Unpacking HHS' Proposal To Amend HIPAA Security Rule

By **Sara Shanti, Carolyn Metnick and Michael Sutton** (February 6, 2025)

Sara Shanti

Carolyn Metnick

Michael Sutton

Just in time to bring in the new year, the U.S. Department of Health and Human Services issued a notice of proposed rulemaking on Dec. 27 to significantly amend the Health Insurance Portability and Accountability Act's security rule.

The security rule, which sets forth the security standards for safeguarding electronic protected health information that govern HIPAA covered entities and business associates, has evolved since its inception in 2003. Upon finalization, it would overhaul the security rule such that HIPAA entities would have a series of material operational changes to implement, as detailed below.

The proposed rule was expected, particularly in light of the incredible increase in data breaches affecting the healthcare industry, including the devastating rise of large scale foreign cyberattacks and ransomware. In particular, some experts have cited data compiled by the Office of Civil Rights in determining that the number of healthcare records affected by breaches has increased more than fivefold since 2020, as well as that the number of individuals affected by cyberattacks have nearly tripled since 2022.

Standards for Assessing Adequacy of Safeguards

The security rule generally requires that HIPAA entities implement reasonable and appropriate administrative, physical and technical safeguards to protect the privacy and security of electronic protected health information.

As a starting point, the proposed rule removes the distinction between "required" and "addressable" safeguards, which has the ultimate effect of rendering all safeguard specifications to be required. HIPAA entities have historically relied on the security rule to allow them to be flexible in implementing addressable safeguards, with a specific emphasis on their resources and scale of operations.

The proposed rule would eliminate this distinction by requiring that HIPAA entities implement all of the standards and specifications, although it would continue to afford a measure of flexibility regarding the manner of implementation.

In other words, the proposed rule would not eliminate the security rule's flexible nature in requiring that all safeguards be applied, but would offer certain factors to be considered in assessing the adequacy of each safeguard, including:

- The size, complexity and capabilities of the entity;

- The entity's technical infrastructure, hardware and software security capabilities;

- The costs of the security measures;

- The probability and criticality of potential risks to electronic protected health information; and

- The effectiveness of the security measure in supporting the resiliency of the entity.

If implemented, HIPAA entities must reevaluate their security frameworks and safeguards to ensure complete implementation of each referenced specification, including encryption, multifactor authentication and network segmentation, among numerous others discussed in greater detail below.

Updated Safeguard Specifications

The security rule has previously established a list of safeguards for how HIPAA entities should go about safeguarding electronic protected health information, and the proposed rule overhauls these requirements by expanding on existing specifications as well as by adding new specifications, including the below.

1. Written Inventory of Technology Assets and a Network Map

The proposed rule would require development of a written inventory of technology assets as well as a network map, where electronic protected health information may be created, received, maintained or transmitted. HIPAA entities must update the inventory and map at least annually.

2. Encryption

The proposed rule would require that HIPAA entities encrypt electronic protected health information both in transit and at rest, while also providing a number of exceptions, such as where the technology assets currently in use do not support encryption, and the HIPAA entity in question adopts a written plan to migrate electronic protected health information to a technology that supports encryption.

While not entirely new, as encryption was previously considered to be addressable, many entities may not have appreciated the importance of ensuring encryption of electronic protected health information when it is being transmitted as well as when it is being stored, such as on a local device, server or even on a cloud.

3. Multifactor Authentication

The proposed rule would require HIPAA entities to deploy multifactor authentication for any action that would change a user's privileges to the HIPAA entity's relevant electronic information systems in a manner that would alter the user's ability to affect the confidentiality, integrity or availability of electronic protected health information. The

effectiveness of such technical controls must be tested at least once every 12 months.

4. Contingency Plans

The proposed rule expands the existing obligation to implement written contingency plans, which must include policies and procedures for responding to emergencies such as fires, system failures and natural disasters.

In particular, the proposed rule would require HIPAA entities to conduct and document the relative criticality of its relevant electronic information systems and implement written policies and procedures to restore loss of critical relevant electronic information systems and data within 72 hours of loss. HIPAA entities would also be required to test such plans at least once every 12 months, document the results of such tests, and modify the plans as appropriate.

5. Network Segmentation

The proposed rule would require HIPAA entities to implement written policies and procedures that segment networks in a manner that limits access to electronic protected health information through authorized workstations.

In addition, the proposed rule would require implementation of technical controls to facilitate network segmentation. This requirement would necessitate completion of an assessment of network architectures, which would likely require consultation with technical experts.

6. Vulnerability Scans

The proposed rule would require HIPAA entities to conduct automated vulnerability scans to identify technical vulnerabilities in accordance with the HIPAA entity's security risk analyses, or SRAs, or at least once every six months, whichever is more frequent.

7. Penetration Testing

The proposed rule would require HIPAA entities to complete penetration testing in accordance with the HIPAA entity's SRAs or at least once every six months, whichever is more frequent.

Penetration testing would need to be conducted through a qualified person with appropriate knowledge of and experience with generally acceptable cybersecurity principles and methods, such as the standards promulgated by the National Institute of Standards and Technology.

8. Backups

The proposed rule would require HIPAA entities to deploy technical controls to create and maintain retrievable copies of electronic protected health information, which are sufficient to ensure that retrievable copies are no more than 48 hours old. In addition, the proposed rule would require deployment of technical controls that alert workforce members in real time of failures and error conditions in required data backups, as well as which record the success, failure and error conditions of backups.

The foregoing technical controls must be tested at least monthly.

While many HIPAA entities may have already implemented variations of the safeguards noted above, many have not, and most would, at a minimum, require updates to meet the proper documentation and timing specifications. If finalized, the above technical safeguards would likely impose an increased administrative and technical burden on HIPAA entities, not the least of which would be cost and risk of compliance violations especially in the event of an investigation by regulators following a security incident or breach.

Updated Standards for Security Risk Analyses

HIPAA security rule risk analyses have been tremendous tools for detecting and addressing vulnerabilities that may otherwise go unnoticed and threaten the security of protected health information.

In addition, SRAs have been a key focus of regulators, including the Office of Civil Rights, which frequently request copies of SRAs in the course of breach investigations to assess whether HIPAA entities acted proactively to identify and remediate security vulnerabilities and, as a result, reasonably avoid security incidents.

The proposed rule seeks to bring clarity by memorializing specific features that the Office of Civil Rights expects of SRAs in order for them to be deemed adequate and effective, many of which are consistent with industry norms, including:

- Review a written inventory of technology assets as well as a network map, which is required to be prepared;

- Compile a list of reasonably anticipated threats to the confidentiality, integrity and availability of electronic protected health information as well as potential vulnerabilities to the HIPAA entity's electronic information systems;

- Complete a documented assessment of the measures the HIPAA entity uses to ensure the security of electronic protected health information;

- Complete a determination of the likelihood that each identified threat may be exploited, and the potential effect of each identified threat in the event of successful exploitation;

- Complete a corresponding assessment of the risk level for each identified threat and vulnerability, considering the likelihood that the threat/vulnerability may be exploited; and

- Complete an assessment of the risks to electronic protected health information that may result from entering into or continuing a business associate agreement, or other agreement with a business associate.

In addition, the proposed rule would also require HIPAA entities to update SRAs on an ongoing basis, but not less frequently than once every 12 months or after a change in a HIPAA entity's environment or operations that may affect electronic protected health information. While completion of an annual SRA has always been recommended, it was not necessarily required.

Updated Standards for Business Associate Agreements

The proposed rule makes a number of revisions to the requirements applicable to arrangements with business associates, including: (1) requiring business associates to notify covered entities upon activation of their contingency plans no later than 24 hours after activation, which would be required to be prepared under the proposed rule; and (2) requiring that covered entities obtain written verification from their business associates, at least once every 12 months, that such business associates have deployed technical safeguards required by the security rule.

If finalized, the proposed rule would require HIPAA entities to revisit their business associate agreements with existing vendors that would necessitate new negotiations and revisions to existing templates across enterprises. As business associate agreements will be changing, adopting appropriately modernized template business associate agreements will be critical to ensure both uniformity and compliance across a range of business relationships.

In addition, ensuring completion of the annual written verification would also present an administrative hurdle, which would be difficult to track, particularly for business associates supporting many covered entities or covered entities relying on a broad array of business associates to sustain their operations.

Takeaways

While not yet finalized, the sweeping changes set forth in the proposed rule amount to nothing short of a referendum on the industry, reflecting a clear concern over the future of health data security. Looking ahead, there are several critical takeaways that the industry should keep in mind:

- HIPAA must ensure ongoing compliance with the current security rule, which remains in effect until HHS publishes a final rule. As has been the case for previous HIPAA-related rulemaking, HHS will likely receive and consider tens of thousands of public comments.

- With the Trump administration assuming power, the proposed rule will likely receive increased scrutiny and may be stalled by the flurry of executive orders and actions that have occurred, including efforts to freeze agency publication of rules and related activities.

- HIPAA entities and other industry participants should proactively assess their operations in light of the proposed rule, especially with respect to safeguarding against cyberattacks and other threats. Proactive action is critical to safeguarding health information.

- The protection of health information will remain a priority at the state and federal level in light of increased cybersecurity threats that are increasingly recognized as national security concerns. Separately, states like New York recently considered a robust health information privacy law, which, if enacted, would impose significant requirements on entities that process such data.

- While the proposed rule does not include changes that are specific to artificial intelligence, HHS is seeking comments on how new and emerging technologies, including AI, are subject to the security rule. As such, HHS is clearly mindful of the importance and unfolding effect that AI will have on the industry and the potential for increased security threats relating to the use of such tools.

Sara Shanti and Carolyn Metnick are partners, and Michael Sutton is an associate, at Sheppard Mullin Richter & Hampton LLP.