akerman

Blog Post

New Year, New HIPAA Security Rule Requirements? OCR Proposes Sweeping Changes for HIPAA Security Rule To Bolster Cybersecurity

January 9, 2025

By Elizabeth F. Hodge, Ameer Al-Khudari, and Jordan T. Cohen

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently proposed a sweeping rewrite of the HIPAA Security Rule that, if finalized, will require that many Covered Entities and their Business Associates (Regulated Entities) invest significant resources to comply with new, less flexible requirements designed to strengthen the cybersecurity posture of the American healthcare system. We discuss below several aspects of OCR's comprehensive overhaul of the Security Rule published in its Notice of Proposed Rulemaking (NPRM) on January 6, 2025, the first proposed revisions to the Security Rule since 2013. The 60-day notice and comment period closes on March 7, 2025.

In a Press Release announcing the proposed updates, OCR Director Melanie Fontes Rainer stated that the NPRM is in response to the "rampant escalation in ransomware" impacting the health care industry and "significant increases in the number of large breaches reported to OCR annually." She went on to say:

> "This proposed rule . . . addresses current future cybersecurity threats. It would require updates to existing cybersecurity

Related People

Ameer Al-Khudari
Jordan T. Cohen
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Healthcare

Related Offices

Chicago
New York
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Read blog posts

> safeguards to reflect advances in technology and cybersecurity, and help ensure that doctors, health plans, and others providing health care meet their obligations to protect the security of individuals' protected health information across the nation."

In addition to protecting electronic protected health information (ePHI), OCR emphasized cyberthreats' impact on patient well-being as justification for the proposed Security Rule revisions. As OCR Deputy Secretary Andrea Palm explained, "The increasing frequency and sophistication of cyberattacks in the health care sector pose a direct and significant threat to patient safety," including disrupted patient care, diverted patients, postponed procedures, and diminished patient trust.

Big Changes Set a High Standard

The Security Rule sets a national standard for the protection of ePHI and requires Regulated Entities to use administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI. When OCR changes that national standard, Regulated Entities must adjust their safeguards accordingly.

In a world where physician and dental practices, other small-scale providers, employer-sponsored health plans, and business associates already struggle to meet the Security Rule's existing requirements, OCR's proposed changes, if enacted, would introduce a more demanding and less flexible compliance standard that Regulated Entities must meet.

For example, the 2003 Security Rule distinguishes between "required" and "addressable" implementation specifications to provide Regulated Entities with some degree of flexibility in determining the reasonable and appropriate safeguards in their specific circumstances. In the

NPRM, OCR expressed concern based upon its investigations and audits that some Regulated Entities interpreted "addressable" implementation specifications to be "optional," but OCR never intended such a reading.

By removing the "addressable" distinction, OCR seeks to provide "greater specificity in the Security Rule" that would benefit Regulated Entities. As a result, encryption of ePHI at rest and in transit and multi-factor authentication (MFA), which are currently "addressable" implementation specifications, would be "required" under the proposed rule. With regard to the former, OCR reasoned that "encryption is built into most software today, and where it is not, there are affordable and easily implemented solutions that can encrypt sensitive information."

In practice, the demise of the "addressable" implementation specifications means OCR is establishing clear expectations for compliance, with limited exceptions that require the Regulated Entity to document in real-time that an exception is applicable and that all other applicable conditions are met.

HHS' Fact Sheet summarizes the other substantive changes in the NPRM, including the following requirements:

- Written documentation of all Security Rule policies, procedures, plans, and analyses.
- Development and revision of a technology asset inventory and a network map that illustrates the movement of ePHI throughout the Regulated Entity's electronic information system(s) on an ongoing basis, but at least once every 12 months and in response to a change in the Regulated Entity's environment or operations that may affect ePHI.
- Notification of certain Regulated Entities within 24 hours when a workforce member's access to

ePHI or certain electronic information systems is changed or terminated.

- Strengthen requirements related to contingency planning and incident response such as requiring Regulated Entities to establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours of initial loss.
- Internal compliance audits at least once every 12 months to ensure Regulated Entities' compliance with the Security Rule requirements.
- Business associates must verify at least once every 12 months for covered entities (and business associate contractors must verify at least once every 12 months for business associates) that they have deployed technical safeguards the Security Rule requires to protect ePHI through a written analysis of the business associate's relevant electronic information systems by a subject matter expert and a written certification that the analysis has been performed and is accurate.
- Vulnerability scanning at least every 6 months and penetration testing at least once every 12 months.
- Network segmentation.
- Business associates must notify covered entities (and subcontractors must notify business associates) upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.
- Group health plans must include in their plan documents requirements for their group health plan sponsors to: comply with the administrative, physical, and technical safeguards of the Security Rule; ensure that any agent to whom they provide ePHI agrees to implement the safeguards of the Security Rule; and notify their group health plans upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.

More on the Risk Analysis Requirement

As HIPAA watchers are aware, risk analyses are a constant pain point in OCR investigations. OCR expressed its dissatisfaction in the NPRM regarding the quality of risk analyses that it has encountered during its enforcement activities. The proposed changes to the risk analysis standard includes eight implementation specifications, including one requiring a written assessment, in which the Regulated Entity must, at a minimum:

- Review its technology asset inventory and the network map mentioned above to identify where ePHI may be created, received, maintained, or transmitted within its information systems.
- Identify all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits and potential vulnerabilities to the Regulated Entity's relevant electronic information systems.
- Create an assessment and documentation of the security measures the Regulated Entity uses to ensure that the measures protect the confidentiality, integrity, and availability of the ePHI it creates, receives, maintains or transmits.
- Make a reasonable determination of the likelihood that each identified threat would exploit the identified vulnerabilities and the potential impact of each identified threat should it successfully exploit the identified vulnerabilities.
- Create an assessment of the risk levels for each identified threat and vulnerability.
- Create an assessment of risks to ePHI posed by entering into or continuing a business associate agreement with any prospective or current business associate based on the written verification obtained from the prospective or current business associate.

Regulated Entities should consider reviewing OCR's preamble discussion about what it deems sufficient

for purposes of conducting a risk analysis.

Proposed Compliance Date

If the proposed rule is finalized, Regulated Entities must comply beginning 180 days after the effective date – with limited extended timelines to provide Regulated Entities additional time, up to one year, to update existing business associate agreements that would not be renewed or modified between the effective date and compliance date of the proposed rule. For its part, OCR explains that it does "not believe that the proposed rule would pose unique implementation challenges that would justify an extended compliance period" beyond the standard 180 days for compliance after the effective date of a final rule.

The Cost of Compliance

HHS estimates that the first-year costs attributable to its proposed rule would "total approximately $9 billion" for Regulated Entities and health plan sponsors "engaging in the regulatory actions described." HHS further estimates that years two through five will have annual costs of $6 billion, attributable to "recurring compliance activities."

However, as HHS notes in the NPRM, many of the benefits of its proposed changes are non-quantifiable at this time, though since 2018 the number of breaches of unsecured PHI grew 100%, and the number of individuals affected by breaches increased by 950%, likely attributable to a "rampant escalation of cyberattacks" including a 260% increase in hacking attacks and a 264% increase in the utilization of ransomware.

HHS' estimates likely understate the true cost to comply with the proposed changes. It is uncertain how small providers, financially strapped rural providers, and employer sponsors of health plans, among others, will obtain the financial and human resources needed to implement the proposed requirements.

The Future

The NPRM comes in the waning days of the Biden-Harris administration. By the time the 60-day deadline for comments on the proposed rule ends on March 7, 2025, the transition to the Trump-Vance administration will be complete. Considering that the initial Security Rule, first proposed in 1998 and not finalized until 2003, faced opposition related in no small part to the potential cost of compliance, it remains to be seen whether OCR's sweeping changes in the NPRM will be finalized as drafted following the comment period.

In light of the significant and potentially costly changes in this proposal, Regulated Entities should consider submitting comments to HHS detailing the impact the NPRM would have on their organization. Meanwhile, the current Security Rule remains in effect, and Regulated Entities should consider reviewing their current compliance posture in light of the proposed updates.

This is an evolving area, and Akerman's health care lawyers will be monitoring the rulemaking process and its developments.
