HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information

Fact Sheet

https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html

On December 27, 2024, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) to modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule to strengthen cybersecurity protections for electronic protected health information (ePHI). OCR administers and enforces the Security Rule, which establishes national standards for the protection of individuals' ePHI by covered entities (health plans, health care clearinghouses, and most health care providers), and their business associates (together, regulated entities). Today's proposed rule seeks to strengthen cybersecurity by updating the Security Rule's standards to better address ever-increasing cybersecurity threats to the health care sector.

The proposed rulemaking is one of many actions taken by HHS in support of President Biden's commitment to improving the cybersecurity of critical infrastructure. In 2023, the Biden-Harris Administration released the National Cybersecurity Strategy and its plan for implementing the strategy; version 2 was released in May of 2024.[1] Also in 2023, HHS released its Healthcare Sector Cybersecurity concept paper outlining the Department's path forward to advance cybersecurity enhancements for the health care sector.[2] These plans included the publication of voluntary cybersecurity best practices and a strategy for greater cybersecurity enforcement and accountability, which included updating the HIPAA Security Rule with new cybersecurity requirements.

The NPRM proposes to strengthen the Security Rule's standards and implementation specifications with new proposals and clarifications, including:

- Remove the distinction between "required" and "addressable" implementation specifications and make all implementation specifications required with specific, limited exceptions.
- Require written documentation of all Security Rule policies, procedures, plans, and analyses.

- Update definitions and revise implementation specifications to reflect changes in technology and terminology.
- Add specific compliance time periods for many existing requirements.
- Require the 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.
- Require greater specificity for conducting a risk analysis. New express requirements would include a written assessment that contains, among other things:
    - A review of the technology asset inventory and network map.
    - Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI.
    - Identification of potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems
    - An assessment of the risk level for each identified threat and vulnerability, based on the likelihood that each identified threat will exploit the identified vulnerabilities.
- Require 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 for planning for contingencies and responding to security incidents. Specifically, regulated entities would be required to, for example:
    - Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.
    - Perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration.
    - Establish written security incident response plans and procedures documenting how workforce members are to report suspected or known security incidents and how the regulated entity will respond to suspected or known security incidents.
    - Implement written procedures for testing and revising written security incident response plans.
- Require regulated entities to conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.
- Require that business associates verify at least once every 12 months for covered entities (and that business associate contractors verify at least once every 12 months for business associates) that they have deployed technical safeguards required by the Security Rule 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.
- Require encryption of ePHI at rest and in transit, with limited exceptions.

- Require regulated entities to establish and deploy technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner. New express requirements would include:
    - Deploying anti-malware protection.
    - Removing extraneous software from relevant electronic information systems.
    - Disabling network ports in accordance with the regulated entity's risk analysis.
- Require the use of multi-factor authentication, with limited exceptions.
- Require vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Require network segmentation.
- Require separate technical controls for backup and recovery of ePHI and relevant electronic information systems.
- Require regulated entities to review and test the effectiveness of certain security measures at least once every 12 months, in place of the current general requirement to maintain security measures.
- Require business associates to notify covered entities (and subcontractors to notify business associates) upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.
- Require group health plans to 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 administrative, physical, and technical 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.

While the Department is undertaking this rulemaking, the current Security Rule remains in effect.

HHS encourages all stakeholders, including patients and their families, health plans, health care providers, health care professional associations, consumer advocates, and government entities, to submit comments through regulations.gov.

Public comments on the NPRM are due 60 days after publication of the NPRM in the Federal Register. The Department will also be conducting a Tribal consultation meeting soon. Information and RSVP details are forthcoming.

The NPRM may be viewed or downloaded at: https://www.federalregister.gov/public-inspection/2024-30983/health-insurance-portability-and-accountability-act-security-rule-to-strengthen-the-cybersecurity-of

Endnotes

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf - PDF.

[2] https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf - PDF.

Content created by Office for Civil Rights (OCR)
Content last reviewed December 27, 2024