Are you Prepared for Changes to the HIPAA Safeguards Rule?

The Department of Health and Human Services (HHS) recently announced significant proposed updates to the HIPAA Security Rule aimed at bolstering protections for electronic protected health information (ePHI). These changes reflect the evolving cybersecurity landscape and heightened threats to the healthcare sector.

LEGION
cyberworks

legioncyber.com

Key Insights into the Proposed HIPAA Cybersecurity Changes

The comment period for the proposed rule ends March 7th, 2025, and if enacted, healthcare organizations would have 180 days from the effective date to be in compliance. Organizations must act now to assess their readiness and plan for compliance as they may need to be in compliance by the end of 2025.

Recent healthcare data breaches and cyber-attacks caused significant damage to healthcare organizations in 2024, underscoring the need for more robust security measures within the healthcare industry.

Major Healthcare Data Breaches in 2024

Change Healthcare (February 2024)

Incident: Change Healthcare, part of UnitedHealth Group, was targeted by the BlackCat (ALPHV) ransomware group.

Impact: The breach exposed personal data of over 100 million individuals, including health insurance details, medical records, and Social Security numbers.

Cause: Stolen credentials used for a Citrix remote access service without multi-factor authentication.

Outcome: UnitedHealth Group paid a $22 million ransom to recover data.

Ascension Health (May 2024)

Incident: Ascension Health, a major healthcare provider, suffered a ransomware attack leading to operational disruptions.

Impact: Approximately 5.6 million patients were affected, with significant delays in medical services and financial losses of $1.1 billion for the fiscal year.

Kaiser Foundation Health Plan (April 2024)

Incident: Inadvertent exposure of sensitive data through embedded tracking codes on the website and mobile app.

Impact: 13.4 million individuals had their protected health information (PHI) shared with third parties, violating HIPAA.

Data Exposed: Names, IP addresses, activity data, and health-related search terms.

Action Taken: Tracking codes were removed to prevent further breaches.

Managed Care of North America (March 2024)

Incident: The ransomware group LockBit attacked MCNA Dental, the largest dental insurer in the U.S.

Impact: Data of 8.9 million patients was stolen, including names, insurance details, Social Security numbers, and treatment information.

Outcome: The stolen data was leaked on the dark web after MCNA Dental refused to pay the ransom.

LEGION cyberworks

What You Need to Know

Uniform Standards

All implementation specifications under the Security Rule are becoming mandatory, with limited exceptions.

Encryption Requirements

All ePHI at rest and in transit must be encrypted.

Proactive Security Testing

Vulnerability scans and penetration tests will become regular, mandatory activities.

Mandatory Multi-Factor Authentication (MFA)

Required layer of protection for access to systems housing ePHI.

Advanced Risk Analysis

Comprehensive assessments must identify threats, vulnerabilities, and their potential impact.

Resilient Recovery Plans

Organizations will need documented plans to restore systems and data within 72 hours following disruptions.

Overview of Proposed Updates to the HIPAA Security Rule

Uniform Implementation Specifications

All Security Rule implementation specifications will become mandatory, with limited exceptions.

Updated Definitions and Terminology

Aligns terminology and requirements with current technology advancements.

Technology Asset Inventory and Network Mapping

Entities must develop and annually update an inventory and network map to track ePHI movement within systems.

Mandatory Security Measures

Multi-factor authentication (MFA) with limited exceptions. Encryption of all ePHI at rest and in transit. Regular vulnerability scans (at least every six months). Annual penetration tests to assess security controls.

Comprehensive Documentation

Entities must maintain written documentation of policies, procedures, plans, and analyses related to the Security Rule.

Defined Compliance Time-frames

Establishes specific periods for compliance with Security Rule requirements.

Enhanced Risk Analysis Requirements

Technology asset inventory and network mapping. Identification of threats and vulnerabilities. Likelihood and impact assessments for potential risks.

Contingency Planning Enhancements

A documented plan to restore systems and data within 72 hours is required. Disaster recovery plans must be tested and verified to satisfy compliance requirements.

Why These Changes Matter and Why Start Planning Now

The proposed updates address critical cybersecurity gaps and aim to safeguard sensitive healthcare information from emerging threats. Compliance will require a significant investment in planning, technology, and expertise.

1 **Shift in Cybersecurity Practices**

The proposed changes signal a shift toward more rigorous cybersecurity practices in healthcare.

2 **Comment Period Ending Soon**

The comment period ends March 7, 2025. The effective date of a final rule would be 60 days after publication.

3 **Early Preparation Benefits**

Early preparation can mitigate the risk of rushed implementation once the rules are finalized.

4 **Risk Mitigation**

By addressing gaps now, organizations can avoid future compliance risks and potential penalties.

How Legion Cyberworks Can Help

Our experienced Chief Information Security Officers (CISOs) and cybersecurity team are uniquely positioned to assist healthcare organizations in navigating these changes.

Here's how we can support you:

Compliance Strategy

Build a roadmap to ensure timely adherence to the new rules.

Gap Assessments

Evaluate your current security measures against the proposed requirements.

Risk Analysis and Management

Develop robust frameworks to identify and mitigate risks to ePHI.

Implementation Support

Assist in deploying technologies such as MFA, encryption, data backup, and vulnerability management solutions.

Policy Development

Create comprehensive documentation to meet enhanced standards.

Testing Services

Conduct penetration tests and vulnerability scans to identify weaknesses.

By partnering with Legion Cyberworks, you can achieve compliance and strengthen your security posture against advanced cyber-threats, thereby protecting your patients and your organization.

Let's Get Started Together!

Don't wait for the final rules to be enacted—take proactive steps now to safeguard your ePHI and meet future standards. There will only be 180 days to implement the required controls once the changes to the Safeguards Rule are effective, potentially by the end of the 2025 calendar year.

For more details and guidance, contact Legion Cyberworks today.

https://legioncyber.com | 919-769-2916 | sales@legioncyber.com