large-scale litigation commence against entities that design or maintain software used in medical devices, similar logic could be used to support federal limitations on liability.

Depending on whether software used in a medical device can be adjusted or personalised by the user or prescribing healthcare provider, the malfunction theory of liability could have more traction than with other devices. If software fails to perform as expected and there is no ability for it to be altered by anyone other than the manufacturer or its agents, then criteria for application of malfunction or *res ipsa loquitur* could apply. Given most software developers routinely seek to disclaim that their software can or will function, including for any particular purpose, this risk should be of keen interest to developers and their advisers.

The typical requirement of a tangible physical injury could also be loosened in product liability litigation over software or software-driven medical devices. Even setting aside potential liability for alleged privacy, which does not require physical injury, the nature of many possible software issues with devices could increase the propensity for claims of liability for fear of injury or increased risk of injury. For example, a false reading on a device that monitors heart rhythm or blood sugar could cause a patient to be concerned about the risk of a particular health outcome or to seek medical care because of the misperception of risk. Other software-related glitches with medical devices could lead to subclinical alterations in medication administration or cardiac stimulation. A software issue across a number of devices at the same time could give rise to a class action asserting product liability claims even without tangible physical injuries in the putative class members.

Software

The Restatement (Third) of Torts defines product as "tangible personal property."[27] Courts across the country have consistently found that software does not qualify as tangible property because it is typically produced for a specific purpose to satisfy the terms of a contract, or is mass produced and licensed out to each user to utilise for their designated purpose.[28] Consequently, courts typically treat software companies differently than device manufacturers by limiting their liability to contract-based theories.[29]

Software-related user licence agreements are intended by their providers to limit and manage risk, including to limit liability. It remains mostly settled law that checking a box or clicking a button or similar affirmative action can demonstrate assent to an agreement, provided the layout and language used is conspicuous and provides reasonable notice of such assent.[30] Incorporation of documentation and acknowledgment of receipt and warnings with software are increasingly commonplace and many software developers take great pains to limit their liability by contract. While courts use "shrink wrap" and "click wrap" terminology routinely in determining the existence of software-related contracts, the touchstone remains whether there is an offer, acceptance, consideration, and legality. Each of these elements is increasingly being contested in litigation and by regulators such as the Federal Trade Commission.

The concept of software liability being governed primarily by contract law is a routine fixture of liability allocation for software developers. Plaintiffs seldom recover on tort claims, with courts tending to conclude that the developer's liability begins and ends with the licence. *Murray v. ILG Techs., LLC*, demonstrates how contract law, not tort law, represents the primary theory used to recover software-related damages.[31] In *Murray*, the plaintiffs alleged damages arising from a bar-exam grading software that erroneously failed a portion of students. The district court dismissed the plaintiffs' product liability claim summarily but allowed the contract claim to proceed.[32]

Product liability trends

The issue of potential product liability for software has been the subject of discussion for some time. As set out above, in 1998, while defining a "product" for purposes of strict product liability as a tangible thing, the discussion accompanying the Restatement (Third) of Torts suggested that software, at least mass-marketed rather than *ad hoc* software, might be considered a product. This speculation was based on shaky ground, as the Ninth Circuit case it cited actually "declin[ed] to expand products liability law to embrace the ideas and expression" found in a book.[33] Over the next two decades, the treatment of software in product liability law did not change much.[34] "Courts have yet to extend products liability theories to bad software, computer viruses, or websites with inadequate security or defective design."[35] The few contrary rulings did not establish a trend, except perhaps in Louisiana. Starting with a ruling from the Louisiana Supreme Court that computer software was "corporeal property" for purposes of taxation,[36] two federal courts later found software to be a product under the unusual "corporeal moveable" definition in the Louisiana Product Liability Act.[37] In addition, an intermediate appellate court in California ruled in 2014 that the company that supplied publishing software to a pharmacy could possibly be subject to product liability for an incomplete drug monograph.[38]

In the last few years, however, the frequency of rulings on this issue has increased and it may be just a matter of time until software is subject to product liability. In *Rodgers v. Christie*,[39] the Third Circuit considered the question in a fairly unusual case of a homicide being blamed on an issue with AI software that ran the New Jersey Public Safety Assessment ("PSA") system used in connection with pretrial services for criminal matters. It held

that the PSA software "is neither 'tangible personal property' nor remotely 'analogous to' it" to qualify as a product under the New Jersey Product Liability Act.[40] In addition to "information, guidance, ideas, and recommendations" not being defined as products under the Restatement (Third) of Torts, "extending strict liability to the distribution of ideas would raise serious First Amendment concerns."[41]

Because of the defences available under the Michigan Product Liability Act, the defendant in *Holbrook v. Prodomax Automation Ltd.*[42] sought to have its software used in connection with an assembly line robot treated as a product. The broad statutory definitions allowed for the conclusion that it was a "component" of a product and thus subject to product liability. The court concluded that the "programming is an 'integral' and 'essential' part of the [assembly] line because... 'without ... the PLC program ... the robotic components would not have been orchestrated to move at all within the line.'"[43] However, the court did limit its ruling to software as a component of a product, noting that the "programming need not qualify as a product itself."[44] By contrast, the conclusion that "programming was completed at the facility does not make it any less a part of the product's design," suggests that some expected downstream modifications may not affect product liability for software as a component of a product.[45]

Because of the quirks in Michigan law, the *Holbrook* decision, like the Louisiana decisions before it, did not signal a sea change in the treatment of software as a product for purposes of tort liability. Indeed, after the *Holbrook* decision, a federal court in Washington issued two orders finding that an online video game was not covered by the state's product liability statute.[46] The game was "software as a service, not an 'object,' hence Plaintiff's product liability claim must fail as a matter of law."[47] Additionally, recent litigation over automobile accidents allegedly caused by distracted driving due to use of software applications on mobile devices has not yet produced direct decisions on whether social media applications/platforms are "products" for purposes of strict liability, because the plaintiffs in those cases have pursued negligence-based theories.[48]

In late 2022, the Fourth Circuit issued its decision in *Lowe v. Cerner Corp.,*[49] which is the first decision that has found software to be a product that is likely to have precedential value outside of one state. At the district court level, the developer and seller of an electronic health records system was granted summary judgment on product liability claims related to injuries to a patient during post-surgery in-patient care, largely because the hospital had made changes to the system after purchasing it.[50] This was so despite the system being "designed to be easily configured by the customer." On appeal, the Fourth Circuit reversed, holding that the plaintiff had presented sufficient admissible evidence of a design defect, a failure to warn, and proximate causation to get to trial on product liability claims against the software developer. However, nowhere in the district court decision, the Fourth Circuit decision, or a vigorous dissent in the Fourth Circuit was there a direct ruling on whether the electronic health records system was a product. That may be because Virginia does not recognise strict product liability. Instead, all recognised product liability claims sound in negligence.[51] Still, a federal circuit decision that takes for granted that an electronic records system – an adaptable software package – is a product subject to the core product liability claims of design defect and failure to warn should not be minimised when projecting the future of digital health law.

The elephant in the room on the role of product liability in allegations of harm from software is the recent creation of a Multidistrict Litigation proceeding in *In re: Social Media Adolescent Addiction/Personal Injury Products Liability Litigation*, pending in the Northern District of California. By its name, this is "products liability litigation" that focuses on parents' allegations that their minor children suffered various harms due to a number of social media platforms. The U.S. Judicial Panel on Multidistrict Litigation characterised the common allegations against the social media platforms being "defective because they are designed to maximize user screen time, which can encourage addictive behavior in adolescents."[52] Because of the nature of Multidistrict Litigation, claims implicating the laws of almost all of the states will be the subject of extensive litigation.[53] This makes it highly likely that the issue of whether strict product liability applies to social media platforms, including the software that runs them, will be decided directly. Those decisions, potentially modified on appellate review, will inevitably influence the legal playing field for potential claims relating to digital health and software-driven medical devices.

New practices of software companies who are manufacturers/sellers

As discussed above, software-development lifecycle best practices are likely to evolve further and familiarity with FDA's risk classification schemes may be a useful starting point for many developers, regardless of whether their software is or may be a medical device. Not only is it possible that companies that develop software for use in or as a medical device will be subject to specific additional requirements, but those that provide software that may be used in digital health or as components in digital health products may find it desirable to take specific additional steps to manage the uncertainty of emerging risks in this area. Greater disclosures regarding the software, specific testing and quality enhancements and improvements, very deliberate approaches to patching and update responsibility and support, and other thoughtful solutions may be helpful to software developers and those who support them. It seems likely that standard-setting bodies and efforts, and additional prescriptive regulations may also come into play. Not only has FDA noted that its authority in this area is limited and should be revisited,[54] but the agency's reluctance to over-classify software used in devices as a "device" and the role of standards is already getting some attention.[55] At the same time, in announcing its National Cybersecurity Strategy March 1, 2023, the Biden Administration stated that because "[s]oftware makers are able to leverage their market position to fully disclaim liability by contract" creating disincentives to use "secure-by-design principles or perform pre-release testing" the U.S. must "begin to shift liability onto those entities to take reasonable precautions."[56] Whether this policy will carry over into digital health and medical devices specifically remains to be seen.[57] In any event, medical device companies, software developers who work with them, and those who assist each with managing and responding to liability risks will benefit from greater understanding of and monitoring this emerging area of the law.

Endnotes

1. *Rosen v. Ciba-Geigy Corp.*, 78 F.3d 316, 319 (7th Cir. 1996) (Posner, J.).
2. "A product is tangible personal property distributed commercially for use or consumption." Restatement (Third) of Torts: Products Liability §19(a) (1998). At the time of this statement, the discussion included the comment that "Under the [Uniform Commercial Code], software that is mass-marketed is considered a good. However, software that was developed specifically for the customer is a service." After the Uniform Commercial Code was

amended in 2005, however, it defined "software" as a "general intangible," not a "good." *Id.* §9-102(42); *see also* U.C.C. §9-102, Commentary, at 4(a); Uniform Computer & Information Technology Act of 2002 §102(a)(35) (likewise defining "information"—as opposed to "goods"—as including "computer programs").

3. *Technical Debt*, Product Plan, https://www.productplan.com/glossary/technical-debt/.
4. 21 CFR 520(h).
5. 21 CFR 520(o)(1)(B); *see also* General Wellness: Policy for Low-Risk Devices (Sept. 27, 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices.
6. *See, e.g.*, Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act (Sept. 27, 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/changes-existing-medical-software-policies-resulting-section-3060-21st-century-cures-act; Policy for Device Software Functions and Mobile Medical Applications (Sept. 28, 2022), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications; Clinical Decision Support Software (Sept. 28, 2022), https://www.fda.gov/medical-devices/software-medical-device-samd/your-clinical-decision-support-software-it-medical-device.
7. Policy for Device Software Functions and Mobile Medical Applications (Sept. 28, 2022), at 6, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications.
8. *Id.*
9. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct. 2, 2014), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices.
10. *See* Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (Apr. 8, 2022), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions.
11. *Id.* Examples include an automatic Insulin pump and digitally controlled blood pressure cuff.
12. *Id.* Examples include attaching blood-glucose strip readers or ECG electrodes, and utilising built-in functionality, such as accelerometers or other sensors, for medical purposes.
13. *Id.* Examples include a dosage calculator for radiation therapy and blood-glucose tracker for abnormal levels.
14. *Id.* at 11 ("FDA intends to apply its regulatory oversight to *only* those software functions that are medical device and whose functionality *could pose a risk to a patient's safety* if the device were to not function as intended") (emphasis added).
15. 304 U.S. 64 (1938).
16. In general, absent unusual facts of a direct relationship between a patient and medical device manufacturer, theories based on express or implied warranties or misrepresentation are unavailable or subsumed within a design or warning theory. Similarly, consumer protection statutes generally do not provide recovery for personal injuries allegedly caused by medical devices or other products.
17. 21 U.S.C. § 360(a).
18. 552 U.S. 312 (2008).
19. True manufacturing defect claims are not preempted because a requirement of approval of a Class III medical device is that what is sold should match the design that was approved and such claims are based on the absence of a match.
20. 518 U.S. 470 (1996).
21. 531 U.S. 341 (2001).
22. According to the Restatement (Third) of Torts, Products Liability §1 (1998), strict product liability "applies only to manufacturers and other commercial sellers and distributors who are engaged in the business of selling or otherwise distributing the type of product that harmed the plaintiff." Some state statutes have similar broad definitions, but the general practice in product liability lawsuits involving medical devices is that manufacturers are the targets and the entities with control over design, labeling, and manufacturing. Indemnity and contribution provisions in contracts between manufacturers and distributors/re-sellers are common and often imposed by law even in the absence of contractual provisions.
23. *See* Vincent J. Vitkowski "The Internet of Things: A New Era of Cyber Liability & Insurance," Declarations, International Association of Claim Professionals, at 3 (Spring 2015) (predicting "IoT devices comprised of integrated hardware and software systems will almost surely be treated as products").
24. *See, e.g., White v. Medtronic, Inc.*, 808 F. App'x. 290 (6th Cir. 2020); *Shuker v. Smith & Nephew, PLC*, 885 F.3d 760 (3d Cir. 2018); *Caplinger v. Medtronic, Inc.*, 784 F.3d 1335 (10th Cir. 2015).
25. 21 U.S.C. § 1601(16).
26. 21 U.S.C. § 1601(15).
27. Restatement (Third) of Torts: Products Liability §19(a) (1998).
28. *See Flores v. Uber Techs.*, No. 19STCV24988, 2022 Cal. Super. LEXIS 9648 (Cal. Super. Ct. L.A. Cnty. Mar. 22, 2022) (holding that software application is a service not a product); *Shema Kolainu-Hear Our Voices v. ProviderSoft, LLC*, 832 F. Supp. 2d 194 (E.D.N.Y. 2010) (software not subject to tort liability because of existence of a licence); *Murray v. ILG Techs., LLC*, 378 F. Supp. 3d 1227 (S.D. Ga. 2019) (granting summary judgment against software-related product liability claims).
29. One recent example is *Quinteros v. Innogames*, where a product liability claim involving an online video game was dismissed because it was "software as a service" and thus not a product. *See Quinteros v. Innogames*, No. C19-1402RSM, 2022 U.S. Dist. LEXIS 55640, at *19 (W.D. Wash. Mar. 28, 2022).
30. *See Sgouros v. TransUnion Corp.*, 817 F.3d 1029, 1033-34 (7th Cir. 2016); *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229 (E.D. Pa. 2007); *Jallali v. Nat'l Bd. of Osteopathic Med. Exam'rs, Inc.*, 908 N.E.2d 1168 (Ind. Ct. App. 2009).
31. *Murray v. ILG Techs., LLC*, 378 F. Supp. 3d 1227 (S.D. Ga. 2019).
32. *Id.*
33. *See Winter v. G.P. Putnam's Sons*, 938 F.2d 1033, 1036 (9th Cir. 1991). The Reporters' Notes to Restatement (Third) of Torts §19 had cited earlier dicta in the same decision that "Computer software that fails to yield the result for which it was designed may be another" intangible treated as a product for the purposes of product liability. *Id.* at 1035.
34. *See, e.g., Sanders v. Acclaim Entertainment, Inc.*, 188 F. Supp.2d 1264, 1278-79 (D. Colo. 2002) (computer games are not

products for strict liability purposes); *Wilson v. Midway Games, Inc.*, 198 F. Supp.2d 167, 173 (D. Conn. 2002) (interactive "virtual reality technology" is not a "[product] for the purposes of strict products liability"); *James v. Meow Media, Inc.*, 90 F. Supp.2d 798, 810 (W.D. Ky. 2000) ("While computer source codes and programs are construed as 'tangible property' for tax purposes and as 'goods' for UCC purposes, these classifications do not indicate that intangible thoughts, ideas, and messages contained in computer video games, movies, or internet materials should be treated as products for purposes of strict liability."), *aff'd*, 300 F.3d 683, 700–01 (6th Cir. 2002) (software makers and website operators do not deal in "products").

35. James A. Henderson, Tort vs. Technology: Accommodating Disruptive Innovation, 47 Ariz. St. L.J. 1145, 1165 n.135 (Winter 2015) (citation and quotation marks omitted). *See also* Seldon J. Childers, Don't Stop the Music: No Strict Products Liability for Embedded Software, 19 U. Fla. J.L. & Pub. Pol'y 125, 151–52 (2008) ("The weight of authority, including case law, finds software is not defined as a 'product' for purposes of tort products liability.").
36. *South Central Bell Telephone Co. v. Barthelemy*, 643 So.2d 1240, 1244 (La. 1994) ("[W]e hold that computer software at issue in this case constitutes corporeal property under our civilian concept of that term.").
37. *Corley v. Stryker Corp.*, No. 6:13-CV-02571, 2014 WL 3375596, at *1, 4 (Mag. W.D. La. May 27, 2014), (applying strict liability under the LPLA to the software in a medical device "designed and manufactured from patient-specific 3D imaging data ... and the use of proprietary 3D imaging software[]" because it was "a necessary part" of the "product"), *adopted*, 2014 WL 3125990 (W.D. La. July 3, 2014); *Schafer v. State Farm Fire & Casualty Co.*, 507 F. Supp.2d 587, 600–01 (E.D. La. 2007) (based on *South Central Bell*, a computer "program may be a product for the purposes of the LPLA").
38. *Hardin v. PDX, Inc.,* 173 Cal. Rptr.3d 397, 407 (Cal. App. 2014) ("But [plaintiff's] theory is that [defendant's] software program, not the information it produces, is the defective product ... [To survive the state court equivalent of a motion to dismiss] causes of action need only be shown to have minimal merit.").
39. 795 F. Appx. 878, 880 (3d Cir. 2020).
40. *Id.*
41. *Id.*
42. No. 1:17-cv-219, 2021 U.S. Dist. LEXIS 178325 (W.D. Mich. Sept. 20, 2021).
43. *Id.* at *16–17 (internal citations omitted).
44. *Id.* at *17.
45. *Id.* at *18.
46. *Quinteros v. InnoGames*, No. C19-1402RSM, 2022 WL 898560 (W.D. Wash. Mar. 28, 2022); *Quinteros v. InnoGames,* No. C19-1402RSM, 2022 WL 953507, at *2 (W.D. Wash. Mar. 30, 2022) ("The Court will not consider new argument related to Plaintiff's product liability claim" and "[i]n any event, Plaintiff has failed to demonstrate manifest error").
47. *Id.* at *7.
48. *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1092–93 (9th Cir. 2021) (plaintiff asserted negligent design theory, but referred to a social media application as a "product"); *Maynard v. Snapchat, Inc.*, 870 S.E.2d 739, 746 (Ga. 2022) (plaintiffs "pursued only a negligence theory of design defect" and also repeatedly referred to the same application as a "product"). *Cf. Grossman v. Rockaway Township*, No. MRS-L-1173-18, 2019 WL 2649153, at *15 (N.J. Super. Law Div. June 10, 2019) (dismissing on other grounds but finding "no facts alleged that would support the theory that [the social media site's] actions qualify or constitute a product under the [New Jersey] Product Liability Act"). Decisions thus far in other litigation over social media have also not directly addressed the viability of product liability allegations. *See Doe v. Twitter, Inc.*, 555 F. Supp.3d 889, 929–30 (N.D. Cal. Aug. 19, 2021) (not reaching question of whether social media is a product; dismissing action for other reasons); *Williams v. Apple, Inc.*, No. 4:19-cv-00782, 2020 WL 1296843, at *2–4 (S.D. Tex. Mar. 24, 2020) (product liability claims involving cell phone software update dismissed for multiple other reasons; status of update as a "product" not addressed); *Herrick v. Grindr, L.L.C.*, 306 F. Supp.3d 579, 592 n.9 (S.D.N.Y. 2018) ("not address[ing the website's] argument that it is not a 'product' for purposes of products liability" given dismissal for other reasons), *aff'd*, 765 F. Appx. 586 (2d Cir. 2019).
49. No. 20-2270, 2022 WL 17269066 (4th Cir. Nov. 29, 2022).
50. *Lowe v. Cerner Health Servs., Inc.*, No. 1:19cv625, 2020 WL 6829770 (E.D. Va. Nov. 20, 2020).
51. *See, e.g., Powell v. Diehl Woodworking Mach., Inc.*, 198 F. Supp. 3d 628, 633 (E.D. Va. 2016) ("Virginia law only recognizes three products liability claims: negligent assembly or manufacture, negligent design, and failure to warn.").
52. *See In re Social Media Adolescent Addiction/Personal Injury Prods. Liab. Litig.*, __ F. Supp. 3d __, 2022 WL 5409144, at *2 (J.P.M.L. Oct. 6, 2022).
53. As of February 16, 2023, there were already 132 separate actions pending in the nascent proceeding. https://www.jpml.uscourts.gov/sites/jpml/files/Pending_MDL_Dockets_By_Actions_Pending-February-16-2023.pdf.
54. *See* Policy for Device Software Functions and Mobile Medical Applications (Sept. 28, 2022), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications. (stating the "Agency will continue to evaluate the potential impact these technologies might have on improving health care, reducing potential medical mistakes, and protecting patients").
55. One of these potential standards is the ONC Health IT Certification Program, which was recently mentioned in the FDA's recent non-binding Policy for Device Software Functions and Mobile Medical Applications. In the guidance released on September 28, 2022, they listed software functions that would not be subject to regulation which included software that complied with the ONC Program.
56. *See* National Cybersecurity Strategy (Mar. 1, 2023) https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
57. *See* 4 Highlights from Biden's Beefed Up Cybersecurity Strategy (Mar. 2, 2023) https://www.law360.com/articles/1581635/4-highlights-from-biden-s-beefed-up-cybersecurity-strategy.

Eric Alexander, a partner at Reed Smith LLP, practises in the area of product liability litigation for pharmaceutical and medical device companies. He has personally tried multiple prescription drug and device cases to verdict and assisted in trying many other prescription drug and medical device cases. Eric's practice has particularly focused on scientific, medical, and regulatory issues in product liability cases, along with novel theories of liability and defence. As such, he has closely followed developments in the digital health and medtech realm, and their intersection with product liability law. Eric is also a member of the blogging team for the award-winning Drug and Device Law blog.

Reed Smith LLP
1301 K Street, N.W., Suite 1000 - East Tower
Washington, D.C., 20005
USA

Tel: +1 202 414 9403
Email: ealexander@reedsmith.com
URL: www.reedsmith.com

Gerard Stegmaier, CIPP/US, a partner at Reed Smith LLP, focuses his practice on corporate governance, intellectual property, and technology – especially as they relate to privacy, information security, and consumer protection. An experienced and pragmatic litigator, Gerry focuses a significant part of his practice on prelitigation and advisory services relating to business strategy for these issues and is widely recognised for his work in data strategy, AI and machine learning. He often acts as strategic counsel and outside product counsel to leading innovators and disruptive technology companies advising and defending their interests, especially to avoid and navigate crises. He has helped health information technology, data management, advertising, and consumer technology companies bring some of the most popular and impactful products and services of the 21st century to market.

Reed Smith LLP
1301 K Street, N.W., Suite 1000 - East Tower
Washington, D.C., 20005
USA

Tel: +1 202 414 9228
Email: gstegmaier@reedsmith.com
URL: www.reedsmith.com

Jamie Lanphear, a counsel at Reed Smith LLP, focuses her practice on products liability litigation for medical device and pharmaceutical companies, with a particular focus on regulatory, scientific, and technical issues. She has extensive experience representing major manufacturers in cases involving defect, failure to warn, wrongful death, and consumer protection claims, and has served on multiple high-profile mass tort trial teams..

Reed Smith LLP
1301 K Street, N.W., Suite 1000 - East Tower
Washington, D.C., 20005
USA

Tel: +1 202 414 9217
Email: jlanphear@reedsmith.com
URL: www.reedsmith.com

Michael Rubayo, an associate at Reed Smith LLP, is a computer scientist whose legal practice includes a focus on privacy, tech and data issues.

Reed Smith LLP
599 Lexington Avenue, 22nd Floor
New York, NY, 10022
USA

Tel: +1 212 549 4707
Email: mrubayo@reedsmith.com
URL: www.reedsmith.com

NORTON ROSE FULBRIGHT

Global resources

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 3700 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

Our global offices

Our office locations

6800+
People worldwide

3500+
Legal staff worldwide

50+
Offices

Key industry strengths

- Financial institutions
- Energy, infrastructure and resources
- Transport
- Technology
- Life sciences and healthcare
- Consumer markets

Europe

- Amsterdam
- Athens
- Brussels
- Düsseldorf
- Frankfurt
- Hamburg
- Istanbul
- London
- Luxembourg
- Milan
- Munich
- Paris
- Piraeus
- Warsaw

United States

- Austin
- Chicago
- Dallas
- Denver
- Houston
- Los Angeles
- Minneapolis
- New York
- St Louis
- San Antonio
- San Francisco
- Washington DC

Canada

- Calgary
- Montréal
- Ottawa
- Québec
- Toronto
- Vancouver

Latin America

- Mexico City
- São Paulo

Asia Pacific

- Bangkok
- Beijing
- Brisbane
- Canberra
- Hong Kong
- Jakarta[1]
- Melbourne
- Perth
- Shanghai
- Singapore
- Sydney
- Tokyo

Africa

- Bujumbura[3]
- Cape Town
- Casablanca
- Durban
- Harare[3]
- Johannesburg
- Kampala[3]
- Nairobi[3]

Middle East

- Dubai
- Riyadh[2]

1 TNB & Partners in association with Norton Rose Fulbright Australia

2 Mohammed Al-Ghamdi Law Firm in association with Norton Rose Fulbright US LLP

3 Alliances

NORTON ROSE FULBRIGHT

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 3500 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

Law around the world

nortonrosefulbright.com

49528_US – 02/23