THOMPSON HINE

# Privacy & Cybersecurity Update

**January 2025**

## HHS Proposes Significant Changes to the HIPAA Security Rule

On December 27, 2024, the U.S. Department of Health and Human Services (HHS) published a proposed rule to amend the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The proposed changes result from the alarming growth in the number of data breaches impacting healthcare entities, the overall number of individuals affected by such breaches, the rampant escalation of cyberattacks using hacking and ransomware, and the magnitude of potential harm from such incidents. The amendment requires HIPAA-covered entities (e.g., health plans, healthcare clearinghouses, and most healthcare providers) and their business associates to implement and maintain certain cybersecurity protections to protect and safeguard certain protected health information (PHI) from unauthorized or otherwise impermissible access, acquisition, use, or disclosure. While HHS is undertaking this rulemaking, the current Security Rule remains in effect.

### Major Changes

The current HIPAA Security Rule, originally published in 2003 and updated in 2013, is increasingly considered outdated by many security and privacy experts. Advances in cybersecurity technologies and the growing complexity of cyber threats have highlighted the need for a more modernized framework.

The proposed HIPAA Security Rule maintains much of the original structure, including the categories of administrative, physical, technical, and organizational controls. However, it offers significantly more detailed guidance on how these controls must be implemented.

Specifically, the OCR issued a Fact Sheet on its rulemaking proposal, and the Fact Sheet includes the following information describing the purpose and scope of its proposed changes to the HIPAA Security Rule:

- Eliminate the distinction between "required" and "addressable" implementation specifications, making all implementation specifications mandatory with narrowly defined exceptions.
- Require written documentation of all Security Rule policies, procedures, plans, and analyses.
- Update definitions and revise implementation specifications to reflect changes in technology and terminology.
- Add specific compliance timelines for many existing requirements.
- Mandate the development and regular updates of a technology asset inventory and network map, including a defined timeline for such revisions.
- Require greater specificity for conducting a risk analysis.
- Require 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.
- Strengthen requirements for planning for contingencies and responding to security incidents. Specifically, regulated entities would be required to, for example: (i) establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours, (ii) perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration, (iii) establish written security incident response plans and procedures documenting how workforce members are

to report suspected or known security incidents and how the regulated entity will respond to suspected or known security incidents, and (iv) implement written procedures for testing and revising written security incident response plans.

- Require regulated entities to conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.
- Require 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 study has been performed and is accurate.
- Require encryption of ePHI at rest and in transit, with limited exceptions.
- Require regulated entities to establish and deploy technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner, such as deploying anti-malware protection.
- Require the use of multi-factor authentication, with limited exceptions.
- Require vulnerability scanning at least every 6 months and penetration testing at least once every 12 months.
- Require network segmentation.
- Require separate technical controls for backup and recovery of ePHI and relevant electronic information systems.
- Require regulated entities to review and test the effectiveness of certain security measures at least once every 12 months, in place of the current general requirement to maintain security measures.
- Require business associates to notify covered entities (and subcontractors to notify business associates) upon activation of their contingency plans without unreasonable delay but no later than 24 hours after activation.

Furthermore, the proposed rule would also mandate that group health plans include provisions in their plan documents requiring health plan sponsors to comply with the Security Rule's administrative, physical, and technical safeguards. Additionally, sponsors must ensure that any agent receiving ePHI agrees to implement these safeguards. The sponsor must also notify their group health plans upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.

## Next Steps

The incoming Trump administration will ultimately decide whether to advance changes to the HIPAA Security Rule proposed under the Biden administration and has not formally clarified its position on the matter. While bipartisan support exists for strengthening cybersecurity protections in the healthcare sector, the proposed changes would entail substantial compliance costs and effort. Covered entities and business associates should closely monitor industry feedback on the proposal and any signals from the Trump administration regarding its approach to these proposed changes.

Amid persistent cybersecurity threats facing the healthcare sector, healthcare-related organizations must continually assess their cybersecurity controls, information security incident response plans, service provider and business associate contracts, and insurance policies to enhance their readiness to prevent and respond to cybersecurity incidents. Comments to the proposed rules are due by March 7, 2025.

## FOR MORE INFORMATION

For more information, please contact:

**Steven G. Stransky**
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
*Certified Information Privacy Professional/Government (CIPP/G) Certified Information Privacy Professional/United States (CIPP/US)*

**Cori R. Haper**
937.443.6856
Cori.Haper@ThompsonHine.com

**Stephen R. Penrod**
216.566.5656
Stephen.Penrod@ThompsonHine.com

**Thora Knight, Ph.D.**
212.908.3971
Thora.Knight@ThompsonHine.com