# Proposed changes to HIPAA Security Rule aim to enhance cybersecurity measures



On December 27, 2024, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced a Notice of Proposed Rulemaking (NPRM) aimed at amending the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This NPRM is designed to bolster cybersecurity protections for electronic protected health information (ePHI) and aligns with the Biden-Harris Administration's 2023 National Cybersecurity Strategy.

This NPRM marks a pivotal update, being the first substantial revision to the HIPAA Security Rule in over a decade. The proposed changes include updates to existing definitions, the removal of the distinction between “required” and “addressable” implementation specifications, and the establishment of all specifications as “required,” with a few exceptions. Furthermore, the NPRM sets specific compliance timelines for numerous existing requirements and mandates comprehensive documentation of Security Rule policies, procedures, plans, and analyses by all HIPAA-regulated entities.

Several key modifications to the Security Rule are highlighted within the NPRM, including:

**Administrative Safeguards:**- **Asset Inventory:** Entities will be required to maintain an ongoing technology asset inventory and a network map, detailing the movements of ePHI, at least annually and whenever operational changes occur.

* Risk Analysis: The NPRM stipulates a detailed risk analysis process that incorporates a review of the asset inventory and network map, identification of potential threats, and assessments of risk levels.
* Patch Management: HIPAA-regulated entities will need to implement formal policies for patch management, requiring reviews and modifications at least annually, alongside timely updates based on the associated risks.
* Workforce Notification: Entities must notify relevant covered parties within 24 hours when a workforce member's access to ePHI is modified or revoked.
* Security Incident Preparedness: The NPRM requires Written procedures for immediate restoration of affected electronic systems within 72 hours of a security incident, enhancing contingency planning.
* Compliance Audits: Entities will be mandated to conduct annual compliance audits to verify Security Rule adherence.
* Oversight of Business Associates: Business associates must confirm annually that they have deployed technical safeguards required by the Security Rule.

**Physical Safeguards:**- The NPRM demands that entities establish robust physical access control policies to safeguard electronic information systems.

**Technical Safeguards:**- Notable requirements in technical safeguards include network segmentation, encryption protocols for ePHI both in transit and at rest, and configuration management practices that stipulate deploying anti-malware protections.

* Additionally, multi-factor authentication will be required for all technology assets in governed information systems, alongside regular vulnerability scanning and penetration testing.
* Entities will also be responsible for ensuring timely backups of ePHI, with recoverable data not exceeding 48 hours older than current data.

While these proposed regulations are currently under review, the existing Security Rule continues to apply until the NPRM is formally enacted. A public commentary period will be open for 60 days following the NPRM's publication in the Federal Register.

The proposed changes signal a significant shift in the regulatory landscape concerning ePHI, necessitating that HIPAA-regulated entities begin evaluating their cybersecurity frameworks in light of the updated requirements. Many alterations suggested in the NPRM have already been in practice due to enforcement actions from the Federal Trade Commission and Attorney General offices across various states, reflecting a growing trend towards rigorous cybersecurity measures within the healthcare sector.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.hstoday.us/subject-matter-areas/cybersecurity/proposed-hipaa-security-rule-aims-to-boost-cybersecurity-for-electronic-health-information/> - Corroborates the announcement of the Notice of Proposed Rulemaking (NPRM) by the HHS Office for Civil Rights to enhance cybersecurity protections for ePHI under the HIPAA Security Rule.
2. <https://www.jdsupra.com/legalnews/proposed-updates-to-hipaa-security-rule-1314208/> - Details the proposed updates to the HIPAA Security Rule, including the alignment with industry best practices like the NIST Cybersecurity Framework and GDPR, and the need for enhanced cybersecurity measures in response to growing cyberattacks.
3. <https://www.hipaajournal.com/hhs-strengthened-hipaa-security-rule/> - Provides information on the proposed rule to upgrade the HIPAA Security Rule, including updates to existing definitions and the removal of the distinction between 'required' and 'addressable' implementation specifications.
4. <https://www.hstoday.us/subject-matter-areas/cybersecurity/proposed-hipaa-security-rule-aims-to-boost-cybersecurity-for-electronic-health-information/> - Explains the administrative safeguards, such as asset inventory, risk analysis, patch management, workforce notification, and security incident preparedness, as outlined in the NPRM.
5. <https://www.jdsupra.com/legalnews/proposed-updates-to-hipaa-security-rule-1314208/> - Discusses the physical safeguards and the requirement for robust physical access control policies to safeguard electronic information systems.
6. <https://www.hipaajournal.com/hhs-strengthened-hipaa-security-rule/> - Details the technical safeguards, including network segmentation, encryption protocols, configuration management, multi-factor authentication, and regular vulnerability scanning and penetration testing.
7. <https://www.hstoday.us/subject-matter-areas/cybersecurity/proposed-hipaa-security-rule-aims-to-boost-cybersecurity-for-electronic-health-information/> - Mentions the requirement for timely backups of ePHI and the need for recoverable data not exceeding 48 hours older than current data.
8. <https://www.jdsupra.com/legalnews/proposed-updates-to-hipaa-security-rule-1314208/> - Explains the compliance audits and oversight of business associates, including annual confirmations of deployed technical safeguards.
9. <https://www.hipaajournal.com/hhs-strengthened-hipaa-security-rule/> - Highlights the public commentary period and the significance of the proposed changes in the regulatory landscape concerning ePHI.
10. <https://www.hstoday.us/subject-matter-areas/cybersecurity/proposed-hipaa-security-rule-aims-to-boost-cybersecurity-for-electronic-health-information/> - Corroborates that the proposed changes are part of the Biden-Harris Administration's 2023 National Cybersecurity Strategy and mark the first substantial revision to the HIPAA Security Rule in over a decade.
11. <https://www.jdsupra.com/legalnews/hhs-ocr-issues-notice-of-proposed-8314152/> - Please view link - unable to able to access data