Proposed Updates to HIPAA Security Rule Would Require Entities to Adopt Enhanced Cybersecurity Measures

Insights
1.07.25

The HIPAA Security Rule may soon undergo a big overhaul that would better defend healthcare data from cybersecurity threats – and require much more from covered entities when it comes to establishing and maintaining defenses. The Department of Health and Human Services (HHS) just published a proposed rule yesterday aimed at securing the confidentiality and integrity of electronic protected health information (ePHI) in response to growing breaches and cyberattacks against healthcare organizations. HIPAA-regulated entities can now submit public comments in response until March 7. With a new administration about to take over in D.C., what can covered entities expect from a finalized rule? This Insight will provide a review of the most significant changes proposed and offer a suggested gameplan as we await finalization.

Why is This Update Needed?

HHS is proposing this update to the HIPAA Security Rule in response to the significant increase in cyberattacks in the healthcare sector.

- Modern healthcare operations heavily rely on interconnected digital tools for activities like appointment scheduling, telehealth services, patient records management, and claims processing.
- These advancements, while beneficial, also increase exposure to cyber risks.
- In recent years, the healthcare industry has witnessed a surge in cybersecurity threats and breaches, including hacking and ransomware attacks.
- HHS is proposing to enhance protections for ePHI by implementing robust cybersecurity requirements and addressing the increasing sophistication of cyberattacks.

The Proposed Rule also attempts to align the Security Rule with industry best practices such as the NIST Cybersecurity Framework and the EU's General Data Protection Regulations (GDPR).

Most Significant Changes in Proposed Rule

The Security Rule, first published in 2003 and only revised once previously in 2013, establishes standards to safeguard PHI. Here are the key changes that would be brought about by the proposed

changes, aimed at bringing standards up to date with technological trends in the healthcare industry.

- **Increase in Required Obligations**: The current Security Rule separates all requirements into two categories. There are "required" implementation specifications – which, as the name suggests, are mandatory – and those that are just "addressable," which are only required if reasonable and appropriate in certain circumstances. The proposal would eliminate the distinction and make all implementation specifications required.
- **Technology Asset Inventory and Network Map**: Regulated entities will need to create and maintain a written inventory of technology assets and a network map that tracks the movement of ePHI through its electronic systems. Organizations would need to review and update them at least annually or when changes occur.
- **Annual Risk Analyses**: While the current rule requires covered entities to conduct a risk analysis, the proposed rule calls for a much more detailed effort. Covered entities would need to develop a detailed written assessment that includes eight separate categories of detail, including identification of reasonably anticipated threats, potential vulnerabilities, and a determination of the risks to ePHI – including those posed by business associates.
- **Risk Management Plan**: Regulated entities must then implement a robust risk management plan addressing risks identified during analyses.
- **Incident and Disaster Response**: The proposed rule requires entities to engage in IT system activity monitoring and develop incident response plans to be tested and revised at least once every year. Further, covered entities would need to establish disaster recovery procedures to restore certain IT systems and data within 72 hours of a loss.
- **Restrict Terminated Employee Access**: Covered entities would also need to implement written policies and procedures that would more tightly control employees' access to data – including cutting off access when an employee is terminated.
- **Annual Compliance Audits**: Entities will need to conduct audits annually to ensure compliance with the Security Rule.
- **Annual Security Awareness Training**: On an annual basis, covered entities will also need to provide security awareness training to personnel with a role in managing or having access to the ePHI.
- **Business Associate Agreements**: The proposed rule requires covered entities to update any business associate agreements to require notification within 24 hours of activating contingency plans. Business associates must also provide annual written analyses and certifications of compliance with technical safeguards, conducted by knowledgeable cybersecurity professionals.
- **Miscellaneous Requirements**: In addition, the proposed rule would also require covered entities to:
    - Encrypt all ePHI (with only limited exceptions);

- Use anti-malware protection;
- Disable network ports in accordance with the regulated entity's risk analysis;
- Use multi-factor authentication;
- Conduct vulnerability scanning every six months and penetration testing annually;
- Implement network segmentation; and
- Maintain separate technical controls for backup and recovery of ePHI.

If you want further detail, HHS has released a high-level fact sheet summarizing major proposed changes to the proposed rule.

What's Next?

HIPAA-regulated entities should consider actively engaging in the rulemaking process by submitting comments by March 7.

- In particular, the proposal to eliminate the **distinction between "required" and "addressable" implementation specifications** could have a significant impact on certain covered entities that are not healthcare providers, and impacted entities should consider providing HHS with their opinions on this proposal.
- HHS is specifically seeking comments on how best to regulate **new and emerging technologies** such as artificial intelligence, quantum computing, and virtual/augmented reality. The proposed rule underscores the importance of thorough risk assessments for new technologies as it relates to the safeguarding of ePHI before adopting such technologies into their practice.

If interested, consider contacting your Fisher Phillips attorney or FP Advocacy to assist with any rulemaking comments.

Once the rule is finalized after the end of the public comment period, entities will have 180 days to comply with the revised Security Rule. However, given the advent of a new administration overseeing HHS while this rule is pending, it will be worthwhile monitoring whether the proposal will be revised, postponed, or otherwise scrapped by new leadership. Moreover, federal agencies often revise proposed rules in response to public comments, so there is a chance that substantive revisions could be made before finalization. We will monitor the situation and provide updates as warranted.

What Should Group Health Plans Do?

Given the extent of these proposed changes, covered entities, business associates, and HIPAA compliance professionals should familiarize themselves with the new rules and requirements. The proposed updates emphasize the importance of proactive risk management and compliance. Group health plans must be prepared to:

health plans must be prepared to:

- Implement advanced security measures to safeguard ePHI within their plan documents and ensure agent compliance;
- Monitor and address emerging cybersecurity threats.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's Privacy and Cyber Team, Healthcare Industry Group, or Employee Benefits and Tax Team. You can also rely on our Data Protection and Cybersecurity Team for guidance and support.

Related People

Lorie Maring
Partner
404.240.4225
Email

Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

Katie Reynolds
Associate
617.532.6945
Email

Service Focus

Privacy and Cyber

Employee Benefits and Tax

Data Protection and Cybersecurity

Industry Focus

Healthcare