SMITH ANDERSON

Navigating Cybersecurity: Compliance Considerations for Primary Care Providers

Presented by: John Gibson

June 6, 2025

EXPECT EXCELLENCE®

Disclaimer

This presentation is informational only and does not constitute legal or professional advice.

Agenda

- Cybersecurity threats
- Cyber insurance considerations
- HIPAA Security Rule and proposed changes
- Q&A

Worrisome Cybersecurity Trends

- Between 2018 and 2023, breaches of unsecured PHI reported to HHS increased by 100%.
- Significant escalation in hacking (260% increase) and ransomware (264%) cases.
- FBI Crime Complaint Center reports more ransomware attacks in healthcare and public health sector than any other industry
- Why are healthcare organizations targeted?

Source: 2024-30983 (90 Federal Register 898)

Types of Cyber Threats

- Phishing
- Ransomware
- Cloud vulnerabilities
- Vendor data breaches

Cyber Insurance Best Practices

- HIPAA coverage
  - Response, notification costs; regulatory fines and penalties
- Ransom costs
- Involve your counsel and advisors
- Third party vendor acts and breaches

Cyber Insurance continued

- Liability limits
- Retroactive coverage
- Incident response procedure (consent for mitigation costs)
- Defense costs

HIPAA Security Rule Generally

- Establishes standards to protect ePHI and requires appropriate safeguards to ensure confidentiality, integrity, and security of ePHI.
- Protect against reasonably anticipated threats to ePHI
- Ensures compliance of workforce
- Business associate requirements
- History of flexibility based on capabilities of covered entity

HHS Proposed Rule

- Designed to modify Security Rule by strengthening cybersecurity protections
- Every stage of healthcare delivery system reliant on secure network technologies
- Upward trend in cyberattacks
- Small, rural providers are often less likely to have invested in cybersecurity infrastructure, making them easier targets

Definition Updates

Deploy and Implementation:

- Updated definitions to require protections be in place throughout organization, not just certain technologies (e.g., laptops or servers)
- Safeguards should be configured and operational, not just addressed in policies

Multi-Factor Authentication (2 out of 3):

- Information known to user (password, PIN)
- Item possessed by user (e.g., smart ID card)
- Personal characteristic of user (e.g., fingerprint, facial recognition)

Security Standards

- Removal of distinction between “required” and “addressable.”
- Covered entities have flexibility in how they meet standards and implementation specifics, but not whether they meet them at all.
- Importance of considering effectiveness of security measure.
- Flexibility remains, but standards must meet floor of protection required under the Security Rule.

Administrative Safeguards

- Proposed rule seeks to address ineffective security maintenance procedures.
- Requirement to review and test security measures on ongoing basis to ensure they work and that workforce members know how to implement them.
- Requirement to maintain written technology asset inventory and network map
  - Examples of technology assets: hardware, software, electronic media, information, and data
  - Flow of ePHI through information systems
  - Accounting of assets and accountable person
  - Required to be reviewed and updated (a) on an ongoing basis, but at least every 12 months and (b) when there is a change in operations that impacts ePHI.

Risk Analysis

- Proposed Rule outlines eight minimum risk analysis standards, to be reviewed at least every 12 months:
  - Review technology asset inventory and network map
  - Identify reasonably anticipated threats to confidentiality/integrity of ePHI
  - Identify potential vulnerabilities to information systems
  - Create assessment/documentation of security measures
  - Make reasonable determination of likelihood of threat of vulnerabilities
  - Make reasonable determination of potential impact of threats
  - Create assessment of risk level of each threat
  - Create assessment of risks for each BAA or other contract

Vulnerability Management, Patch Management, and Risk Management Plan

- Requirement to deploy technical controls to identify and address vulnerabilities in information systems (e.g., automated scans)
- Requirement to review patch management processes at least once every 12 months
- Risk management plan tailored to entity's specific circumstances to address risks to ePHI, including risks identified in risk analysis
  - Also required to be reviewed every 12 months and in response to changes in risk analysis

Workforce Topics

- Requirement to establish sanction policies related to security policies and procedures
- Notification requirements to other regulated entities of a change in or termination of a workforce member's authorization to access ePHI when the ePHI is maintained by the other entity and the workforce member was authorized to access by the reporting entity.
- Security workforce training at least every 12 months, but also periodic training such as test phishing/scam emails.

Contingency/Security Incident Plans

- Procedures to restore information systems and data within 72 hours of incident
- Analysis of criticality of systems and prioritize restoration of technology assets and information systems
- Procedure for how workforce members report security incidents
- Procedure for updating incident response plans
- Requirement to review and test response plans at least every 12 months and document results

Safeguards

- Implement workstation protections
- Require encryption of ePHI at rest and in transit
- Require network segmentation
- Require vulnerability scanning at least every six month and penetration testing at least once every 12 months
- Require separate technical controls for backup and recovery of PHI and relevant electronic information systems
- Deploy anti-malware protection
- Remove extraneous software
- Disable ports in accordance with risk analysis

Business Associate (BA) Considerations

- Requirement to verify BA has deployed technical safeguards (obtain written verification)
- Verification to include written analysis of BA's electronic information systems
- Business Associate Agreements would be required to include provision that BA must report activation of contingency plan no later than 24 hours

Questions?

John Gibson

Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.
Wells Fargo Capitol Center
150 Fayetteville Street, Suite 2300
Raleigh, North Carolina 27602-2611
(919) 821-1220
jgibson@smithlaw.com