

The background of the entire page is a dark blue, textured surface with a grid of small dots. Overlaid on this is a futuristic digital interface. A hand is shown pointing at a large, glowing hexagon in the center. This hexagon contains the word "HIPAA" in a bold, white, sans-serif font. Surrounding this central hexagon are several other smaller, glowing hexagons, each containing a different icon: a padlock, a dollar sign inside a padlock, a person silhouette, and a group of three people silhouettes. Arrows and lines connect these hexagons, suggesting a flow or relationship between the concepts. The overall aesthetic is high-tech and digital.

HIPAA



Your Guide to Proposed Changes to the HIPAA Security Rule

Overview

On December 27, 2024, the Office for Civil Rights (OCR) issued a Notice of Proposed Rulemaking (NPRM) aimed at strengthening cybersecurity protections for electronic protected health information (ePHI). These changes will have significant implications for healthcare organizations, requiring enhanced security measures and stricter compliance protocols.

Key Details About the NPRM



Public Comment Period

Open until March 7, 2025. OCR may make modifications based on public feedback.



Effective Date

The final rule would take effect 60 days after publication, followed by a 180-day compliance period.



Transition Period

Additional time is proposed for updating Business Associate Agreements (BAAs) to align with new requirements.



Uncertainty in Timeline

Possible administrative changes could influence the implementation schedule and direction of updates.



Significant Proposals in the NPRM

1. Compliance Requirements for All Standards
 - » The NPRM proposes eliminating the "Required" and "Addressable" designations, making all standards mandatory.
2. Technology Asset Inventory and Network Mapping
 - » Maintain a detailed inventory of all technology assets.
 - » Develop a network map illustrating ePHI movement, updated annually.
3. Risk Analysis Enhancements
 - » Review asset inventory and network maps.
 - » Identify threats and vulnerabilities to ePHI.
 - » Assess the likelihood and impact of potential threats.
4. Contingency Planning and Incident Response
 - » Establish written procedures for restoring data within 72 hours.
 - » Prioritize data recovery based on system criticality.
5. Compliance Audits
 - » Conduct internal audits of Security Rule compliance on an annual basis.
6. Reviews and Tests of Security Measures
 - » Review and test security measures annually to ensure effectiveness.
7. Vulnerability Scans and Penetration Tests
 - » Perform vulnerability scans at least every six months.
 - » Conduct penetration testing annually to identify security gaps.
8. Encryption Requirements
 - » Mandatory encryption of all ePHI at rest and in transit.
9. Multi-Factor Authentication (MFA)
 - » Implement MFA for all systems containing ePHI.
10. Network Segmentation and Anti-Malware Protection
 - » Protect sensitive data with network segmentation and anti-malware solutions.

11. Portable Device Controls

- » Extend security measures to mobile devices, tablets, and other portable devices that access ePHI.

12. Patch Management

- » Implement timely patching and updates to mitigate security vulnerabilities.

13. Removal of Unnecessary Software and Ports

- » Identify and remove extraneous software.
- » Disable unused network ports based on risk analysis findings.

14. Data Backup and Recovery

- » Implement distinct technical controls for ePHI storage and system recovery.

15. Business Associate Cybersecurity

- » Annually verify that business associates and contractors adhere to cybersecurity standards.

Additional Resources

OCR Fact Sheet on Proposed Changes: [OCR HIPAA Security Rule NPRM Fact Sheet](#)

Full NPRM Text on Federal Register: [HIPAA Security Rule NPRM](#)



Get Compliant with Fortified Health Security

Ensuring compliance with these proposed changes can be complex. [Fortified Health Security](#) offers expertise in navigating these healthcare cybersecurity updates and helping organizations meet compliance requirements effectively.

For guidance and support, consult with cybersecurity specialists like Fortified Health Security to streamline the compliance process and safeguard your organization.

[Contact Fortified Health Security](#)