AN A.S. PRATT PUBLICATION
SEPTEMBER 2026
VOL. 12 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT



EDITOR'S NOTE: THE NEXT FRONTIER
Victoria Prussen Spears

SURVEILLANCE PRICING: THE NEXT FRONTIER OF PRIVACY LITIGATION
Matthew M. Morrissey, Josh Mahoney, Michael William Fires, Kate C. Goldberg and Tyler J. Hoguet

DRIFT PROTOCOL EXPLOIT: WHY "SOCIAL TRUST" IS THE NEWEST CYBERSECURITY GAP
Rajeev Raghavan, Anand Sithian and Sarah Rippy

GENETIC DATA AND ARTIFICIAL INTELLIGENCE TRAINING FOLLOWING ACQUISITIONS: EMERGING LITIGATION RISK AND A RAPIDLY EXPANDING STATE REGULATORY LANDSCAPE
Jason Johnson, Linda Malek and Sarah Rippy

NAVIGATING AI COMPLIANCE WITH HIPAA ESSENTIALS
Jeff Wurzburg, Susana Medeiros, Susan Linda Ross, Abel Chacko and Kathleen Rubinstein

THIRD CIRCUIT OFFERS CLARITY ON DATA PRIVACY AND REPLAY CODE: 3 PROACTIVE STEPS FOR BUSINESSES FOLLOWING DUAL RULINGS
Risa B. Boerner, Logan S. Booth and Catherine M. Contino

U.S. STATE PRIVACY ENFORCEMENT: KEY PRIORITIES AND PRACTICAL GUIDANCE FROM STATE REGULATORS
Jason Johnson and Linda Malek

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 7** **September 2026**

Editor's Note: The Next Frontier 221
Victoria Prussen Spears

Surveillance Pricing: The Next Frontier of Privacy Litigation 223
Matthew M. Morrissey, Josh Mahoney, Michael William Fires, Kate C. Goldberg and Tyler J. Hoguet

Drift Protocol Exploit: Why "Social Trust" Is the Newest Cybersecurity Gap 236
Rajeev Raghavan, Anand Sithian and Sarah Rippy

Genetic Data and Artificial Intelligence Training Following Acquisitions: Emerging Litigation Risk and a Rapidly Expanding State Regulatory Landscape 240
Jason Johnson, Linda Malek and Sarah Rippy

Navigating AI Compliance With HIPAA Essentials 243
Jeff Wurzburg, Susana Medeiros, Susan Linda Ross, Abel Chacko and Kathleen Rubinstein

Third Circuit Offers Clarity on Data Privacy and Replay Code: 3 Proactive Steps for Businesses Following Dual Rulings 248
Risa B. Boerner, Logan S. Booth and Catherine M. Contino

U.S. State Privacy Enforcement: Key Priorities and Practical Guidance From State Regulators 251
Jason Johnson and Linda Malek

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.
LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2026 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2026–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR
Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Norton Rose Fulbright US LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenisberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Sidley Austin LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2026 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Navigating AI Compliance With HIPAA Essentials

By Jeff Wurzburg, Susana Medeiros, Susan Linda Ross, Abel Chacko and Kathleen Rubinstein*

In this article, the authors discuss how healthcare providers can remain compliant with HIPAA rules.

Healthcare providers are increasingly deploying artificial intelligence (AI) tools for diagnostics, documentation and operational efficiency. In fact, over the last months, large AI platforms are now marketing AI-enabled tools directly to healthcare providers. Providers must navigate a rapidly evolving regulatory landscape, while keeping in mind existing and longstanding requirements intended to safeguard the privacy and security of patient data. The U.S. Department of Health and Human Services (HHS) has proposed updates to the HIPAA Privacy[1] and Security[2] rules, scheduled for July of 2027, but without nationwide AI standards, existing HIPAA obligations continue to govern AI use. At the same time, providers may be subject to state regulation of AI. For instance, Texas providers face added complexity from new state-specific AI requirements. The central question emerges: How can providers remain compliant as federal and state rules continue to evolve?

HIPAA ESSENTIALS

The HIPAA Privacy Rule[3] governs the use and disclosure of protected health information (PHI). The HIPAA Security Rule[4] imposes administrative, physical and technical safeguards for electronic PHI (ePHI). "Covered entities" include healthcare providers, health plans and healthcare clearinghouses. "Business associates" are persons or entities who create, receive, maintain or transmit PHI on behalf of covered entities.

Healthcare data privacy breaches often result from routine errors, such as misdirected electronic communications or unencrypted messages; external threats, including

* The authors, from Norton Rose Fulbright US LLP, may be contacted at jeff.wurzburg@nortonrosefulbright.com, susana.medeiros@nortonrosefulbright.com, susan.ross@nortonrosefulbright.com, abel.chacko@nortonrosefulbright.com and kathleen.rubinstein@nortonrosefulbright.com, respectively.

[1] https://www.federalregister.gov/documents/2021/01/21/2020-27157/proposed-modifications-to-the-hipaa-privacy-rule-to-support-and-remove-barriers-to-coordinated-care.

[2] https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information.

[3] 45 C.F.R. Part 164, Subpart E, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[4] 45 C.F.R. Part 164, Subpart C, https://www.hhs.gov/hipaa/for-professionals/security/index.html.

phishing, ransomware and hacking; and unauthorized access through vendor platforms. When a provider suspects such activity, it must investigate the source and mitigate any harm.

Providers face liability from the HHS Office for Civil Rights (OCR) and state attorneys general. Federal civil penalties are inflation-adjusted, with annual caps for repeated violations now exceeding US$2 million.[5] Criminal penalties for knowing violations can also include up to 10 years imprisonment.

Most states, including Texas, allow their attorneys general to enforce HIPAA violations through state consumer protection or health privacy statutes. State penalties can exceed US$250,000 per violation. Criminal violations can carry felony fines up to US$250,000 and more than 10 years of imprisonment, with even harsher penalties when identity theft or computer crime statutes apply.

Where HIPAA does not apply (for example, direct-to-consumer wellness apps), the Federal Trade Commission (FTC) oversees data security under the Health Breach Notification Rule,[6] which covers both data security breaches and unauthorized disclosures.

THE NATIONAL AND STATE AI LANDSCAPE

HHS has not issued a final update to the HIPAA Privacy and Security rules addressing AI, but the federal government is moving toward a unified framework and leveraging existing health programs to shape expectations. On December 11, 2025, the Trump administration issued the Executive Order "Ensuring a National Policy Framework for Artificial Intelligence."[7] This order directs the DOJ to challenge onerous state AI laws and tasks agencies with creating preemptive reporting standards to avoid a "patchwork" of 50 different state rules. Additionally, on December 23, 2025, HHS issued a Request for Information[8] on what HHS can do to accelerate the adoption and use of AI as part of clinical care.

HHS and the Centers for Medicare & Medicaid Services (CMS) have advanced AI through programs like the WISeR Model,[9] a 2026 Center for Medicare and Medicaid Innovation model that uses AI to automate prior authorizations under traditional Medicare for a limited set of services. This model is now operating in six states, including Texas.

---

[5] See 2026 Annual Civil Monetary Penalties Inflation Adjustment, available at https://www.govinfo.gov/content/pkg/FR-2026-01-28/pdf/2026-01688.pdf.

[6] 16 CFR Part 318, https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.

[7] https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

[8] https://www.govinfo.gov/content/pkg/FR-2025-12-23/pdf/2025-23641.pdf.

[9] https://www.cms.gov/priorities/innovation/innovation-models/wiser.

Despite federal efforts to harmonize AI, at least thirty-eight states have enacted AI-related legislation and over 400 AI-related bills are currently pending in state legislatures. Multi-state providers must track these varying obligations as there is no federal pre-emption for AI regulation.

TEXAS LEGISLATIVE CHANGES

Texas has moved to the forefront of AI regulation. SB 1188[10] and HB 149[11] require healthcare providers to disclose to patients the use of AI in a clear and conspicuous manner.

SB 1188 (effective September 1, 2025)

Expressly permits AI for diagnostic purposes if the practitioner:

a. Stays within the practitioner's licensed scope;

b. Discloses the use of AI; and

c. Reviews all AI-generated records in accordance with Texas Medical Board standards.

It also requires that electronic health records data be maintained within the U.S. by January 2026.

HB 149, The Texas Responsible AI Governance Act (TRAIGA) (effective January 1, 2026)

Requires healthcare providers to disclose the use of AI in relation to healthcare services or treatment no later than the date of treatment. Failure to disclose may be considered a deceptive trade practice under Texas Law.

WHERE HIPAA MEETS AI

Although HIPAA predates modern AI, its requirements are intentionally technology neutral. The HIPAA Security Rule still applies, meaning covered entities must conduct an accurate and thorough risk analysis to identify vulnerabilities to the confidentiality, integrity and availability of PHI before adopting AI tools. Sharing PHI with an AI vendor will almost always require a Business Associate Agreement (BAA), and HIPAA remains the baseline standard for any AI system that handles PHI. Covered entities and business associates must maintain appropriate administrative, physical and technical safeguards and continue to perform the risk assessments emphasized by HHS for all ePHI.

---

[10] https://capitol.texas.gov/tlodocs/89R/billtext/html/SB01188E.htm.

[11] https://capitol.texas.gov/tlodocs/89R/billtext/pdf/HB00149I.pdf.

In practice, this requirement means identifying AI use cases involving PHI, updating or executing BAAs with AI vendors, limiting access to approved tools and documenting risk analyses using recognized frameworks as federal and state regulations evolve. A "HIPAA first" governance approach, paired with close attention to emerging federal standards and state specific obligations, helps organizations stay aligned as the regulatory landscape shifts.

PRACTICAL RECOMMENDATIONS (H.I.P.A.A. FRAMEWORK)

(H)onest disclosure

- Clearly disclose AI use to patients, ensuring compliance with state-specific laws like TRAIGA in Texas.

(I)mplement safeguards

- Establish policies, procedures and workforce training for approved AI tools.
- Use robust data encryption and strict access controls.
- De-identify data wherever possible before AI processing to minimize risk.
- Consider retention settings associated with approved AI tools and whether this aligns with data minimization standards for maintaining PHI (see Section §164.502(b), describing the minimum necessary standard).
- Ensure a licensed professional reviews AI outputs before sharing with a patient.

(P)HI sharing

- Instruct users never to input PHI into public AI.
- Execute BAAs with all AI software vendors.
- Explicitly define permissible uses of data and prohibit the re-identification of de-identified datasets.

(A)udit AI use

- Conduct thorough risk assessments for every tool, using resources like the National Institute of Standards and Technology (NIST) AI Risk Management Framework.[12]

[12] https://www.nist.gov/itl/ai-risk-management-framework.

- Maintain a written inventory of all technology assets that interact with electronic PHI.

(A)sk

- The regulatory landscape is shifting rapidly. Asking experienced lawyers and professionals to monitor these developments closely can help companies stay compliant.

THE ROAD AHEAD…

A thoughtful, well structured approach to AI governance is no longer optional for healthcare organizations in Texas and across other jurisdictions. As federal agencies refine national standards and states chart their own paths, providers that ground their AI strategies in HIPAA fundamentals, transparent patient communication and disciplined vendor oversight will be best positioned to adapt. By investing early in governance, documentation and cross functional coordination, organizations can stay ahead of regulatory change and deploy AI to strengthen patient trust and support long term operational resilience.