Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Health Cos. Can Navigate Data Security Regulation Limbo

By **William Li** (March 20, 2025, 5:35 PM EDT)


William Li

Healthcare organizations face a critical dilemma: As data breaches reach unprecedented levels, the regulatory framework designed to protect patient information hangs in limbo.

With the Trump administration's freeze on proposed Health Insurance Portability and Accountability Act security rule updates, the industry must navigate rising cybersecurity threats without clear federal guidance.

In 2024 alone, HIPAA-covered entities reported data breaches affecting more than 170 million individuals — over half the U.S. population. According to IBM and the Ponemon Institute, the average breach cost the healthcare industry $9.77 million in 2024, maintaining the industry's position as the costliest sector for data breaches since 2010.[1] However, this financial analysis does not account for the human cost to these violations.

Under HIPAA, the definition of "health information" includes any information, including genetic information, about an individual's mental and physical health status, diagnosis, treatment, and provision of payment. This definition of healthcare information is broad, but nevertheless focuses on data that is both medical and personal.[2]

Indeed, according to a report released by Verizon last year, "Personal Data has eclipsed Medical data as the preferred target for threat actors."[3] It's a basic expectation for any individual that their healthcare information be kept secure, and naturally quite disturbing and frustrating that the healthcare industry has struggled to do so.

Although HIPAA's security and privacy rules are important, the legal landscape is complex and ever evolving. To begin with, it's important to understand HIPAA enforcement actions solely come through the U.S. Department of Health and Human Services; there is no private right of action for individuals to bring a HIPAA data breach lawsuit.

However, HIPAA is not the only basis of legal protections for an individual's health data. In 2024, the federal regulations protecting the confidentiality of substance use disorder patient records were amended to align with HIPAA.[4]

Additionally, there are protections for health data under the Federal Trade Commission Act that apply to certain businesses that would not otherwise be covered by HIPAA.[5] While HIPAA does not grant a private right of action, many state-level privacy laws do. Additionally, there are common law legal

theories based on negligence and breach of contract.

The U.S. Supreme Court's 2016 holding in Spokeo v. Robins laid out a general requirement with data breach litigation. To have standing, plaintiffs must show a concrete injury that has actually happened to that particular individual or a concrete injury that is imminent.[6] There are a variety of interpretations among the federal circuits and highest state-level courts about the concreteness of the injury or what imminent.

However, the HIPAA definition of breach is a useful and powerful conceptual grounding:

> the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information[7]

In R. K. v. St. Mary's Medical Center Inc. in 2012, the Western Virginia Supreme Court of Appeals observed that "several courts have found that a HIPAA violation may be used either as the basis for a claim of negligence per se, or that HIPAA may be used to supply the standard of care for other tort claims."[8]

Highlighting the standard of care frames a data breach as a failure of duty and reflects a policy viewpoint that healthcare organizations can and should be doing more to strengthen the security of patient data.

Modernizing the HIPAA Security Rule

With healthcare data breaches on the rise,[9] it's easy to see why the HIPAA security rule has once again entered the national conversation. Although it has been cautiously adjusted over the years, it is overdue for a more comprehensive update.

In December 2024, HHS posted a proposed rule aimed at bolstering HIPAA's cybersecurity requirements.[10] A public comment period opened, which was supposed to last until early March.

Although there was not a single event that prompted the proposed rule, so much as an overall view that the work of safeguarding patient data by healthcare providers, payors, and their business associates ought to operate at a higher level of maturity and efficacy.

Shortly after taking office, President Donald Trump issued an executive order freezing all proposed rules for 60 days,[11] including the proposed changes to HIPAA's security rule. The idea was that his administration could review all the proposed rules and decide whether to continue them, make adjustments or discontinue them altogether.

The Impact of the New Administration's Freeze

It is unclear how Trump will move forward with the proposed HIPAA security rule changes. During the previous Trump administration, there was bipartisan support for encouraging healthcare organizations to implement practical improvements.

Consequently, on Jan 5, 2020, Trump signed H.R. 7898, which amended the Health Information Technology for Economic and Clinical Health Act.

Under that amendment, HHS' Office of Civil Rights was required, when investigating a HIPAA breach, to take into account a healthcare organization's use of "best practices, methodologies, procedures, and processes developed under [the NIST Act], the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs" as a "safe harbor."[12]

The legislation's goal was to provide an incentive to the industry to mature the design of their systems and processes.

Fast-forward five years, and it seems plausible that Trump might preserve some aspects of the proposed HIPAA security rule amendments, especially if the final rule is presented as a continuation of reforms from the previous Trump administration. However, there is still a lot of uncertainty around what decisions will be made and whether there will be less regulation related to reporting requirements and breach investigations.

Less Regulation Could Prove Challenging

For incident reporting to be effective, regulations must strike a balance between prescriptive requirements that are often impractical to carry out and vague requirements that yield more ambiguity when regulators review an incident.

There's also tension between notifying people promptly and notifying them so frequently that they stop viewing a breach as a serious issue. There are times when critical near-miss situations or attempted attacks could be a bellwether for a more sophisticated attack wherein it may be potentially important to coordinate with law enforcement without signaling to the threat actor that they have been detected.

Getting the balance right is tricky, and it requires a deep understanding of all the nuances. That's why the public comment period is so important.

The Trump administration appears to be taking a different approach to regulating federally mandated activities and enforcing those regulations. Some of the normative aspects of federal agencies are changing, including the longstanding leadership at the Office of Inspector General and HHS.

There is an intentional push to overturn traditional regulatory norms. The president has committed to governing differently, and so far, that commitment has been playing out.

However, less regulation may not be the best strategy for ensuring healthcare data security. Healthcare organizations have a mission to improve people's health, and public trust is an essential part of that. Being able to point to consistent compliance with best practice security measures is one way healthcare organizations maintain the public's trust.

Also, being able to predict how a regulator will react to a breach is helpful for organizations as they respond to unforeseen events. Less regulation might lead to more private litigation and other unintended outcomes.

Critical Steps Healthcare Leaders Can Take Today

Preserving data security is challenging at any time, but it gets even harder when the rules are changing in unknown and unpredictable ways. The good news is that there are things organizations can do now despite the ambiguity.

Implement recognized security best practices if you haven't already.

The first Trump administration was in favor of healthcare organizations implementing recognized security best practices. If providers and payers do not currently have such practices in place, they should prioritize implementation now.

The National Institute of Standards and Technology's cybersecurity framework[13] is an especially useful approach to information security. It consists of five core functions — identify, protect, detect, respond and recover — that provide a flexible, risk-based framework that organizations of all sizes can use.

NIST is an outcomes-based model that is less prescriptive than other cybersecurity models, and it allows substantial flexibility in how an organization implements security protocols and responses. By using this model, healthcare organizations can improve their security in ways that align with their unique needs and situations.

Understand how artificial intelligence is changing the game.

AI is advancing at quite a clip. Although the Biden administration's 2023 directive encouraged caution because there were so many unknowns,[14] the first Trump administration was more concerned about the U.S. falling behind as the leader in AI research, and under the current Trump administration, this has reemerged as the policy priority.[15]

To date, HIPAA has primarily focused on traditional cybersecurity threats, and many best practices have remained relatively constant because, even though technology has evolved, the best practices are still based on traditional computing models.

However, there are significant differences between machine learning-based AI architectures and traditional deterministic rule-based algorithms.

Consequently, there are qualitatively different risks. Understanding where traditional cybersecurity risks and AI risks intersect and diverge will be crucial to creating data security programs that can easily flex and evolve over time.

In addition, as Trump pushes for the U.S. to be a leader in advancing AI, the chances of unanticipated consequences increase. It's hard to predict what the impact of less regulation will be in this area, so having a strong understanding of AI and its potential risks and benefits will be important.

Shift from being compliant to doing what's right.

As the nuances of the security rule evolve, healthcare organizations would be wise to focus less on what it means to be compliant and more on designing and executing programs that align with their mission and values.

Consider your true north, your operational strengths and weaknesses, your personnel, and your current resources. Ask yourself, "What is the best way to approach cybersecurity for us?"

Start with the basics, do what's feasible, weave in good habits and build success upon success. This may require a mindset shift from the C-suite. Your executive team must have a vision and passion for

continuous improvement in this area and a willingness to be patient and persevere.

Focus internal and external resources.

We may not know what's going to change, but you can be prepared to respond to changes as they emerge and commit to being focused. Organizations can adapt faster if they pull together a core strategic group to anticipate issues, work through potential impacts, respond quickly, and scale up as needed.

This team should include representatives from every area involved with and affected by cybersecurity regulations and challenges.

For example, members of the C-suite can ensure alignment with your organization's mission and vision; legal experts can weigh in on potential liability issues; information technology professionals can think through risks and what fixes are possible; and clinical leaders can surface the practical implications for healthcare delivery.

Success relies on clear communication and a shared commitment to collaboration. It's essential that everyone involved acknowledges and respects each other's subject matter expertise as this is crucial to developing an effective, cohesive strategy.

The Great Wave

In describing the need for a focused team, I am reminded of Hokusai's famous woodblock print from "Thirty-six Views of Mount Fuiji," "The Great Wave off Kanagawa."

The rough ocean waters dominate the scene as an incredibly powerful and dangerous force, and they are. The three small vessels and their crew appear modest by comparison. Look closer though, and all oars are pulling in the same direction. The only way to stay afloat is to go straight through. Indeed, all three vessels are making their way. None have capsized. Finally, there at the extreme edge, the prow of the lead craft is breaking through the cresting wave and will soon be upon calmer waters.

Healthcare providers and payers should prepare for what is likely to be a period of upheaval and uncertainty until things settle down on the regulatory front. Even if Trump lifts the freeze and proceeds with the comment period without changes, it will be 2026 before a final security rule is published. And because of the shake-up in HHS and Office of Inspector General leadership, how the rule is administered is going to be different.

Bottom line? Things are going to be ambiguous for a while. Having a best-practice mindset and a cross-functional strategic team that can think through possible ramifications and next steps will help you navigate the uncertainty and keep your organization's best interests top of mind.

William Li is an attorney at Axiom Law.

[1] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2024." The report notes that healthcare has maintained the highest average breach cost position for 14 consecutive years.

[2] 45 CFR § 160.103, which defines "health information" under HIPAA regulations.

[3] Verizon Business, "2024 Data Breach Investigations Report (DBIR)," p. 27.

[4] 42 CFR Part 2 was revised in 2024 to align with HIPAA's Privacy Rule while maintaining enhanced protections for substance use disorder records.

[5] 16 CFR Part 318 (Health Breach Notification Rule).

[6] Spokeo, Inc. v. Robins, 578 U.S. 330, 136 S. Ct. 1540 (2016). The Court held that Article III standing requires a concrete injury-in-fact that is "actual or imminent, not conjectural or hypothetical."

[7] 45 CFR § 164.402, which provides the HIPAA definition of "breach."

[8] R. K. v. St. Mary's Med. Ctr., Inc., 229 W. Va. 712, 720, 735 S.E.2d 715, 723 (2012).

[9] Adler, Steve, HIPAA Journal, "Healthcare Data Breach Statistics," January 20, 2025. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[10] Department of Health and Human Services, "Proposed Rule to Strengthen HIPAA Security Requirements," published in the Federal Register, December 2024.

[11] White House, "Executive Order on Regulatory Freeze Pending Review," January 20, 2025.

[12] H.R. 7898 (116th Congress), signed into law on January 5, 2021, which amended the HITECH Act to require HHS to consider certain recognized security practices when imposing penalties for HIPAA violations.

[13] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 16, 2018. The framework provides a flexible approach to addressing and managing cybersecurity risk across sectors including healthcare.

[14] EO 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," 88 FR 75191 (Oct 30, 2023).

[15] Compare EO 13859 "Maintaining American Leadership in Artificial Intelligence", 84 FR 3967 (Feb 11, 2019) with EO 14179 "Removing Barriers to American Leadership in Artificial Intelligence, 90 FR 8741 (Jan 31, 2025) (rescinding Biden's EO 14110).