Hacking Heathcare - Weekly Blog

Hacking Healthcare	TLP:WHITE	Alert Id: 088787ea	2025-01-10 19:33:59

This week, Health-ISAC®'s Hacking Healthcare® opens 2025 with a look at the new proposed revisions to the HIPAA Security Rule. After providing a high-level overview of what the U.S. Department of Health and Human Services ("HHS") has put forward, we will dive into the analysis section to provide our thoughts on what is included and what the potential path forward for this revision might be as we transition to the Trump administration.

Welcome back to Hacking Healthcare®.

HHS Publishes Proposed HIPAA Security Rule Revision

While it may have taken a little longer than was initially expected, on January 6, HHS officially published their notice of proposed rulemaking ("NPRM") to modify the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule") under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act").

Coming in at just under 400 pages of text,[i] the NPRM is roughly broken into five sections. Sections 1 and 2 make up the first 25 pages and cover the executive summary, HHS statutory authority to conduct this update, and the regulatory history behind it. Starting on page 26 and continuing until page 71, Section 3 provides detailed justifications for why HHS is proposing these modifications. The bulk of the NPRM is within Section 4, which runs to page 299. This section provides a "section-by-section" description of all the proposed changes alongside explanations as to why they are being proposed. Finally, Section 5 provides a detailed regulatory impact analysis.

Why is HHS proposing an update?

A lot has changed since the last time the HIPAA Security Rule was revised in 2013. Some of these new developments are rather obvious, such as the continual evolution of technology generally, the increased adoption and modernization of technology used by regulated entities, and the growth in scale and complexity of the threat environment. Perhaps less obvious to many, HHS also cited the negative impact of certain court decisions[ii] and the HHS's own audit experience, revealing a widespread failure of regulated entities to fully comply with the standards and implementation specifications of the Security Rule.

What approach is HHS taking?

HHS describes their NPRM as a substantial revision of the regulatory text to explicitly codify any activities that are critical to protecting the security of ePHI as requirements and to provide greater detail for such requirements while not substantially changing existing obligations. While the proposal would reduce the flexibility of the current rule to some degree, it would still largely retain the non-prescriptive approach.

What are the proposed changes?

Over 200 pages of the NPRM are dedicated to a section-by-section description of the current security rule provisions, the particular issues that HHS identified, and the proposed solutions. While we cannot adequately cover them all here, HHS's Fact Sheet summarized many of the more significant proposed changes:[iii]

- 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 antimalware 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 multifactor 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.

What happens now?

The NPRM is open to comments until March 7 (60 days from publication). After the comment period closes, the expectation is that HHS will review stakeholder input and consider revisions before revising the proposal into a final rule. HHS has indicated that the effective date for the final rule would be 60 days from its publication. The compliance date would be 180 days from the effective date, and there would be an additional transition period to modify business associate contracts or other written arrangements that qualify.

Action & Analysis

Included with Health-ISAC Membership

Member Engagement

While it isn't clear what may happen with this effort after the Trump administration transition, any final rule might be in place for many years. As such, we highly encourage Health-ISAC members to review the entirety of the NPRM and to provide HHS with detailed comments on the proposals you agree and disagree with.

Health-ISAC, in partnership with the Health Sector Coordinating Council, will submit comments on behalf of the health industry. For organizations that want to submit their own comments directly to HHS, follow the instructions in the Fact Sheet. If you would like to have Health-ISAC submit your comments as part of the overall industry voice, please send your inputs to membership@h-isac.org. We will be accepting member inputs until February 21, so that we can consolidate the comments and submit them in aggregate by the HHS deadline of March 7.

[i] Page numbers reflect the PDF version of the document that was published for Public Inspection on December 27th at U.S. Federal Register website (https://public-inspection.federalregister.gov/2024-30983.pdf). This format of the text is generally more navigable and easier to read than the printed version published at https://www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf

[ii] In particular, HHS cites University of Texas M.D. Anderson Cancer Center v. HHS whereby the U.S. Court of Appeals for the Fifth Circuit decision effectively stated that the Security Rule does not say anything about how effective an encryption mechanism used to satisfy requirements must be.

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

[iv] https://public-inspection.federalregister.gov/2024-30983.pdf

[v] https://public-inspection.federalregister.gov/2024-30983.pdf

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

Reference(s): govinfo, federalregister, HHS
Report Source(s): Health-ISAC
Release Date: Jan 11, 2025 (UTC)

Tags: Rulemaking, Security Rule, Regulation, Hacking Healthcare, HHS, HIPAA
TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
For Questions and/or Comments:
Please email us at contact@h-isac.org
Conferences, Webinars, and Summits:
https://h-isac.org/events/
Hacking Healthcare:
Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal:
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).