# HIPAA Security Rule: Today vs. the Proposed Update



| | TODAY<br>Current HIPAA Security Rule | PROPOSED UPDATE<br>Proposed requirements (NPRM) |
|---|---|---|
| **RISK ASSESSMENT** | Conduct an accurate and thorough assessment of risks and vulnerabilities to ePHI. | More detailed, documented risk analysis and risk management requirements. |
| **ENCRYPTION** | Encryption is an addressable implementation specification. | Require encryption of ePHI at rest and in transit, subject to limited exceptions. |
| **ACCESS SECURITY** | Implement access controls to restrict access to ePHI to authorized users and appropriate roles. | Require multi-factor authentication (MFA), subject to limited exceptions. |
| **SECURITY TESTING** | Perform periodic technical and nontechnical evaluations of security measures. | Conduct vulnerability scans at least every six months and penetration tests at least annually. |
| **INCIDENT RECOVERY** | Maintain contingency plans, including data backup and disaster recovery procedures. | Establish more detailed written contingency procedures, including proposed 72-hour restoration requirements. |
| **ASSET INVENTORY & NETWORK MAPPING** | Address risks to ePHI through existing risk analysis and security safeguards. | Maintain technology asset inventories and network maps, with annual and change-driven reviews. |

**REGULATORY NOTE**

The proposed update is not the current enforceable rule. Existing HIPAA Security Rule requirements remain in effect while rulemaking proceeds.

www.ampcuscyber.com | letsconnect@ampcuscyber.com