Published on *The National Law Review* https://natlawreview.com

# HHS's Proposed Security Rule Updates Will Substantially Increase the Controls Needed to Comply with the Technical Safeguard Requirements

Article By:

Eric Setterlund

Brett Lawrence

In this week's installment of our blog series on the U.S. Department of Health and Human Services' (HHS) HIPAA Security Rule updates in its January 6 Notice of Proposed Rulemaking (NPRM), we are tackling the proposed updates to the HIPAA Security Rule's technical safeguard requirements (45 C.F.R. § 164.312). Last week's post on group health plan and sponsor practices is available here.

## Existing Requirements

Under the existing regulations, HIPAA-covered entities and business associates must generally implement the following five standard technical safeguards for electronic protected health information (ePHI):

1. **Access Controls –** Implementing technical policies and procedures for its electronic information systems that maintain ePHI to allow only authorized persons to access ePHI.
2. **Audit Controls –** Implement hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI.
3. **Integrity –** Implementing policies and procedures to ensure that ePHI is not improperly altered or destroyed.
4. **Authentication –** Implementing procedures to verify that a person seeking access to ePHI is who they say they are.
5. **Transmission Security –** Implementing technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic network.

The existing requirements either do not identify the specific control methods or technologies to implement or are otherwise "addressable" as opposed to "required" in some circumstances for regulated entities — until now.

## What Are the New Technical Safeguard Requirements?

The NPRM substantially modifies and specifies the particular technical safeguards needed for compliance. In particular, the NPRM restructured and recategorized existing requirements and added stringent standard and implementation specifications, and HHS has proposed removing the distinction between “required” and “addressable” implementation specifications, making all implementation specifications required with specific, limited exceptions.

A handful of the new or updated standards are summarized below:

- **Access Controls –** New implementation specifications to require technical controls to ensure access are limited to individuals and technology assets that need access. Two of the controls that will be required are network segmentation and account suspension/disabling capabilities for multiple log-in failures.
- **Encryption and Decryption –** Formerly an addressable implementation specification, the NPRM would make encryption of ePHI at-rest and in-transit mandatory, with a handful of limited exceptions, such as when the individual requests to receive their ePHI in an unencrypted manner.
- **Configuration Management –** This new standard would require a regulated entity to establish and deploy technical controls for securing relevant electronic information systems and the technology assets in its relevant electronic information systems, including workstations, in a consistent manner. A regulated entity also would be required to establish and maintain a minimum level of security for its information systems and technology assets.
- **Audit Trail and System Log Controls –** Identified as “crucial” in the NPRM, this reorganized standard formerly identified as the “audit control” would require covered entities to monitor in real-time all activity in its electronic information systems for indications of unauthorized access and activity. This standard would require the entity to perform and document an audit at least once every 12 months.
- **Authentication –** This standard enhances the implementation specifications needed to ensure ePHI is properly protected from improper alteration or destruction. Of note, the NPRM would require all regulated entities to deploy multi-factor authentication (MFA) on *all technology assets*, subject to limited exceptions with compensating controls, such as during an emergency when MFA is infeasible. One exemption is where the regulated entity’s existing technology does not support MFA. However, the entity would need to implement a transition plan to have the ePHI transferred to another technology asset that does support MFA within a reasonable time. Medical devices authorized for marketing by the FDA before March 2023 would be exempt from MFA if the entity deployed all recommended updates and after that date if the manufacturer supports the device or the entity deployed any manufacturer-recommended updates or patches.
- **Other Notable Standards –** In addition to the above, the NPRM would add standards for integrity, transmission security, vulnerability management, data backup and recovery, and information systems backup and recovery. These new standards would prescribe new or updated implementation specifications, such as conducting vulnerability scanning for technical vulnerabilities, including annual penetration testing and implementing a patch management program.

Listen to this article



National Law Review, Volume XV, Number 37

Source URL:https://natlawreview.com/article/hhss-proposed-security-rule-updates-will-substantially-increase-controls-needed