Now & Next
Healthcare Alert

December 31, 2024

OCR announces proposed updates to HIPAA Security Rule

By Laurie Cohen, Jéna Grady, Meredith LaMaster, Freddy Lopez, and Valerie Breslin Montague

The Notice of Proposed Rulemaking (NPRM) is intended to improve the industry's cybersecurity posture but may be administratively challenging and costly for some HIPAA-regulated entities to implement.

What's the impact?

- While the NPRM may be modified by the incoming administration, and a final rule may not be on the immediate horizon, HIPAA-regulated entities should consider whether to weigh in on the changes.
- The 60-day public comment period commences upon the publication of the NPRM in the *Federal Register*.

On December 27, 2024, the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced proposed modifications to the HIPAA Security Rule, the first updates since 2013.[i]

Proposed HIPAA Security Rule changes

The NPRM, scheduled to be published in the *Federal Register* on January 6, 2025, proposes to clarify existing Security Rule requirements and add new obligations, including the following:

- Development and maintenance of a written technology asset inventory and a network map of a regulated entity's electronic information systems and all technology assets.
- Requirement for covered entities to obtain, on an annual basis, written verifications from business associates that the business associates have deployed HIPAA technical safeguards. Business associates would also be expected to obtain such verification from their subcontractors. Requirement to update new and existing business associate agreements to include a provision requiring a business associate to report to the covered entity activation of the business associate's contingency plan, without unreasonable delay but no later than 24 hours after activation. Adoption of new or revised security policies addressing workforce member access to electronic protected health information (ePHI) and termination of such access, as well as enhanced security awareness training for all workforce members.
- Defining "deploy"—clarifying that it refers to the process of installing, configuring, and ensuring security measures are in place and operational throughout the entire regulated entity environment—and defining "implement"—clarifying that safeguards must be established and in effect throughout the regulated entity's enterprise and not just a subset of information systems or ePHI. By doing so, this proposal clarifies that a regulated entity is not expected to merely establish policies and procedures but must continue to verify the ongoing operation of technical controls used in relevant electronic information systems.
- Elevating risk management from a required implementation specification under the technical safeguards to a standard under a new proposed section, which, among other things, would require a regulated entity to establish and implement a written risk management plan for reducing the risks identified through its risk analysis activities. (Note that HHS uses the phrase "reasonable and appropriate" and, under the proposed risk management standard and its accompanying implementation specifications, interprets it to require that a regulated entity will take into account not only its specific circumstances but also the criticality of the risks identified).
- Elevating encryption from an addressable implementation specification to a required standard, acknowledging that with the prevalence of more encryption solutions, their increased affordability, and their vital importance to protecting information, its elevation to a required standard will increase its visibility and prominence. The NPRM requires regulated entities to encrypt all ePHI at rest and in transit, with limited exceptions.

How can HIPAA-regulated entities prepare?

With a new administration taking over in a matter of weeks, it is likely that the NPRM will face challenges or that a final rule may be postponed or never promulgated. HHS has estimated that the first-year costs incurred by regulated entities to comply with the new requirements would total approximately $9 billion and, for years two through five thereafter, the annual cost for recurring compliance activities would be approximately $6 billion. Of note, HHS also asserts that "the enhanced security posture of regulated entities would likely reduce the number of breaches of ePHI and mitigate the effects of breaches" such that "if the proposed changes in the NPRM reduce the number of individuals affected by breaches by 7 to 16 percent, the revised Security Rule would pay for itself." Even if increased security measures lead to lower breach expenses, it would be difficult for a HIPAA-regulated entity to balance such savings with the likely increase in compliance costs if the OCR proposals are finalized.

As discussed above, these costs will include, among other actions, performing a Security Rule compliance audit, updating business associate agreements, and reporting the activation of contingency plans. Most of the proposed modifications will involve significant time and financial investments in an entity's information technology infrastructure.

Despite Medicaid making federal matching funds available for certain state administrative costs, these funds are limited specifically to operational costs, not HIPAA compliance activities. Additional pushback is expected from covered entities already facing budgetary shortfalls, staffing shortages, and other barriers impacting clinical care and operations. With the new administration's focus on cutting healthcare costs, the content and timing of a final rule related to these proposed measures is uncertain.

Public comment period open

As it mentions in its Fact Sheet, OCR encourages all stakeholders to submit comments on the NPRM through regulations.gov. Comments are due sixty (60) days from the NPRM's publication in the *Federal Register*.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Laurie T. Cohen
518.427.2708
lauriecohen@nixonpeabody.com

Jéna M. Grady
212.940.3114
jgrady@nixonpeabody.com

Meredith D. LaMaster
312.977.9257
mlamaster@nixonpeabody.com

Freddy R. Lopez
213.629.6038
flopez@nixonpeabody.com

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

[i] In the White House Office of Management and Budget Fall 2024 Unified Agenda of Regulatory Plan released on December 13, 2023, OCR noted that it evaluated whether the below new obligations could be issued instead as guidance rather than new requirements. However, OCR determined that such guidance could not be sufficient enough to properly address the cybersecurity threats and vulnerabilities currently facing healthcare organizations.