People. Trust. Results.
Since 1960

Proposed Update to the HIPAA Security Rule

The U.S. Department of Health and Human Services (HHS) has proposed significant updates to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, aiming to enhance the cybersecurity of electronic protected health information (ePHI). These proposed changes, expected to be implemented in 2025, introduce several mandatory implementation standards for covered entities and their business associates. Below outlines the main requirements proposed in this rule.

1. **Technology Asset Inventory and Network Mapping**
   Covered entities will be required to maintain a comprehensive inventory of all technology assets that handle ePHI. This includes creating detailed network maps to visualize the flow of ePHI within their systems. Such measures are designed to enhance visibility and control over ePHI, thereby reducing vulnerabilities.

2. **Enhanced Risk Assessment Protocols**
   The proposed rule mandates a thorough risk assessment process that identifies gaps and analyzes risks across eight specific categories. Entities must develop a final risk management plan based on this assessment to address identified vulnerabilities and implement appropriate security measures, with testing conducted at least annually and when new technology is adopted.

3. **Incident Response and Contingency Planning**
   Entities are required to establish incident response and contingency plans and procedures that ensure the restoration of critical systems and data within 72 hours following a disruption. This includes conducting an analysis to determine the priority of system restorations based on their criticality to operations. Revisions to the plans will be implemented in response to ongoing testing results.

4. **Business Associate Notification Requirements**
   Business associates must notify covered entities within 24 hours of any changes in or termination of a workforce member's electronic access to ePHI. This prompt notification aims to prevent unauthorized access and maintain the integrity of ePHI. Additionally, Business Associates must notify Covered Entities no later than 24 hours of activating their contingency plan.

5. **Annual Vendor Audits**
   Covered entities are obligated to conduct annual audits of their vendors, including downstream entities, to ensure compliance with the Security Rule. These audits must be performed by qualified cybersecurity professionals or similar experts to verify that appropriate security measures are in place.

6. **Data Encryption**
   The proposed updates require the encryption of ePHI both in transit and at rest. This measure ensures that ePHI remains secure during transmission and storage, protecting it from unauthorized access.

People. Trust. Results.
Since 1960

7. **Anti-Malware Measures**
   Entities must implement robust anti-malware solutions to detect and prevent malicious software from compromising ePHI. Regular updates and monitoring of these solutions are essential to maintain their effectiveness against evolving threats.

8. **Network Port Management**
   The proposed rule emphasizes the importance of disabling unnecessary network ports based on the entity's risk assessment. This practice minimizes potential entry points for unauthorized access and reduces the attack surface.

9. **Regular Vulnerability Scanning and Penetration Testing**
   Entities are required to conduct vulnerability scans every six months and perform penetration testing at least annually. These proactive assessments help identify and remediate security weaknesses before they can be exploited.

10. **Network Segmentation**
    Implementing network segmentation is mandated to isolate sensitive ePHI environments from other parts of the network. This strategy limits the spread of potential breaches and enhances overall security.

11. **Separate Technical Controls for Backup and Recovery**
    The proposed updates require the establishment of distinct technical controls for backup and recovery processes. This ensures that backup data is protected and can be reliably restored in the event of data loss or corruption.

These proposed updates reflect HHS' commitment to strengthening the cybersecurity posture of healthcare organizations in response to evolving threats. Entities are encouraged to review these proposals thoroughly and prepare for their implementation to ensure compliance and safeguard patient information, which will ensure your practice is compliant. APS has all of these requirements in place and will continue to stay in front of privacy and security requirements. If you have any questions, please contact your Practice Manager.