New legal developments herald big changes for HIPAA compliance in 2025

By Erin Whaley, Esq., Brent Hoard, Esq., and Emma Trivax, Esq., Troutman Pepper Locke LLP

APRIL 7, 2025

2025 could be poised to be the biggest year for health care data yet. The increasingly ubiquitous use of AI and new technological advancements have organizations relying on and investing in data more than ever. However, these developments come with new legal risks and security threats for protected health information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA).

With responsible data use, patient data rights, data security, and privacy top of mind, the HIPAA compliance landscape is positioned for continued evolution and increased scrutiny.

Here's what to expect and how to prepare in the coming year.

The health care industry is gearing up for a data security revamp

With a 264% increase in ransomware attacks in 2024, the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) heavily enforced ransomware incidents last year, settling five ransomware investigations. The OCR also introduced its Risk Analysis Initiative at the end of 2024, focusing OCR enforcement on entities that fail to properly conduct the required periodic security risk analysis (SRA).

While there is no required format or method for an SRA under HIPAA, OCR is specifically cracking down on entities that only conduct cursory SRAs that do not thoroughly evaluate and address potential security risks or fail to conduct an SRA at all.

Security considerations are further compounded by HHS' proposed rulemaking in January to revamp HIPAA's Security Rule. The proposed changes aim to modernize the Security Rule, addressing technical aspects — such as patching, encryption, multifactor authentication, and penetration testing — and enhancing training and awareness regarding social engineering to mitigate common data breach risks.

While these rules reaffirm the OCR's data security efforts, the proposed rule's administrative and technical aspects would be costly and burdensome, particularly for smaller medical practices, self-funded health plans, and health care businesses.

Whether or not the proposed updates to the Security Rule are finalized or are materially modified from the current form, organizations must be proactive in keeping their security policies and procedures up to date. This includes implementing training to educate staff on new and emerging security threats and conducting regular, in-depth SRAs, as perfunctory SRAs are becoming an area of increasing enforcement risk.

Patient access remains a high priority

Patient right to access continues to be an area of significant focus for the OCR. From March to November 2024, the OCR settled five right to access cases, with another enforcement just announced on March 7, 2025.

With responsible data use, patient data rights, data security, and privacy top of mind, the HIPAA compliance landscape is positioned for continued evolution and increased scrutiny.

The OCR continues to stress the importance of providing timely record access to patients and their personal representatives. Considering that most of these enforcement actions were triggered by a single incident or patient request, it is evident that widespread patient access issues can be exposed by just one individual, potentially subjecting a covered entity to significant financial and legal risk.

This OCR enforcement focus also aligns with one of the core goals of HHS' Information Blocking Rule, which aims to improve the flow of essential electronic health information between necessary parties. Most recently, HHS released two final rules aimed at improving interoperability and addressing information blocking issues. These rules, effective December 2024, provide clarity on when health care providers can share electronic health information, introduce new privacy and security requirements, and expand upon some information blocking

exceptions to allow providers to comply with patient requests.

Covered entities and business associates should take recent information blocking rule changes as an opportunity to review patient access policies and procedures from both a HIPAA and information blocking perspective and confirm compliance.

Responsible data use considerations extend to protected health information

The OCR has placed a heavy focus on the potential for unauthorized use or disclosure of PHI through the use of emerging technologies. Thus, enforcement under HIPAA is also likely to evolve in response to the increased emphasis on responsible data use — which has become an essential component of AI's integration into business operations across industries.

Whether or not the proposed updates to the Security Rule are finalized or are materially modified from the current form, organizations must be proactive in keeping their security policies and procedures up to date.

HHS has not yet released any AI-specific HIPAA requirements, but it has issued other guidance that suggests AI technologies could be scrutinized to the extent they result in an unauthorized use or disclosure.

Additionally, the OCR previously issued a bulletin warning of the legal perils of online-tracking technologies that collect information about individuals using webpages and mobile applications of HIPAA-regulated entities. In *American Hospital Association v. Becerra*, a federal court in the Northern District of Texas struck down a portion of the guidance related to tracking on unauthenticated web pages on the grounds that it exceeded HHS' authority under HIPAA. The guidance, however, still applies and remains in effect for tracking activities on authenticated web pages (i.e., pages that require user log-in). HHS announced that it is "evaluating its next steps" in light of the court's order.

While the court limited the scope of the tracking technology guidance, regulated entities should still carefully evaluate how PHI is being used and accessed by third-party AI tools and tracking technologies. In addition to incorporating policies that address responsible data use, entities must be aware of technologies that may inconspicuously gain unauthorized access and use of PHI.

Entities should also consider how AI can increase the risk of inadvertent disclosure due to its ability to process and potentially infer PHI from various non-sensitive data points (e.g., reidentification of deidentified data).

Reproductive health privacy remains contested

Effective Dec. 23, 2024, HHS issued a final rule to protect the privacy of reproductive health care information. Under the final rule, the use or disclosure of an individual's PHI is prohibited for the purpose of conducting criminal, civil, or administrative investigations or for imposing liability on anyone for the act of seeking, obtaining, providing, or facilitating reproductive health care that was lawful at the time it was provided.

The rule also mandates that any requests for reproductive health care PHI for specific purposes must include an attestation confirming that the use or disclosure of PHI is not for a prohibited purpose and covered entities must update their notice of privacy practices (NPPs) to reflect the new requirements.

Last fall, in *State of Texas v. U.S. Department of Health and Human Services*, the State of Texas challenged the newly finalized 2024 final rule on reproductive health care information and a privacy rule issued in 2000, which prohibits the disclosure of reproductive health PHI unless the request meets a three-part test. Texas argues that both rules inhibit law enforcement's ability to enforce its laws on abortion. This case is currently pending and unresolved in the federal Northern District of Texas.

With the final rule now in effect, providers must comply despite the ongoing legal challenges pending against it. Covered entities should ensure they make appropriate updates to their NPPs by the required Feb. 16, 2026, deadline and update policies and procedures to reflect the rule as it currently stands, while also remaining on top of new legal developments. Not only could the rules be potentially narrowed in scope or struck down by the Texas federal court, but there is also the potential for additional rule changes under the new administration.

Conclusion

As 2025 unfolds, the evolving health care landscape will continue to drive legal shifts in the areas of data security and patient access and privacy. Covered entities and business associates can stay ahead of the curve by taking proactive compliance and risk-mitigation measures, including rigorous SRAs, evaluation of technical controls, staff training, and review of policies and procedures for effectiveness and consistency with ever-changing legal requirements.

About the authors



Erin Whaley (L) is a partner at **Troutman Pepper Locke LLP** where she represents health care providers and payers on the full spectrum of legal issues. Her regulatory experience includes advising clients on compliance with the plethora of federal laws that govern the health care industry, including Stark, the Anti-Kickback Statute (AKS), the False Claims Act, and HIPAA, as well as state laws including state licensure, corporate practice of medicine, and certificates of need. She also assists clients with investigations and resolving compliance concerns. She is based in Richmond, Virginia, and can be reached at erin.whaley@troutman.com. **Brent Hoard** (C) is a partner at the firm. He has helped an array of clients — from Fortune 50 companies to early-stage innovators, across a spectrum of industries — to protect and maximize the value of their data through assessment, development, implementation, and enhancement of their privacy, information security, risk management, and HIPAA programs. These industries include technology, social media, health care, pharma and life sciences, digital health, internet, retail, insurance/reinsurance, fintech, and travel/hospitality. He is located in West Palm Beach, Fla., and can be reached at brent.hoard@troutman.com. **Emma Trivax** (R) is an associate at the firm. She represents a wide range of health care providers, including pharmacies, physician practices, management service organizations, dental service organizations, hospitals, clinical laboratories, skilled nursing facilities, ambulatory surgical centers, DMEPOS suppliers, and behavioral health providers. She is located in Detroit, and can be reached at emma.trivax@troutman.com. Timothy Shyu, an associate at the firm, contributed to this article.

This article was first published on Reuters Legal News and Westlaw Today on April 7, 2025.