Articles + Publications | January 6, 2025

HIPAA Security Rule Revamp Is on the Horizon

WRITTEN BY

Brent T. Hoard | Emma E. Trivax

On January 6, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published significant proposed amendments (proposed rule) to the Security Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Key drivers for the proposed rule include the dramatic increase in cyberattacks, including ransomware, the rapid adoption of cloud computing, mobile devices, and other technologies, and inconsistent compliance with the existing Security Rule identified by the OCR's investigations.

The proposed rule introduces changes that will modernize the Security Rule, including certain technical aspects (*e.g.*, patching, encryption, multifactor authentication, penetration testing), as well as training and awareness regarding social engineering to help address and mitigate against common breach issues. However, the inventory, mapping, assessment, analysis, testing, audit, and verification requirements may be burdensome and challenging to achieve and maintain for entities that do not have the ability to draw on readily available resources. We also note that the OCR's cost estimates for these initiatives (Tables 6 and 7) could be significantly understated.

For example, the proposed rule would require regulated entities to:

- Maintain an accurate and thorough inventory of their technology assets and create a network map of their electronic information systems, which must be updated at least every 12 months.
- Conduct and document an annual audit of compliance with each standard and implementation specification of the Security Rule (in addition to the annual risk analysis).
- Conduct vulnerability scanning at least every six months and penetration testing at least every 12 months.
- Verify business associate/subcontractor technical safeguards at least every 12 months as part of the business associate agreement contracting process, including a written analysis of the business associate's information systems and certification by an authorized person at the business associate.
- Establish and implement a written contingency plan that includes procedures for data backups, disaster recovery, and emergency mode operations. Notably, disaster recovery plans must now set forth a procedure for restoring critical systems within 72 hours of a loss.

For organizations that have self-funded health benefit plans, note that the proposed rule will require Security Rule compliance by any plan sponsor that receives ePHI from a group health plan beyond summary health information

for premium bids or to modify, amend, or terminate the group health plan, enrollment/disenrollment information, or ePHI pursuant to an authorization.

The proposed rule includes a transition period to allow regulated entities time to comply with the new requirements. Entities will be expected to comply with the new requirements within 180 days of the effective date of the final rule. Entities will also have additional time to update their business associate agreements, which will be by the earlier of the contract renewal date or within one year of the final rule's effective date. Public comments on the proposed rule are due within 60 days of its publication in the Federal Register on January 6.

At this point, we suggest that stakeholders analyze how the potential changes may generally impact their organization and existing HIPAA programs, develop a plan for allocating resources to achieve and manage the potential ongoing compliance obligations, and closely monitor the progress of, and any changes to, the proposed rule.

The Troutman Pepper Locke team is ready to assist with your HIPAA, privacy, cybersecurity, and compliance needs. We will keep you up to date on any updates surrounding the proposed rule. Please contact Brent Hoard at brent.hoard@troutman.com or Emma Trivax at emma.trivax@troutman.com for more information or if you are interested in submitting a public comment to the proposed rule.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Health Care + Life Sciences
- Health Care Regulatory
- Privacy + Cyber