HIPAA Security Rule Proposed Rule

Dan Steinberg, JD, CIPP/G, CIPM
Senior Cybersecurity Engineer

February 2025

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

General Assumptions

- **History:**
  - We all know it
  - Assume familiar with the history of the HIPAA Security Rule; it's status as a regulation and not a statute; that separate rules address privacy and security; penalties, etc.
  - Standards vs. implementation specifications ("steps or elements")
  - "Required" versus "addressable"
  - Updates 2008 (GINA), 2009 (HITECH), and 2013
- **Why the Update?**
  - Significant changes in technology
  - Changes in breach trends and cyberattacks
  - HHS Office for Civil Rights' (OCR's) enforcement experience
  - Other guidelines, best practices, methodologies, procedures, and processes for protecting ePHI
  - Court decisions that affect enforcement of the Security Rule
- **NPRM**
  - Understand that this is a proposed rule; there is the Final Rule and then the effective date of the Final Rule
  - Start thinking about compliance early:
    - Prediction of what will survive the comment period
    - What will survive other challenges
    - Worth considering how much the standard of care has shifted

Notice of Proposed Rulemaking (NPRM)

- **Published January 6, 2025**
  - Available at 90 Fed Reg 898
  - HHS Fact Sheet available
  - Comment period through March 7, 2025
- **Past Dates**
  - HIPAA enacted August 1996
  - First proposed Privacy Rule November 1999; Final August 2002 (2 years, 10 months)
  - First proposed Security Rule August 1998; Final February 2003 (4 years, 7 months)
  - Whenever the final is published—180 days to compliance/longer to amend Business Associate Agreements
- **Loper challenges are possible**
  - Removal of “Chevron deference”
  - HIPAA Rules are created pursuant to explicit authority in the HIPAA statute
  - Possible to claim executive overreach

Most changes have precedent in the existing Rule…

Requirement	A, T, P	Precedent in the Existing HIPAA Security Rule
Remove the “required vs. addressable” framework	A	45 CFR § 164.306(d): Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity’s electronic protected health information
Document “policies, procedures, plans, and analyses”	A	45 CFR § 164.312 Policies and procedures and documentation requirements
Align with updated definitions	A,T,P	45 CFR § 160.103 Definitions; 45 CFR § 160.304 Definitions
Align with updated compliance time periods	A	45 CFR § 164.318 Compliance dates for the initial implementation of the security standards
Conduct a technology asset inventory	P	45 CFR § 164.308(a)(1) Security Management Process; 45 CFR § 164.308(a)(1)(ii)(A) Risk analysis
Report changes of access to individuals	A	45 CFR § 164.308(a)(3)(ii)(C) Termination procedures
Update and align contingency planning	T	45 CFR § 164.308(a)(7) Contingency Plan
Conduct compliance audit/*evaluation*	A,T,P	45 CFR § 164.308(a)(8) Evaluation
Require business associates to report on compliance	A	45 CFR § 164.308(b)(1) Business Associate Contracts and Other Arrangement
Encrypt PII at rest and in transit	T	45 CFR § 164.312(a)(2)(iv) Access Control: Encryption and Decryption; 45 CFR § 164.312(e)(2)(ii) Transmission Security: Encryption
Establish and *deploy* technical controls	T	45 CFR § 164.306(A)(1): ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits
Deploy multi-factor authentication	T	[Consistent with General Requirements]
Conduct vulnerability scanning	A,T,P	45 CFR § 164.312(b) Audit controls
Segment networks	A,T,P	[Consistent with General Requirements]
Update backup and recovery processes	A,T,P	45 CFR § 164.310(d)(2)(iv) Data Backup and Storage
Test certain controls annually	A,T,P	45 CFR § 164.306(e) Maintenance
Require business associates to report implementation of contingency plans	A	45 CFR 164.314 (a)(2)(i)(C) Report to the covered entity any security incident of which it becomes aware
Group health plans: Parallel requirements for group health plan sponsors	A	[Consistent with General Requirements]

Changes to Definitions

- “Deploy” and “Implement”
- “Relevant” electronic information system
- “Facility” versus “Building”
- “Access” and “Authentication” – of both individuals and assets
- Vulnerability x Threat = Risk

“Asset Inventory” and “Network Map”

- **Asset inventory**
  - Conduct and maintain an accurate and thorough written technology asset inventory
  - Foundation for a fulsome and accurate risk analysis
  - Identify information systems that create, receive, maintain, or transmit ePHI and all technology assets
- **Network map**
  - “Determine the movement of ePHI through, into, and out of” information systems”
  - Describe such movement in a network map

The end of “Addressable” Implementation Specifications?

- **HIPAA Security Rule 68 FR 8377 (2003): 45 CFR § 164.306(d): For addressable implementation specifications, a covered entity must:**
  - (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity’s [ePHI]; and
  - (ii) As applicable to the entity—
    - (A) Implement the implementation specification if reasonable and appropriate; or
    - (B) If [not:]
      - (1) Document why it would not be reasonable and appropriate [...]; and
      - (2) Implement an equivalent alternative measure if reasonable and appropriate.
- **NPRM 45 CFR § 164.306(b): *Flexibility of approach.***
  - (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
  - (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
    - (i) The size, complexity, and capabilities of the covered entity or business associate.
    - (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
    - (iii) The costs of security measures.
    - ***(iv) The probability and criticality of potential risks to electronic protected health information.***

MITRE

Evaluation

- **NPRM 45 CFR 164.308(a)(3)(i)**
- **Evaluation previously referred to an initial or *periodic review and assessment of controls***
- **An evaluation as now required "looks at a specific change that a regulated entity intends to make before the change is made."**
- **Relevant changes may include:**
  - Adoption of new technology assets
  - Upgrading, updating, or patching of technology assets
  - Newly recognized threats to the confidentiality, integrity, or availability of ePHI
  - A sale, transfer, merger or consolidation of all or part of the regulated entity with another person
  - A security incident that affects the confidentiality, integrity, or availability of ePHI
  - Relevant changes in Federal, State, Tribal, and territorial law.

Multi-Factor Authentication

- **Two out of three factors:**
  - Information known by the user, including but not limited to a password or personal identification number (PIN).
  - Item possessed by the user, including but not limited to a token or a smart identification card.
  - Personal characteristic of the user, including but not limited to fingerprint, facial recognition, gait, typing cadence, or other biometric or behavioral characteristics.
- ***"Something you know, something you have, or something you are."***

Encryption at Rest and in Transit

- **This is a clarification of an existing requirement:**
  - Access Control: Encryption and Decryption 164.312(a)(2)(iv) (addressable)
  - Transmission Security: Encryption 164.312(e)(2)(ii) (addressable)
- **"…while in 2003 and even in 2013, encryption might have been out of reach for many regulated entities because of cost or a similar reason, today, encryption solutions are generally considered to be widely accessible.**
- **45 CFR Sec 164.312(B) Standard: Encryption and decryption.**
  - (1) General. Deploy technical controls to encrypt and decrypt [ePHI] using encryption that meets prevailing cryptographic standards.
  - (2) Implementation specification. Encrypt all electronic protected health information at rest and in transit, except to the extent that an exception at paragraph (b)(3) of this section applies.
  - (3) [Exceptions]

Other Interesting Changes

- **Review and Testing of Controls Every Twelve Months**

• **Risk Analysis**	• **Patch Management**	• **Sanctions**
• **Workforce Security**	• **Security Incident Response**	• **Contingency Plans**

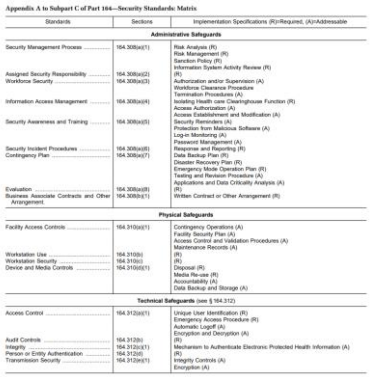
- **Patch Management**
- **Report changes to individuals' access**
- **Business Associate requirements**
  - Annual reporting on compliance
  - Reporting on implementation of contingency plans
- **Network segmentation**

Will the new HIPAA Security Rule be simpler?

“City Lights,” 1931
(dir., C. Chaplin)

“The Fellowship of the Ring,” 2001
(dir., P. Jackson)

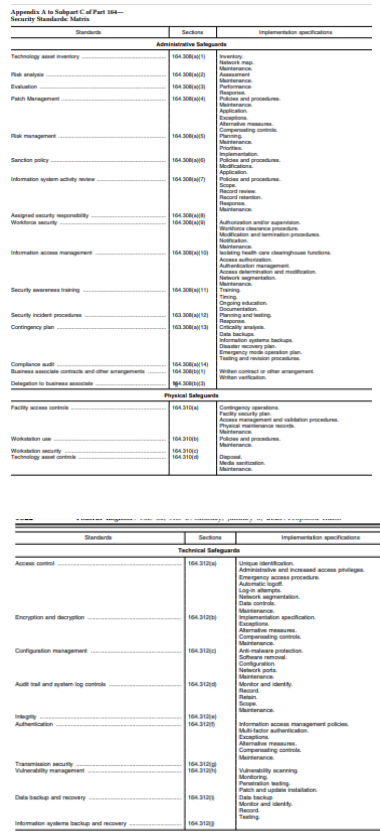
HIPAA Security Rule (Final)
68 Fed. Reg. 8380 (2/20/2003)



Appendix A to Subpart C of Part 164—Security Standards: Matrix

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

HIPAA Security Rule (NPRM)
90 Fed. Reg. 1022 (1/6/2025)



Appendix A to Subpart C of Part 164—
Security Standards: Matrix

Standards	Sections	Implementation specifications
Administrative Safeguards		
Technology asset inventory	164.308(a)(1)	Inventory. Network map. Maintenance.
Risk analysis	164.308(a)(2)	Assessment. Maintenance.
Evaluation	164.308(a)(3)	Performance. Response.
Patch Management	164.308(a)(4)	Policies and procedures. Maintenance. Application. Exceptions. Alternative measures. Compensating controls.
Risk management	164.308(a)(5)	Planning. Maintenance. Priorities. Implementation.
Sanction policy	164.308(a)(6)	Policies and procedures. Modifications. Application.
Information system activity review	164.308(a)(7)	Policies and procedures. Scope. Record review. Record retention. Response. Maintenance.
Assigned security responsibility	164.308(a)(8)	
Workforce security	164.308(a)(9)	Authorization and/or supervision. Workforce clearance procedure. Modification and termination procedures. Notification. Maintenance.
Information access management	164.308(a)(10)	Isolating health care clearinghouse functions. Access authorization. Authorization management. Access determination and modification. Network segmentation. Maintenance.
Security awareness training	164.308(a)(11)	Training. Timing. Ongoing education. Documentation.
Security incident procedures	163.308(a)(12)	Response and reporting. Response.
Contingency plan	163.308(a)(13)	Criticality analysis. Data backups. Information systems backups. Disaster recovery plan. Emergency mode operation plan. Testing and revision procedures.
Compliance audit	164.308(a)(14)	
Business associate contracts and other arrangements	164.308(b)(1)	Written contract or other arrangement. Written verification.
Delegation to business associate	164.308(b)(3)	
Physical Safeguards		
Facility access controls	164.310(a)	Contingency operations. Facility security plan. Access management and validation procedures. Physical maintenance records. Maintenance.
Workstation use	164.310(b)	Policies and procedures. Maintenance.
Workstation security	164.310(c)	
Technology asset controls	164.310(d)	Disposal. Media sanitization. Maintenance.

Standards	Sections	Implementation specifications
Technical Safeguards		
Access control	164.312(a)	Unique identification. Administrative and increased access privileges. Emergency access procedure. Automatic logoff. Log-in attempts. Network segmentation. Data controls. Maintenance.
Encryption and decryption	164.312(b)	Implementation specification. Exceptions. Alternative measures. Compensating controls. Maintenance.
Configuration management	164.312(c)	Anti-malware protection. Software removal. Configuration. Network ports. Maintenance.
Audit trail and system log controls	164.312(d)	Monitor and identify. Record. Retain. Scope. Maintenance.
Integrity	164.312(e)	
Authentication	164.312(f)	Information access management policies. Multi-factor authentication. Exceptions. Alternative measures. Compensating controls. Maintenance.
Transmission security	164.312(g)	
Vulnerability management	164.312(h)	Vulnerability scanning. Frequency. Penetration testing. Patch and update installation.
Data backup and recovery	164.312(i)	Data backup. Monitor and identify. Record. Testing.
Information systems backup and recovery	164.312(j)	

To Submit Comments:

- **Federal eRulemaking Portal at https://www.regulations.gov**
- **Search for Docket ID HHS–OCR–0945–AA22**
- **Instructions at https://www.regulations.gov**
- **Attachments should be in Microsoft Word or PDF**

Questions?

Effects (per the HHS Fact Sheet) (1 of 4)

- Remove the distinction between “required” and “addressable” implementation specifications and make all implementation specifications required with specific, limited exceptions.
- Require written documentation of all Security Rule policies, procedures, plans, and analyses.
- Update definitions and revise implementation specifications to reflect changes in technology and terminology.
- Add specific compliance time periods for many existing requirements.
- 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, but at least once every 12 months and in response to a change in the regulated entity’s environment or operations that may affect ePHI.

Effects (per the HHS Fact Sheet) (2 of 4)

- Require greater specificity for conducting a risk analysis. New express requirements would include a written assessment that contains, among other things:
  - 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
  - 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.
- Require notification of certain regulated entities within 24 hours when a workforce member's access to ePHI or certain electronic information systems is changed or terminated.
- Strengthen requirements for planning for contingencies and responding to security incidents. Specifically, regulated entities would be required to, for example:
  - 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.
  - Implement written procedures for testing and revising written security incident response plans.

Effects (per the HHS Fact Sheet) (3 of 4)

- Require regulated entities to conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.
- Require that business associates verify at least once every 12 months for covered entities (and that business associate contractors verify at least once every 12 months for business associates) 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.
- Require encryption of ePHI at rest and in transit, with limited exceptions.
- Require regulated entities to 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.
  - Disabling network ports in accordance with the regulated entity's risk analysis.

Effects (per the HHS Fact Sheet) (4 of 4)

- Require the use of multi-factor authentication, with limited exceptions.
- Require vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Require network segmentation.
- Require separate technical controls for backup and recovery of ePHI and relevant electronic information systems.
- Require regulated entities to review and test the effectiveness of certain security measures at least once every 12 months, in place of the current general requirement to maintain security measures.
- 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.
- Require group health plans to include in their plan documents requirements for their group health plan sponsors to: comply with the administrative, physical, and technical safeguards of the Security Rule; ensure that any agent to whom they provide ePHI agrees to implement the administrative, physical, and technical safeguards of the Security Rule; and notify their group health plans upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.