KIRKLAND & ELLIS

Kirkland Alert

OCR Proposes Changes to the HIPAA Security Rule

06 January 2025

On December 27, 2024, the U.S. the Department of Health and Human Services (HHS), Office for Civil Rights (OCR), issued a proposed rule to modify the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), Security Rule to strengthen cybersecurity safeguards for regulated entities and electronic protected health information (ePHI) (the "Proposed Rule").

The Proposed Rule aims to modernize cybersecurity requirements, bridge compliance gaps, and tackle evolving threats with new administrative, technical, and physical safeguards. Key features include mandatory encryption, enhanced access controls, expanded risk analysis requirements, and revised business associate agreement obligations.

These updates may require additional investment in regulated entities' cybersecurity and HIPAA compliance program but taking required measures may help mitigate remediations costs related to future incidents. With the change in administration, it is unclear whether a final rule will reflect the changes outlined in the Proposed Rule or whether a final rule will be adopted. While the Proposed Rule may be impacted by the change in administration, cybersecurity is an area with bipartisan support. HIPAA-regulated entities should consider evaluating their cybersecurity posture considering the Proposed Rule's requirements and engaging in the public comment process before the Proposed Rule is finalized.

Background

Since its implementation in 2003, the current HIPAA Security Rule has set standards for covered entities (e.g., healthcare providers, health plans, and clearinghouses) and

their business associates (e.g., contractors or vendors handling ePHI) to safeguard the confidentiality, integrity, and availability of ePHI. ePHI includes identifiable health information about a person's health, treatment, or payment but excludes de-identified data, employment records, and certain education records that are produced, saved, transferred, or received in an electronic form. HIPAA remains the primary health data privacy and security law in the United States, particularly at the federal level.

Rising Threats Fueling Reforms

In the past decade, the healthcare landscape has undergone significant digitization. Technologies such as telehealth and electronic health records (EHRs) have improved patient care but have also introduced heightened cybersecurity risks. In 2024, over 180 million people were affected by breaches involving PHI, setting a new record. Recent healthcare breaches have reportedly cost an average of $10.1 million per incident, generally making them more expensive than breaches in any other industry. To address these risks, HHS has proposed the first major Security Rule update in over a decade, introducing more explicit obligations for covered entities and business associates to safeguard patient data.

Key Takeaways from the Proposed Rule

Certain notable requirements under the Proposed Rule, including the following:

- **Eliminating the Distinction between "Addressable" and "Required"**. The Proposed Rule eliminates the distinction between "addressable" and "required" standards to improve the consistency with which regulated entities apply current Security Rule standards. Previously, the "addressable" classification provided flexibility in meeting safeguards. However, HHS notes that many entities considered such safeguards optional and failed to implement important protections. The Proposed Rule makes clear that HIPAA-regulated entities are required to comply with all security standards, with specific, limited exceptions.
- **Enhanced Administrative Safeguards**. The Proposed Rule includes several enhanced administrative safeguards, including:
  - **Technology Asset Inventory**: Under the Proposed Rule, HIPAA-regulated entities would be required to maintain a technology asset inventory and network map of electronic information systems. Notably, under the network map requirement, a HIPAA-regulated entity is required to illustrate the movement of ePHI throughout

its systems to better understand potential vulnerabilities. The Proposed Rule would require regular review of the inventory and network map when there are changes in environment or at least every twelve (12) months.

- **Risk Analysis and Evaluation**: The Proposed Rule also includes new directives for conducting full risk assessments, including conducting both gap assessments (e.g., assessing gaps between current practices and requirements) and risk analyses (e.g., assessing the potential risks and vulnerabilities to ePHI) and assigning categories of potential impact of the identified risk. Under the Proposed Rule, risk analyses should be conducted at least once every twelve (12) months, with evaluations conducted when new technology is adopted.
- **Patch Management**: Timely implementation of patches, updates, and upgrades can help companies defend against common cyberattacks. Accordingly, the Proposed Rule includes updated requirements for patch management, including annually updating policies and procedures for identifying, installing, and verifying the timely installation of patches, updates, and upgrades throughout electronic information systems.
- **Contingency Planning**: To ensure limited downtime in response to cyberattacks and emergencies like system failures, fires, floods, and other natural disasters, the Proposed Rule requires the implementation of a contingency plan. Under the Proposed Rule, a compliant contingency plan includes a data backup plan, written procedures to restore crucial data within seventy-two (72) hours of the loss, consistent review of policies and procedures, and ongoing testing and revision of the plan.

- **Enhanced Technical Safeguards**. The Proposed Rule requires covered entities and business associates to deploy a wider and more specific set of technologies and controls, including:
  - **Encryption**: Encryption is now a mandatory requirement, requiring the use of a secure encryption algorithm for all ePHI, with limited exceptions. Regulated entities that currently meet HHS's expectations for encryption (e.g., requiring encryption where "reasonable and appropriate") will already be in compliance without major changes.
  - **Network Segmentation**: The Proposed Rule requires network segmentation (a process of dividing computer networks into small, isolated components) where "reasonable and appropriate" is based on a risk analysis. Especially for large entities, network segmentation can be a complicated, time-consuming, and highly technical process to implement.
  - **Multi-Factor Authentication (MFA)**: MFA, defined in the Proposed Rule as requiring at least two forms of authentication (e.g., password and biometric verification or smart identification card), will be a required safeguard for accessing systems containing ePHI under the Proposed Rule. MFA has become a key focus of

regulators, as some well-known data breaches have resulted from a failure to implement MFA.

- **Enhanced Physical Safeguards**. The Proposed Rule clarifies the definition of "workstation" to include mobile devices such as smart phones or tablets, and requires regulated entities to address the physical characteristics of workstations that can access ePHI in their policies and procedures, including the removal and movement of such workstations within and outside of a facility.
- **Required Notifications**. The Proposed Rule implements various new (and arguably aggressive) notification requirements for regulated entities. For instance, a business associate must notify a covered entity within twenty-four (24) hours when there is a change in or termination of a workforce member's access to ePHI or electronic information systems and that workforce member had access to such covered entity's ePHI. Additionally, a business associate is required to provide notice to a covered entity no later than twenty-four (24) hours after a contingency plan (as detailed above) is activated.
- **Business Associate Review and Delegation**. In addition to obtaining satisfactory assurances that a business associate will comply with the current Security Rule, the Proposed Rule requires a regulated entity to verify that its business associates have technical safeguards in place to protect ePHI at least every twelve (12) months. The verification includes a written analysis by a cybersecurity professional to ensure the business associate's compliance. Additionally, the Proposed Rule clarifies that a regulated entity may allow a business associate to serve as the entity's Security Officer.

Practical Implications for Healthcare Investors and Compliance Officials

- Cost Increases: Compliance with encryption, MFA, and expanded risk analysis requirements may necessitate significant investments, particularly for smaller providers who have not yet implemented such measures.
- Mitigating Cyber Risk: Implementing these standards may help to mitigate the financial and reputational damage from breaches, which, according to one study, cost healthcare organizations an average of $10.1 million per incident.
- Regulatory Risk: HHS's emphasis on recent breaches, widespread non-compliance, and enforcement challenges under the current Security Rule suggests a heightened risk of enforcement actions if the Proposed Rule is adopted. Non-compliance with the updated standards could result in enforcement actions and penalties, as HHS has indicated a stronger focus on enforcement under the Proposed Rule.

- Bipartisan Support: While the Proposed Rule was published under the Biden administration and will likely undergo some revision, it may (in some form) retain support from the incoming Trump administration, given that healthcare cybersecurity has emerged as a bipartisan concern.

Conclusion: Preparing for Stronger Cybersecurity Standards

The Proposed Rule reflects the urgent need to address growing cybersecurity risks in healthcare. Covered entities and business associates may consider assessing the readiness of their cybersecurity programs, participating in the comment process, and aligning operations with the proposed standards to minimize disruption.

Compliance Deadlines and Key Dates

1. **Comment Deadline**: March 7, 2025.
2. **Effective Date of Final Rule**: Sixty (60) days after Final Rule's publication in the Federal Register.
3. **Compliance Deadline**: One hundred eighty (180) days from the Effective Date for most provisions.
4. **Business Associate Agreement Transition Period**: Additional time will be allowed to revise business associate agreements to meet updated requirements.

Related Professionals

Dennis Williams

Partner / New York

Sunil Shenoi

Partner / Chicago

Robert Kantrowitz

Partner / New York

Micah J. Desaire

Associate / New York

Cecilia Brisuda

Associate / Chicago

Marie Macaulay

Associate / Chicago

Related Services

Practices

- Healthcare & Life Sciences Regulatory
- Government, Regulatory & Internal Investigations

Suggested Reading

- 01 January 2025 In the News Healthcare and Life Science Deals Attys Expect In 2025
- 27 December 2024 Press Release Kirkland Advises ContourGlobal on Successful Completion of $612 Million Refinancing of Natural Gas Portfolio in the U.S.
- 27 December 2024 Kirkland Alert Federal Court Reimposes Suspension of Corporate Transparency Act Reporting Obligations