BLANKROME

Privacy, Security & Data Protection

JANUARY 6, 2025

HHS OCR Issues Notice of Proposed Rulemaking to Strengthen Cybersecurity for ePHI

On December 27, 2024, the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") issued a Notice of Proposed Rulemaking ("NPRM") to amend the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule to strengthen cybersecurity protections for electronic protected health information ("ePHI"). The NPRM is intended to support the Biden-Harris Administration's 2023 National Cybersecurity Strategy and its implementation plan, and to align with HHS' 2023 Healthcare Sector Cybersecurity concept paper that outlines HHS' path to advance cybersecurity enhancements for the health care sector.

The NPRM proposes the first significant updates to HIPAA's Security Rule in over a decade. The NPRM revises definitions of current terms and adds new terms to be consistent with modern best practices in cybersecurity. The NPRM also removes the distinction between "required" and "addressable" implementation specifications and makes all implementation specifications "required" with specific, limited exceptions, and adds specific compliance time periods for many existing requirements. Additionally, the NPRM requires all HIPAA-regulated entities to document all Security Rule policies, procedures, plans, and analyses.

Key changes to the Security Rule under the NPRM are as follows:

ADMINISTRATIVE SAFEGUARDS

- **Asset Inventory** – requires HIPAA-regulated entities to conduct and maintain a technology asset inventory and a network map that illustrates the movement of ePHI throughout the 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 entity's environment or operations that may affect ePHI.

- **Risk Analysis** – requires greater specificity for conducting a risk analysis, which now must include: (1) a review of the technology asset inventory and network map; (2) identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI; (3) identification of potential vulnerabilities and predisposing conditions to the HIPAA-regulated entity's relevant electronic information systems; and (4) an assessment of the risk level for each identified threat and vulnerability, based on the likelihood that each identified threat will exploit the identified vulnerabilities.

- **Patch Management** – requires HIPAA-regulated entities to implement written policies and procedures for patch management and to review, test and, where appropriate, modify such policies and procedures at least once every 12 months. Further requires patching, updating, or upgrading the configuration of a relevant electronic information system within a specified period of time relevant to the type of risk (*e.g.,* critical or high risk).

- **Workforce** – requires notification to relevant covered entities and business associates within 24 hours when a workforce member's access to ePHI or certain electronic information systems maintained by such covered entity or business associate is changed or terminated.

- **Security Incident** – strengthens requirements for planning for contingencies and responding to security incidents. Specifically, HIPAA-regulated entities would be required to, for example:

  - Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.

  - Perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration.

  - Establish written security incident response plans and procedures documenting how workforce members are to report suspected or known security incidents and how the entity will respond to suspected or known security incidents.

  - Implement written procedures for testing and revising written security incident response plans.

- **Compliance Audits** – requires HIPAA-regulated entities to conduct a compliance audit at least once every 12 months to ensure compliance with the Security Rule requirements.

- **Oversight of Business Associates** – requires that business associates verify at least once every 12 months for covered entities (and that business associate contractors verify at least once every 12 months for business associates) 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. Also requires 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.

PHYSICAL SAFEGUARDS

- **Facility Access Controls** – requires HIPAA-regulated entities to establish and implement written policies and procedures to limit physical access to all of its relevant electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

- **Workstation** – requires HIPAA-regulated entities to establish and implement written policies and procedures that, among other things, specify the physical attributes of workstation surroundings, including the removal of workstations from a facility and the movement of workstations within and outside of a facility, and to review, test, and, where appropriate, modify such policies and procedures at least once every 12 months.

TECHNICAL SAFEGUARDS

- **Network Segmentation** – requires network segmentation.

- **Encryption** – requires encryption of ePHI at rest and in transit, with limited exceptions.

- **Configuration Management** – requires HIPAA-regulated entities to establish and deploy technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner. New express requirements would include: (1) deploying anti-malware protection; (2) removing extraneous software from relevant electronic information systems; and (3) disabling network ports in accordance with the entity's risk analysis.

- **Audit Trails and System Logs** – requires HIPAA-regulated entities to deploy technology assets and/or technical controls that monitor in real-time all activity in their relevant electronic information systems, identify indications of unauthorized persons or unauthorized activity as determined by the entity's risk analysis, and alert workforce members of such indications.

- **Multi-factor authentication** – requires the use of multi-factor authentication to all technology assets in the HIPAA-regulated entity's electronic information systems, with limited exceptions.

- **Vulnerability Scanning** – requires vulnerability scanning at least every six months and penetration testing at least once every 12 months.

- **Backups** – requires HIPAA-regulated entities to create backups of ePHI with such frequency to ensure retrievable copies of ePHI are no more than 48 hours older than the ePHI maintained in the entity's relevant electronic information systems. Also, requires separate technical controls for backup and recovery of relevant electronic information systems, which must be reviewed, tested and, where appropriate, modified at least once every six months or in response to environmental or operational changes.

While HHS is undertaking this rulemaking, the current Security Rule remains in effect. Public comments on the NPRM are due 60 days after publication of the NPRM in the Federal Register.

Many of the changes to the Security Rule set forth in the NPRM have already been part of regulatory enforcement for some time, including through the enforcement actions by the Federal Trade Commission and States' Attorneys General. Such sweeping technical changes require significant investment of time, money, and resources to implement. Accordingly, while HIPAA-regulated entities will need to continue to monitor for comments and developments to the NPRM, HIPAA-regulated entities should take steps to evaluate and increase their cyber maturity along the lines suggested by the NPRM now.

For more information or assistance, please contact Sharon R. Klein, Alex C. Nisenbaum, Karen H. Shin, or a member of Blank Rome's Privacy, Security, & Data Protection group.

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Alex C. Nisenbaum
949.812.6011| alex.nisenbaum@blankrome.com

Karen H. Shin
949.812.6012 | kshin@blankrome.com