

TYPES NOT MAPPED YET January 10, 2025 | TTR not mapped yet | Milada R. Goturi, Dani Elks

OCR Proposes Significant Changes to HIPAA Security Rule

On January 6, 2025, the Office of Civil Rights for the Department for Health and Human Services (“OCR”) published a notice of proposed rulemaking announcing significant changes to the HIPAA Security Rule (“Proposed Rule”) in an effort to strengthen cybersecurity protections for electronic protected health information (“PHI”). OCR noted several considerations that require these changes: (a) changes in healthcare environment, (b) sharp increase in breaches and cyberattacks, (c) common deficiencies observed by the OCR in its enforcement activity, (d) other cybersecurity industry guidelines, best practices and processes for protecting PHI, and (e) court decisions that affect enforcement of the Security Rule.

If finalized, the changes to the HIPAA Security Rule described in the Proposed Rule would impose multiple additional compliance obligations on HIPAA covered entities and business associates. Examples of the requirements with which covered entities and business associates would be required to comply include:

- Meet all security standards and implementation specification as the Proposed Rule removes the distinction between “addressable” and “required” implementation specifications of the security standards.
- Perform and document an audit at least once every 12 months of the covered entity’s or business associate’s compliance with each security standard and implementation specification.
- Perform and document a risk analysis in compliance with the implementation specifications identified in the Proposed Rule and review and update the risk analysis at least once every 12 months and in response to changes in operations.
- Implement a written risk management plan to reduce risk to PHI to a reasonable and appropriate level and review such plan at least once every 12 months.
- Conduct and maintain an accurate and thorough written inventory and a network map of electronic information systems and all technology assets that may affect the confidentiality, integrity or availability of PHI.
- Implement written policies and procedures for applying patches and updating the configurations of the relevant electronic information systems within specified time depending on the risk (e.g., within 15 days to address a critical risk).
- Encrypt PHI in transit and at rest, with limited exceptions.
- Terminate a workforce’s member access to PHI and relevant electronic information systems no later than one hour after the employment ends.
- Establish, review and test security incident response plan at least once every 12 months.
- Establish procedures to restore the loss of critical relevant electronic information systems and data within 72 hours of the loss.
- Deploy technical controls to protect PHI from improper alteration or destruction when at rest and in transit and review and test such controls at least once every 12 months.
- Deploy multi-factor authentication to all technology assets to verify that the person seeking access is the user the person claims to be, with limited exceptions.

- Obtain written verification from business associates that the business associates have deployed appropriate technical safeguards at least once every 12 months.
- Ensure that business associate agreements include a provision mandating the business associate to report activation of its contingency plan no later than 24 hours after activation.
- Conduct automated vulnerability scanning at least once every six months.
- Perform penetration testing on relevant information systems at least once every 12 months.
- Deploy technical controls to create and maintain exact retrievable copies of PHI which are no more than 48 hours older than the PHI maintained in the live, relevant electronic information system.
- Maintain written documentation of compliance with the Security Rule and review and update security policies and procedures at least once every 12 months.

Submitting Public Comments. OCR is soliciting comments on the Proposed Rule from industry stakeholders through March 7, 2025. The Proposed Rule may be modified in consideration of comments submitted.

authorsTest

milada

Milada R. Goturi

dani

Dani Elks