SALUS GROUP

HHS Proposes Changes to HIPAA Security Rule to Strengthen Cybersecurity for Electronic PHI

On Dec. 27, 2024, the U.S. Department of Health and Human Services (HHS) released a proposed rule that would modify the HIPAA Security Rule to strengthen cybersecurity protections for electronic protected health information (ePHI). Although the changes are substantial, they are only in proposed form at this point. Employers with self-insured health plans and those with fully insured health plans that have access to ePHI should monitor developments and plan to improve safeguards for ePHI if the changes are finalized.

Background

The HIPAA Security Rule sets a national floor for the protection of individuals' ePHI by covered entities (health plans, health care clearinghouses and most health care providers) and their business associates (collectively, regulated entities). These standards require regulated entities to analyze the risks and vulnerabilities of the confidentiality, integrity and availability of their ePHI. The risk assessment process helps regulated entities implement reasonable and appropriate administrative, physical and technical safeguards to protect their ePHI.

Proposed Changes

Since the Security Rule was issued in 2003, the health care environment has changed significantly. Not only is protected health information increasingly maintained and transmitted electronically, but treatment is also increasingly provided electronically. According to HHS, the proposed rule would update the Security Rule's standards to better address ever-increasing cybersecurity threats in the health care sector. HHS' proposal to strengthen the Security Rule includes the following changes for regulated entities:

- Requires written documentation of all Security Rule policies, procedures, plans and analyses;
- Adds specific compliance time periods for many existing requirements;
- Requires the development and revision of a technology asset inventory and a network map that illustrates the movement of ePHI throughout the regulated entity's electronic information system(s) on an ongoing basis but at least once every 12 months and in response to a change in the regulated entity's environment or operations that may affect ePHI;
- Requires greater specificity for conducting a risk analysis, including a written assessment that includes specific information, such as a review of the technology asset inventory and network map;
- Requires notification of certain regulated entities within 24 hours when a workforce member's access to ePHI or certain electronic information systems is changed or terminated;
- Strengthens requirements for planning for contingencies and responding to security incidents;
- Requires a compliance audit at least once every 12 months to ensure regulated entities' compliance with the Security Rule;
- Requires that business associates verify at least once every 12 months for covered entities that they have deployed technical safeguards required by the Security Rule to protect ePHI through a written analysis of the business associate's relevant electronic information systems by a subject matter expert and a written certification that the analysis has been performed and is accurate;
- Requires encryption of ePHI at rest and in transit, with limited exceptions;
- Requires the establishment and deployment of technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner;
- Requires the use of multi-factor authentication, with limited exceptions;
- Requires vulnerability scanning at least every six months and penetration testing at least once every 12 months;
- Requires the review and testing of certain security measures at least once every 12 months, in place of the current general requirement to maintain security measures;
- Requires business associates to notify covered entities upon activation of their contingency plans without unreasonable delay but no later than 24 hours after activation; and

- Requires group health plans' documents to include requirements for their sponsors, including complying with the Security Rule's administrative, physical and technical safeguards, ensuring that any agent to whom they provide ePHI agrees to implement the Security Rule's safeguards and notifying their group health plans upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.

Effective Date

If the proposed changes are finalized, they would be effective 60 days after their publication. Regulated entities would be required to comply with the finalized changes within 180 days after the final rule's effective date. To reduce administrative burdens, the proposed rule would provide regulated entities with additional time to modify business associate agreements. These agreements would need to be revised by the earlier of the contract renewal date that falls after the final rule's compliance date or within one year of the rule's effective date. In the meantime, the Security Rule's current requirements remain in effect.

Provided by Salus Group

This Legal Update is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice. © 2025 Zywave, Inc. All rights reserved.
This information is not meant to be legal advice and is for consultative purposes only. Please contact Valerie Bruce Hovland, Salus Group's V.P. of Compliance at vbrucehovland@thesalusgroup.com if you need additional information.