PROGRAM MATERIALS
Program #35140
July 22, 2025

The 2025 Proposed HIPAA Security Rule: Steps to Prepare

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

The 2025 Proposed HIPAA Security Rule: Steps to Prepare

Adam Laughton

JULY 4, 2025

I. Background

GT GreenbergTraurig

Background

- Health Insurance Portability and Accountability Act (HIPAA) (not Health Information Privacy and _____ Act) passed in 1996
  - Not primarily about health information, privacy or security
- HIPAA Security Rule proposed in 1998; Final Rule published in 2003; implementation date in 2005
- Enforcement Rule promulgated in 2006 (applies to both Security and Privacy Rules)
- Omnibus HIPAA Final Rule in 2013

GT GreenbergTraurig

Proposed Rule

- Issued in December 2024 (Biden)
- Comments due by March 7, 2025
  - Over 4,000 received
- Prospects for changes and finalization?

GT GreenbergTraurig

Why now?

- Dependence of healthcare system on technology
- Threats to PHI and data
- Pandemic experience with telehealth
- Avoid patchwork of state laws
- New technologies (AI)
- Lack of investment

GT GreenbergTraurig

Structure of existing rules

- Administrative vs. physical vs. technical
- Standards vs. implementation specifications

II. Major Changes

GT GreenbergTraurig

“Required” vs. “Addressable”

- What does “addressable” mean?
- Proposal does not mean that everything is required.
- Standard shifts from “what organization believes is reasonable and appropriate” to “required to implement standards and implementation specifications and must adopt reasonable and appropriate security measures”
  - Not whether or not to do it, but flexibility still in how to achieve compliance

GT GreenbergTraurig

Updated Definitions

- Examples
  - “Access”
  - “Risk”
  - “Physical Safeguards”
  - “Technical Controls”/”Technical Safeguards”

GT GreenbergTraurig

Business Associate Changes

- Documented certification for technical safeguards only
- Report to covered entities regarding contingency plan

GT GreenbergTraurig

Updates to Technology

- Not a separate rule (yet…)
- Request for further information

III. Risk Analysis

GT GreenbergTraurig

New risk assessment/risk analysis requirements

- Many covered entities get penalized for lack of risk assessment
- Used to play into the required/addressable distinction

GT GreenbergTraurig

Elements

- Technology asset inventory and network map (hardware and software) (“foundation for a fulsome and accurate risk analysis”)
- Identification of all ePHI that travels through the system (including external sources and recipients)
- “Reasonably anticipated” threats to ePHI (can be human, natural or environmental)
- Potential vulnerabilities
- Assess risk level of each threat and vulnerability
- Documentation

IV. Contingencies and Incidents

GT GreenbergTraurig

Contingency Plans

- Big theme of Proposed Rule
- 72 hour restoration is the standard
- Written procedures, assessment of "criticality"/prioritization as part of risk assessment
- Incident response plan and procedure
  - Addresses workforce members
- Testing

V. Compliance Audits

GT GreenbergTraurig

New requirement

- Annual compliance audit
- Conducted by who? (not specified)
- Existing published guidance
- Additional requirement (separate section) to test security measures against intrusion (once every 12 months)

VI. Other Changes

GT GreenbergTraurig

Encryption

- Formerly an “addressable” implementation specification
- All ePHI at rest and in transit
- Exceptions
  - Technology asset that does not support encryption
  - Access by individuals (i.e. patients)
  - Marketing-authorized FDA-approved medical devices
  - Circumstances where encryption is infeasible (emergency)

GT GreenbergTraurig

Multi-factor authentication

- Now required in lieu of “default passwords”
- Required for any action that would change a user’s privileges and affect their access to ePHI
- Exceptions require an alternative

GT GreenbergTraurig

Adam Laughton

(713) 374-3611

Adam.Laughton@gtlaw.com