PUBLICATION

Proposed HIPAA Security Rule Updates

Authors: Alisa L. Chestler, Layna S. Cook Rush

January 09, 2025

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) on December 27, 2024, to update the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule and its requirements. The official version was published on January 6, 2025. This is the first update in a decade for the security framework that has been in effect since 2003. Based on the preamble language, the proposed changes evidence OCR's frustration with covered entities and their business associates due to persistent noncompliance with many of the regulations it routinely encounters in investigations. When the Security Rule was adopted in 2003, its standards were purposefully developed to be scalable and flexible so that health care entities could implement security measures appropriate to their size, complexity, and specific needs, rather than requiring a one-size-fits-all approach. While OCR maintains that a level of flexibility remains, the updates are intended to bring specificity to several cybersecurity requirements for electronic protected health information (ePHI). Many of the new requirements are now considered standard practice in the health care industry but are specifically articulated in the proposed changes to reduce confusion in the industry and improve clarity about compliance obligations and the OCR's expectations. Additionally, the new requirements better align with the NIST Cybersecurity Framework and HHS' Cybersecurity Performance Goals which were promulgated in the spring of 2024.

Artificial Intelligence and Emerging Technologies

Of note, the NPRM devotes a section to new and emerging technologies including not only artificial intelligence but also quantum computing and virtual and augmented reality. All three have significant implications for the uses and disclosures of information, and OCR wants to ensure that all organizations with compliance obligations devote time and resources to the appropriate understanding of how emerging technologies will affect the privacy and security programming of the organization. Even if an organization does not anticipate the affirmative use of quantum computing or virtual and augmented reality technologies in the near future, the strategic and cyber considerations must be considered now by both privacy and security professionals.

All Standards are Required and Not Merely Addressable

The NPRM makes numerous changes to the sections of the Security Rule on administrative, physical, and technical safeguards, as well as organizational and documentation requirements. Some of the modifications are made through the sections. For instance, the NPRM removes the distinction between "required" and "addressable" implementation specifications and makes all implementation specifications required with specific, limited exceptions. OCR opined that in the past, organizations have mistaken "addressable" with "optional" and have failed to articulate how the specification was to be implemented.

Written Documentation

Additionally, the OCR has always required written documentation; however, the previous articulation of this was apparently not strong enough for organizations to understand the obligation to maintain all Security Rule policies and procedures in written form and to regularly evaluate and update the documentation to correspond with the evolving IT environment(s). The NPRM specifies the requirement for written documentation according to the security standards.

Compliance Time Periods

OCR proposes specific compliance time periods for many existing requirements to ensure organizations understand the expectations. New implementation specifications for review, verification, and update of policies and procedures at least once every 12 months are included. Regulated entities must also review and test the effectiveness of certain security measures at least once every 12 months. There are specific requirements for vulnerability scanning at least every six months and penetration testing at least once every 12 months. These activities are considered industry standard, as they are generally not expensive and are incredibly helpful in their ability to identify potential exposures before they are exploited by threat actors.

Updated and New Defined Terms

OCR also articulates numerous updates to current definitions and adds new defined terms to reflect changes in technology and to help illustrate what effective compliance requires. For example, OCR proposes to clarify the definition of "workstation" to include additional examples of what constitutes a workstation that were not prevalent when the Security Rule was originally adopted including a server, virtual device, and a mobile device such as a smartphone or tablet. The NPRM adds a definition for "deploy" to mean "to configure technology for use and implement such technology." The addition is to address the concern that some regulated entities merely adopt policies and procedures addressing technical requirements but do not actually apply the policies and procedures throughout their enterprise. Additional new regulatory terms include "implement," "electronic information system," "multifactor authentication," "relevant electronic information system," "risk," "technical controls," "technology asset," "threat," and "vulnerability."

New Security Standards

The NPRM includes a number of new standards, some of which are detailed below:

- **Technology Asset Inventory**. While one could argue an asset inventory is implicitly required to meet existing security standards, OCR will 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. OCR further articulated a specific obligation to update the inventory at least once every 12 months and in response to a change in the regulated entity's environment or operations that may affect ePHI.

- **Compliance Audits**. This new standard requires regulated entities to perform and document an audit of their compliance with each standard and implementation specification of the Security Rule at least once every 12 months. Given OCR's limited resources to perform audits of regulated entities, this requirement would likely be a critical piece of documentation when OCR or a state attorney general is investigating noncompliance concerns or a breach. The Compliance Audit may prove helpful in mitigating the OCR's concern that the organization has not appropriately monitored compliance.

- **Patch Management**. The proposed changes would require a regulated entity to implement written policies and procedures for applying patches and updating the configuration of its relevant information systems. The OCR opined that this proposed standard would ensure that a regulated entity is aware of its liability for appropriately safeguarding ePHI by installing patches, updates, and upgrades throughout its relevant electronic information systems.

- **Encryption and Decryption**. Encryption and decryption were addressable implementation specifications for the Transmission Security standard. They are redesignated as a required standard. Encryption was previously expensive and complicated and therefore addressable, leaving some ability for an organization to avoid encryption for certain systems. The NPRM would require encryption of ePHI at rest and in transit, with limited exceptions.

- **Configuration Management**. This proposed standard would require the establishment and deployment of technical controls to secure relevant electronic information systems and technology assets in its relevant electronic information systems, including workstations, in a consistent manner. A regulated entity also would be required to establish a baseline level of security for each relevant electronic information system and technology asset and to maintain such information systems and technology assets according to those secure baselines.

- **Vulnerability Management**. This new standard would require a regulated entity to deploy technical controls to identify and address technical vulnerabilities in the regulated entity's relevant electronic information systems. The deployment of technical controls should be consistent with the regulated entity's patch management policies and procedures.

- **Data Back Up and Recovery**. The proposed standard would require a regulated entity to deploy technical controls to create and maintain exact retrievable copies of ePHI. The proposed changes would remove the existing implementation specification for this activity from the physical safeguards section and place it in technical safeguards. The OCR opined that elevating data backup and recovery to a standard would increase the prominence of this requirement and highlight the liability of regulated entities for creating the capacity to restore systems after a data breach.

Notable New Implementation Specifications

In addition to elevating some prior implementation specifications to standards and adding new standards, the OCR also proposes several new implementation specifications in support of both prior and new standards. The following are notable implementation specifications that are proposed in the NPRM:

- **Risk Analysis**. The obligations of a risk analysis have been long articulated via guidance; however, OCR will now require greater specificity for conducting a risk analysis. The OCR has proposed eight implementation specifications for the risk analysis that are consistent with prior guidance. The implementations include the following:

  - 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; and
  - 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.

- **Workforce Security**. The OCR imposes a new implementation specification that requires notification of certain other regulated entities within 24 hours when a workforce member's access to ePHI or certain electronic information systems is changed or terminated.

- **Contingency Planning**. The OCR proposes to add specific requirements for planning for contingencies and responding to security incidents. Specifically, regulated entities would be required to:

  - 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; and
  - Implement written procedures for testing and revising written security incident response plans.

- **Business Associate Contracts**. The NPRM adds additional requirements for business associate relationships. Business associates must verify at least once every 12 months 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. Additionally, OCR would 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.

- **Configuration Management**. OCR proposes implementation specifications for the new configuration management standard. The new specifications require regulated entities to establish and deploy technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner and include the following:

  - Deploying anti-malware protection;
  - Removing extraneous software from relevant electronic information systems. Too often obsolete software remains, is forgotten, or becomes an easy target as it is not properly updated or monitored; and
  - Disabling network ports in accordance with the regulated entity's risk analysis.

- **Authentication**. The OCR seeks to clarify that the regulated entity is to deploy technical controls to verify that a person seeking access to the regulated entity's relevant electronic information systems is the one claimed. To that end, the OCR will require the use of multifactor authentication (MFA), with limited exceptions.

- **Access Control**. The OCR proposes new implantation specifications to require technical controls to ensure access is limited to individuals and technology assets that need access. One of the technical controls that will be required is network segmentation. This is likely to be one of the costliest for organizations to implement if they have not yet addressed network segmentation to any degree.

While the HHS is undertaking this rulemaking, the current Security Rule remains in effect. The HHS is seeking comments on the NPRM and has called out specific issues and questions where it is seeing input. Public comments are due by March 7, 2025.

Next Steps

While the regulations are "proposed," much of what is articulated includes certain presumptions of what should exist today and the reality that many regulated entities do not meet the requirements of the existing HIPAA Security Rule or other notable guidance such as the NIST Cybersecurity Framework and HHS' Cybersecurity Performance Goal.

If you have questions or concerns regarding this alert, please contact Alisa L. Chestler, Layna Cook Rush, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity team.