HIPAA Security Rule Overview

John Petrozzelli

Director, MassCyberCenter

Agenda

- Overview of Proposed Security Rule
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Current Provisions

Under these rules, regulated entities are required to do all of the following:

- Ensure the confidentiality, integrity, and availability of all ePHI the regulated entity creates, receives, maintains, or transmits.
- Protect against reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information not permitted by the Privacy Rule.
- Ensure that workforce members comply with the Security Rule.

Rulemaking now - Effective date 60 days after publication

Regulated entities would have until the “compliance date” to establish and implement policies, procedures, and practices to achieve compliance with any new or modified standards.

Regulated entities would be permitted to comply earlier than the compliance date, but the Department would not take action against them for noncompliance with the proposed changes that occurs before the compliance date. Except as otherwise provided, 45 CFR 160.105 provides that regulated entities must comply with the applicable new or modified standards or implementation specifications no later than 180 days from the effective date of any such change.

“Required” vs “Addressable” Implementation

The NPRM proposes to strengthen the Security Rule’s standards and implementation specifications with new proposals and clarifications, including remove the distinction between “required” and “addressable” implementation specifications and make all implementation specifications required with specific, limited exceptions.

Elements of the Security Rule

Administrative Safeguards – actions, policies, and procedures to manage the selection, development, implementation, and maintenance (including reviewing and modifying) of security measures to protect ePHI.

Physical Safeguards – policies and procedures that limit physical access to their relevant electronic information systems to only authorized workforce members.

Technical Safeguards – “technical safeguards” includes the technology and policy and procedures for its use that protect ePHI and control access to it.

“Implement” – safeguard must be put into place and be in effect throughout the enterprise, as opposed to only some components of a regulated entity's relevant information systems.

Security Risk Assessment Tool

Downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

- https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Security Rule Policies, Procedures

Written Information Security Program

- Employee Acknowledgement Form
- Acceptable Use Policy
- Facility Security Plan
- Access control Policy
- Onboarding/Offboarding Policy
- Third Party Vendor Risk Management
- Mobile Device and removeable media
- Software and Hardware Asset Management Policy
- Auditing and Accountability
- Vulnerability Management
- Security Awareness and training
- Network Management
- Change Management
- Incident Response Plan
- Business Continuity
- Password Management

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf?language=es

Admin Safeguards
Section B: Required Implementation of Admin Safeguards

Clarify that regulated entities would be required to implement all of the administrative safeguards of the Security Rule to protect the confidentiality, integrity, or availability of all ePHI that they create, receive, maintain, or transmit. Thus, when read together, proposed 45 CFR 164.308(a) and 164.316(a) would require that a regulated entity implement and document, in writing, its implementation of the administrative safeguards required by the Security Rule.

Admin Safeguards
Section C: Asset Inventory and Network Map

Asset Inventory

- Hardware assets that comprise physical elements, including electronic devices and media, that make up an organization's networks and systems. This may include mobile devices, servers, peripherals (*e.g.,* printers, USB hubs), workstations, removable media, firewalls, and routers.
- Software assets that are programs and applications that run on an organization's electronic devices.
- Data assets that include ePHI that an organization creates, receives, maintains, or transmits on its network, electronic devices, and media.

Network Map

- Determine the movement of ePHI into and out of information systems.
- Use a network map to describe that movement.
- Not only mapping the whole network. Also separating out where the ePHI is transiting.

Review and update at least once every 12 months or when system changes.

Admin Safeguards
Sections D and G: Risk Analysis and Risk Management

- Review the technology asset inventory and the network map to identify where ePHI may be created, received, maintained, or transmitted within its information systems.
- Identify all reasonably anticipated threats to the confidentiality, integrity, and availability (CIA) of ePHI that it creates, receives, maintains, or transmits.
- Make a reasonable determination of the likelihood to each identified threat to exploit the identified vulnerabilities.
- Identify potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems.

Risk Management Video

Admin Safeguards
Section F: Patch Management Six changes

1. Establish written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades.
2. Patch, update, and upgrade the configurations of its relevant electronic information systems in accordance with its written policies and procedures and based on the results of:
   a) the regulated entity's risk analysis
   b) vulnerability scans
   c) monitoring of authoritative sources
   d) penetration tests
3. Within 15 calendar days of a patch, update, or upgrade becoming available. 30 days for high risk.
4. Regulated entity would be required to document that an exception applies and that all other applicable conditions are met.
5. Document in real-time the existence of the applicable exception and to implement reasonable and appropriate compensating controls.
6. Regulated entity would be required to implement reasonable and appropriate security measures as compensating controls to address the identified risk according to the timeliness requirements in proposed.

Admin Safeguards
Section K: Workforce Security

Ensure that workforce members only have access to ePHI that they need to perform their assigned functions and are prevented from accessing ePHI that they are not authorized to access to perform such functions.

NIST also recommends establishing criteria and procedures for hiring and assigning tasks and ensuring that these requirements are included as part of the personnel hiring process.

Admin Safeguards
Section L: Information Access Management

Regulated entity must determine those persons and technology assets that need access to ePHI within its environment.

- Role Based Access Control
- Least Privilege
- Onboarding and Offboarding policies
- Segmentation of the network if possible

Admin Safeguards
Section M: Security Awareness training

Requiring a regulated entity to train workforce members to:

- Maintain written policies and procedures
- Guard against, detect, and report suspected or known security incidents, including, but not limited to, malicious software and social engineering.
- At least annual training for each employee. Initially no later than 30 days after the workforce member first has access to the regulated entity's relevant electronic information systems
- Document training provided

Admin Safeguards
Section N: Security Incident Response Procedures

Regulated entity must:

- Implement written procedures for testing and revising the security incident response plan(s) and then, using those written procedures.
- Review and test its security incident response plans at least once every 12 months and document the results of such tests.
- Modify the plan(s) and procedures as reasonable and appropriate, based on the results of such tests and the regulated entity's circumstances.

Admin Safeguards
Section O: Contingency Planning

Perform and document an assessment of the relative criticality of its relevant electronic information systems and technology assets in its relevant electronic information systems.

Establish (and implement as needed) written procedures to restore both its critical relevant electronic information systems and data within 72 hours of the loss, and to restore the loss of other relevant electronic information systems and data in accordance with its criticality analysis.

Test and update plan at least every 12 months.

Admin Safeguards
Section Q: Business Associate Contracts

Regulated entity must obtain written verification from its business associates that they have deployed technical safeguards combined with the existing requirement to obtain written satisfactory assurances that they safeguard ePHI, aligns with the Department's essential CPG for Vendor/Supplier Cybersecurity Requirements.

Section R: Delegation to Business Associate

Regulated entity may permit a business associate to serve as its designated security official. However, a regulated entity that delegates actions, activities, or assessments required by the Security Rule to a business associate remains liable for compliance with all the applicable provisions of the Security Rule.

Physical Safeguards
Section B: Facility Access Controls

Require regulated entities to establish and implement written procedures to both authorize and manage a person's role-based access to facilities.

- Add security cameras to the list of examples of physical security components

Test its written policies and procedures at least once every 12 months, and to modify those policies and procedures as reasonable and appropriate based on that review.

Physical Safeguards
Section C: Workstation Security

Implement physical safeguards for workstations that access ePHI or relevant electronic information systems to comply with its written policies and procedures for workstation use.

Such physical safeguards must be modified in response to any modifications to the written policies and procedures for workstation use.

Provide role-based security awareness training on its Security Rule policies and procedure.

Technical Safeguards
Section C: Encryption and Decryption

Ensure that an encryption solution that it adopts meets prevailing cryptographic standards prior to using it.

Adding a requirement to assign a unique identifier for tracking each technology asset.

Deploy updated encryption solutions as prevailing cryptographic standards evolve, consistent with both of the proposed requirements discussed above: (1) to review, verify, and update its risk analysis in response to changes in its environment that may affect ePHI; and (2) to review and modify, as reasonable and appropriate, its risk management plan in response to changes in its risk analysis.

Encrypt all ePHI at rest and in transit, with limited exceptions.

Technical Safeguards
Section E: Audit Trail and System Log Controls

Deploy technology assets and/or technical controls that monitor in real-time (*i.e.,* contemporaneously) all activity occurring in a regulated entity's relevant electronic information systems and identify indications of unauthorized persons and unauthorized activity.

Deploy technology assets and/or technical controls that record in real-time all activity in the regulated entity's relevant electronic information systems.

Retain records of all activity in its relevant electronic information systems as determined by the regulated entity's policies and procedures for information system activity review.

Review and test controls every 12 months.

Technical Safeguards
Section G: Authentication

Deploy technical controls in accordance with its information access management policies and procedures, including technical controls that require users to adopt unique passwords. (i.e.) change default passwords).

Deploy MFA everywhere.

Deploy MFA for any action that would change a user's privileges to the regulated entity's relevant electronic information systems in a manner that would alter the user's ability to affect the confidentiality, integrity, or availability of ePHI.

Deploy MFA for changed privileges in both types of systems.

Technical Safeguards
Section I: Vulnerability Management

Conduct automated scans of the regulated entity's relevant electronic information systems.

Review and test the effectiveness of the technology asset(s) that conducts the automated vulnerability scans every 12 months.

Monitor authoritative sources for known vulnerabilities on an ongoing basis and take action to remediate identified vulnerabilities in accordance with the regulated entity's patch management program.

Conduct periodic testing of the regulated entity's relevant electronic information systems for vulnerabilities, commonly referred to as penetration testing. Penetration tests identify vulnerabilities in the security features of an application, system, or network by mimicking real-world attacks. Would be tested by qualified person.

Technical Safeguards
Section J: Data Backup and Recovery

Create copies of ePHI in a manner that ensures that such copies are no more than 48 hours older than the ePHI maintained in the regulated entity's relevant electronic information systems.

Deploy technical controls that, in real-time, monitor, and alert workforce members about, any failures and error conditions of the backups required by the first implementation specification.

Deploy technical controls that record the success, failure, and any error conditions of backups required.

Test it at least monthly.

Technical Safeguards
Section K: Information Systems Backup and Recovery

Technical controls to create and maintain backups of relevant electronic information systems.

Review and test the effectiveness of such technical controls at least once every six months or in response to environmental or operational changes, whichever is more frequent.

MassCyberCenter Team

John Petrozzelli
Director
Petrozzelli@masstech.org

Meg Speranza
Resiliency Program Manager
Speranza@masstech.org

Max Fathy
Senior Program Manager,
Cybersecurity Innovation
Fathy@masstech.org

Nick Butts
Outreach Program Manager
Butts@masstech.org

Questions?

Visit our website to connect with us and learn more:

MassCyberCenter.org

MassCyberCenter
at MassTech