Proposed Rule for Amendments to HIPAA Security Rule

Insights 01.09.25

PROFESSIONAL

SUNAYA PADMANABHAN
Associate
San Francisco

CLAIRE ERNST
Director, Government Relations & Public Policy
Washington, D.C.

ALICIA MACKLIN
Partner
Los Angeles

STEPHEN K. PHILLIPS
Partner
San Francisco

The Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") issued a notice of proposed rulemaking ("NPRM"), on December 27, 2024, to amend the Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Security Rule implements standards to protect an individual's electronic protected health information ("ePHI"). The proposed changes aim to modernize the Security Rule to address the evolving cybersecurity landscape and enhance the protection of ePHI. This Alert outlines the key provisions of the NPRM and the guiding reasoning behind HHS' proposed changes.

Summary of Key Proposed Amendments

In the NPRM, HHS discusses two main concerns: (1) the ambiguity and misinterpretation of the existing Security Rule and (2) the inadequate security practices in an evolving healthcare environment. To address these issues, HHS proposes modifications and new requirements to the Security Rule; this Alert summarizes certain key proposed amendments below. During the proposed rulemaking process, the current version of the Security Rule remains in full force and effect.

Implementation.

- **Addressable v. Required Implementation Specification**. To address HHS's concern that regulated entities (*e.*, covered entities and business associates) often treat "addressable" implementation specifications as "optional," the proposed amendments would eliminate the distinction between "addressable" and "required" implementation specifications. Regulated entities would still retain flexibility in how they comply with an implementation specification; however, all implementation specifications would be required.
- **Resiliency**. The NPRM attempts to de-emphasize cost as a factor regulated entities may consider when selecting implementation specifications by proposing a new factor: the effectiveness of an implementation specification in supporting the regulated entity's resilience – *e.*, the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems.

Business Associates and Subcontractors.

- **Notification**. HHS proposes requiring that business associates report activation of their contingency plan (for any event that adversely affects relevant electronic information systems) within 24 hours of activation. The

reporting is intended to address business associates failing to promptly notify covered entities of security incidents.

- **Verification and Certification**. HHS recognizes that although business associates must provide written assurance that they will appropriately safeguard ePHI, the Security Rule does not require regulated entities to verify the deployment of such protections. To facilitate business associate compliance, HHS proposes that the regulated entity obtain written verification of the business associate's deployment of technical safeguards, every 12 months. The verification must be performed by an individual with the requisite knowledge to evaluate compliance and include a written analysis of the business associate's relevant electronic information systems. The verification must be accompanied by a written certification by a person who has the authority to act on behalf of the business associate that the analysis has been performed and is accurate. Business associates would have to receive such verification and certification from any subcontractor business associates. A regulated entity would need to 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.

Security Management.

- The NPRM highlights HHS' concern that regulated entities do not have a complete understanding of all of their technology assets. Without such knowledge, HHS argues that regulated entities cannot currently account for all the risks to ePHI. The proposed amendments would require a regulated entity to maintain and update (i) a technology asset inventory and (ii) a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI. These records would include ePHI created, received, maintained, or transmitted to a business associate or the technology assets used by the business associates to create, receive, maintain or transmit ePHI. Using the technology asset inventory and network map, regulated entities would be required to perform an in-depth risk assessment of the potential and likely threats to ePHI every year.

Encryption and Multi-Factor Authentication.

- To modernize the Security Rule to current technological standards, HHS proposes requiring (i) encryption of all ePHI, with certain limited exceptions, and (ii) multi-factor authentication across the regulated entity's systems.

Policy Outlook

Over the last five years, OCR has documented a significant increase in major privacy breaches, with a new record of 167 million individuals affected in 2023. According to HHS, the increase reflects more aggressive and sophisticated hacking and ransomware attacks, such as the 2024 Change Healthcare cyberattack. The Biden Administration intends for the NPRM, if finalized, to better protect individuals' ePHI against cyberattacks. The comment period, however, ends after the Trump Administration takes office, requiring the new Administration to finalize these amendments. Finalizing the NPRM is unlikely to happen quickly given routine procedural requirements under the Administrative Procedure Act, as well as the time it will take for the incoming Administration to pause and review pending rules.

More generally, although it is unclear what direction the incoming Administration will go in strengthening the country's defenses against cyberattacks, including health care cyberattacks, it is likely that both congressional and regulatory steps will be taken to mitigate potential threats. Cybersecurity remains a bipartisan issue that will continue to grab the attention of policy makers.

RELATED CAPABILITIES

Digital Health

Health Information Privacy and Security

Government Relations and Public Policy