POLSINELLI

Publications

January 6, 2025 • Updates

OCR Proposes Regulatory Facelift to the HIPAA Security Rule: Addressing the Current Cybersecurity Environment with More Specificity and Additional Requirements

On January 6, 2025, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published a "Notice of Proposed Rulemaking," *HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information* (the "Proposed Rule").[1]

The Proposed Rule aims to strengthen cybersecurity protections for electronic protected health information (ePHI), including pursuant to a March 1, 2023, directive from President Biden.[2] Specifically, OCR is revising the HIPAA Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") to address the following:

1. Changes in the health care sector;
2. Significant increases in breaches and cyber-attacks;
3. Common deficiencies OCR observed in investigations into Security Rule compliance by HIPAA covered entities and their business associates (collectively, "Regulated Entities");
4. Cybersecurity guidelines, best practices, methodologies, procedures and processes; and
5. Court decisions that affect the enforcement of the Security Rule.

Highlights of Proposed Changes

With respect to all ePHI, the Proposed Rule removes the distinction between "required" and "addressable" implementation specifications for all types of enumerated safeguards under the Security Rule and makes all implementation specifications required with specific, very limited exceptions. The Proposed Rule also includes changes to—and the addition of new—definitions used in the Security Rule, bringing such definitions in line with current cybersecurity risk and control environments (e.g., multi-factor authentication). The Proposed Rule includes sweeping changes with increased specificity to the standards and implementation specifications to both Administrative and Technical Safeguard requirements.

Related People

- ILIANA L. PETERS
- Rebecca Frigy Romine
- Hiba Al-Ramahi

Related Capabilities

- Privacy & Cybersecurity
- HIPAA/Health Information Privacy & Security

Administrative Safeguards

Under the proposed changes, Regulated Entities would be required to implement and document, in writing, their implementation of the administrative safeguards required by the Security Rule.

In place of the existing standard for security management process, Regulated Entities would be required to develop a technology asset inventory and a network map that illustrates the movement of ePHI into, through, and out of the Regulated Entity's electronic information system(s). As an example, OCR has proposed a Regulated Entity's network map must include the technology assets used by its business associates, including offshore business associates, regardless of the physical location of such assets, even though such assets are not part of the Regulated Entity's own electronic information system.

With respect to the risk analysis (sometimes referred to as an enterprise security risk assessment) standard, OCR proposes eight specific implementation specifications that Regulated Entities would be required to perform and document, and to review, verify and update on an ongoing and at least every 12-month basis:

1. Review the technology asset inventory and the network map to identify where ePHI may be created, received, maintained or transmitted within its information systems.
2. Identify all reasonably anticipated threats to the confidentiality, integrity and availability of ePHI that it creates, receives, maintains or transmits.
3. Identify potential vulnerabilities and predisposing conditions to the Regulated Entity's relevant electronic information systems—that is, its electronic information systems that create, receive, maintain or transmit ePHI or that otherwise affect the confidentiality, integrity or availability of ePHI.
4. Create an assessment and documentation of the security measures it uses to ensure that the measures protect the confidentiality, integrity and availability of the ePHI created, received, maintained or transmitted by the Regulated Entity.
5. Make a reasonable determination of the likelihood that each identified threat would exploit the identified vulnerabilities.
6. Make a reasonable determination of the potential impact of each identified threat should it successfully exploit the identified vulnerabilities.
7. Create an assessment of risk level for each identified threat and vulnerability.
8. Create an assessment of risks to ePHI posed by entering into or continuing a business associate agreement or other written arrangement with any prospective or current business associate, respectively, based on the written verification obtained from the prospective or current business associate.

Other proposed changes to the administrative safeguard requirements include that a Regulated Entity must:

- Implement more detailed written procedures related to patch management and configuration updates, including addressing timely evaluation and installation of patches. The Proposed Rule includes risk-based timeframes in which a patch, configuration, or upgrade must be applied.
- Related to information access management, establish written policies and procedures that ensure that Regulated Entity's relevant electronic information systems are segmented to limit access to ePHI to authorized workstations.
- Perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration.
- Establish written procedures to restore the loss of certain critical relevant electronic information systems and data within 72 hours.

- 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, as well as written procedures for testing and revising written security incident response plans.
- Conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.
- Require business associates to verify in writing at least once every 12 months to covered entities (and business associate subcontractors verify at least once every 12 months to their immediate upstream business associate) that (i) 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 (ii) certification by someone with authority to act on behalf of the business associate that the analysis has been performed and is accurate.

Technical Safeguards

Generally, OCR retains the requirements for technical safeguards and proposes additions and modifications to the existing standards and implementation specifications. Under the Proposed Rule, Regulated Entities would need to:

- Encrypt ePHI at rest and in transit, with limited exceptions.
- 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 and disabling network ports in accordance with the Regulated Entity's risk analysis.
- Use multi-factor authentication, with limited exceptions.
- Perform vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Perform network segmentation.
- Implement separate technical controls for backup and recovery of ePHI and relevant electronic information systems.

Physical Safeguards

Generally, OCR retains the four standards that comprise the Security Rule's physical safeguards and proposes several modifications to address OCR's expectations regarding implementation specifications, memorializing policies and procedures in writing, documenting the implementation of, reviewing, and modifying such policies and procedures and clarifying the scope of the electronic information systems and their components that Regulated Entities are expected to consider when establishing their policies and procedures.

Business Associate Agreements

To address the increased risk of security incidents and deficiencies in protections, OCR proposes an implementation specification that would require a business associate agreement to include a provision for a business associate to report to the covered entity (and subcontractors to notify business associates) activation of its contingency plan (maintained in compliance with 45 CFR 164.308(a)(13)) without unreasonable delay, but no later than 24 hours after activation. The Proposed Rule does not require reporting on the cause of the contingency plan activation; rather, reporting is required solely on the fact that the contingency plan was activated. Additionally, this proposed requirement would not alter the business associate's breach reporting obligations under the Breach Notification Rule.

Documentation Requirements

While 45 C.F.R. § 164.316 currently addresses policies and procedures and documentation, the section does not require or include standards to govern how Regulated Entities must implement, maintain and document the implementation of all security measures. OCR believes this to be a deficiency and therefore proposes the following requirements for Regulated Entities:

1. Have written documentation of all required Security Rule policies, procedures, actions, activities, assessments and analyses.
2. Review and update documentation for security measures at least once every 12 months.

Specific Requirements for Health Plans

The Proposed Rule requires group health plans to include certain requirements in their plan documents for their group health plan sponsors to:

1. Comply with the administrative, physical and technical safeguards of the Security Rule;
2. Ensure that any agent to whom they provide ePHI agrees to implement the administrative, physical and technical safeguards of the Security Rule; and
3. Notify their group health plans upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.

Public Comments

Public comments on the Proposed Rule are due 60 days after publication of the Proposed Rule in the Federal Register, which is March 7, 2025.

[1] *See* Health Insurance Portability and Accountability Act Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 898 (Jan. 6, 2025), *available at* https://www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf.

[2] *See* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.