OCR Proposes Sweeping Changes to the HIPAA Security Rule

By Thomas J. DeMayo, Partner and Robert Gaines, Director

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services recently issued a Notice of Proposed Rulemaking (NPRM) to update the Health Insurance Portability Accountability Act (HIPAA) security rule. The rule has remained relatively unchanged over the years because it was designed to be flexible and driven by the risk assessment process of covered entities. In response to the evolving nature of cybersecurity threats and the ever-increasing reliance on digital technology in health care, changes have been proposed to strengthen cybersecurity protections for electronic protected health information (ePHI).

Backdrop

The HIPAA security rule was first introduced in 2003. It was subsequently revised in 2013 as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, more commonly known as the Omnibus Rule. The rule was initially designed to protect the confidentiality, integrity and availability of ePHI by requiring covered entities and business associates to implement safeguards. This includes access controls, encryption and audit controls to secure data from unauthorized access or breaches.

Over time, most entities do not perform proper risk assessments, resulting in unaddressed information security risks and, consequently, an unending wave of health-care-related breaches. And threats are evolving rapidly, as we've seen with the attack on UnitedHealth that leaked the private information of more than 190 million patients earlier last year.

Proposed Controls

The updated rule proposes sweeping changes. It increases specificity of required controls to strengthen the security standards and implementation specifications with new proposals and clarifications, including:

- All security measures will be mandatory, with a few clearly defined exceptions.
- Written documentation of all security rule policies, procedures, plans and analyses will be required.
- Revision of technical definitions and implementation specifications to align with current industry standards.

The proposed rules will also involve:

Security Enhancements

- Mandatory use of multi-factor authentication.
- Requiring the encryption of ePHI at rest and in transit, with limited exceptions.

- Deploying network segmentation.
- Mandating separate technical controls for backup and recovery of ePHI.

System Configuration and Asset Management

- Standardizing the configuration of information systems to include anti-malware protection, removing redundant software and disabling unused network ports.
- Creating an asset inventory and a data flow diagram that illustrates the movement of ePHI through the entity's information system, which is reviewed every 12 months.

Risk Analysis and Compliance Monitoring

- Adding new requirements for conducting a risk analysis that involves reviewing the technology asset inventory and network map, identifying threats and vulnerabilities to ePHI, and assessing the risk level and likelihood of exploitation for each identified threat and vulnerability.
- Performing vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Auditing regulated entities for compliance at least once every 12 months that reviews and tests the effectiveness of specific security measures.

Incident Response and Notification Requirements

- Increasing requirements for incident response planning by identifying and prioritizing critical systems and technologies for restoration and establishing written procedures to recover essential systems and data within 72 hours.
- Requiring staff reporting protocols and response strategies as a component of the incident response plan and implementing regular testing and updates of the plan.
- Annually confirming that business associates and their contractors have the necessary security measures to protect ePHI and must notify covered entities no later than 24 hours after an incident.
- Notifying within 24 hours if a workforce member's access to ePHI or certain electronic information systems is changed or terminated.

Additional Compliance Requirements

- Adding compliance periods to existing requirements.
- Requiring group health plan sponsors to follow the Security Rule requirements for controls and notification if they store or maintain ePHI.

Enforcement

Public comments on the NPRM will run for another 50 days, but until then, the current security rule remains in effect. The enforcement of the rule change is expected to be more aggressive than in previous years to more effectively prevent sensitive information from being leaked by cyberattacks like the ones that hit Ascension and UnitedHealth. Oversight will continue from the OCR at the U.S. Department of Health and Human Services.

How to Prepare

While the rule remains in public commentary, covered entities should evaluate the sufficiency of their overall cyber and information security program to ensure it is reasonable and aligned with industry best practices. Now is the time to consider performing or updating a comprehensive risk assessment to identify potential hazards that have gone unaddressed or would benefit from an additional or modified set of controls.

Contact Us

We have a team of Cybersecurity and IT Privacy professionals who specialize in helping covered entities and businesses manage the ever-evolving cyber and regulatory landscape. If these new changes impact your business and you need assistance, please contact your client service team or:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Robert Gaines, CISSP, CECI, CCFI, C|OSINT
Director
Cybersecurity and Privacy Advisory
rgaines@pkfod.com | 425.518.1974