Buchalter
CLIENT ALERT

January 24, 2025

SIGNIFICANT NEW HIPAA OBLIGATIONS ON THEIR WAY FOR 2025

By: T. Mark Tubis

The Department of Health & Human Services (HHS) issued proposed changes to the HIPAA Security Rule ("Proposed Rule") on January 6, 2025, and is accepting comments from the public until March 7, 2025. The Proposed Rule includes several significant changes, and compliance will require considerable time and expense for covered entities and their business associates ("Regulated Entities"). These include the implementation of additional security measures and updates to all existing business associate agreements. HHS estimates that the industrywide first year costs of the Proposed Rule will be $9 billion, with a five-year estimate of $33 billion.

After the comment period ends, HHS will publish the Final Rule in the Federal Register, and the new rules will become effective 60 days after publication. The compliance deadline for the requirements will be 180 days after publication. Although the date of publication is not yet known, it is likely that compliance with the new rules will be required before the end of 2025.

The changes include the following:

- Compliance time periods and documentation requirements are added
- Risk analyses must include:
    - A review of the technology asset inventory and network map
    - Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI
    - Identification of potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems
    - 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
- Relevant covered entities and business associates must be notified within 24 hours when a workforce member's access to ePHI or certain electronic information systems is changed or terminated.
- A written contingency plan must be established and implemented that includes procedures for data backups, disaster recovery, and emergency mode operations. Disaster recovery plans must now set forth a procedure for restoring critical systems within 72 hours of a loss.

- Business associates must notify covered entities (and subcontractors must notify business associates) upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.
- New security controls must be implemented, including encryption of ePHI at rest and in transit, as well as the use of multi-factor authentication
- Covered entities and business associates must conduct compliance audits at least once every 12 months
- Written documentation is required of all Security Rule policies, procedures, plans, and analyses
- Business associates must verify at least once every 12 months for covered entities (and business associate subcontractors 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.

If you wish to comment, then it should be identified by RIN Number 0945–AA22 and can be submitted by any of the following ways:

- Federal Register website at https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information#footnote-21-p901. Select the "Submit a Public Comment" button and complete the form.
- **Federal eRulemaking Portal** at https://www.regulations.gov by searching for the Docket ID number HHS-OCR-2024-0020.
- **Regular, Express, or Overnight Mail** to the following address: U.S. Department of Health and Human Services, Office for Civil Rights, Attention: HIPAA Security Rule NPRM, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue SW, Washington, DC 20201.

Note that duplicate comments should not be submitted.

Buchalter attorneys partner closely with clients ranging from closely held practices to nationwide healthcare businesses to provide broad, protective counsel that minimizes risk exposure. Our critical risk-management solutions allow clients to focus on managing their businesses while we manage the details of their healthcare regulatory, corporate, and employment issues. We work closely with business management to ensure workplace and industry compliance, and to respond immediately when conflict arises. We prepare and implement patient and provider documents, and advise on corporate structures, healthcare privacy and fraud and abuse.

As always, our team stands ready to assist your business with all of its health care, corporate, employment, or any other legal needs. If you have questions or need assistance, please feel free to contact the attorneys listed below.

T. Mark Tubis
Attorney
(949) 224-6414
mtubis@buchalter.com