Health Law Alert: New HIPAA Rule to Aid Health Care Organizations in Managing Cyber Risk

March 16, 2016

On Feb. 24, the Department of Health and Human Services' Office for Civil Rights (OCR) published a HIPAA Security Rule Crosswalk designed to assist health care organizations that are covered entities or business associates in strengthening their cybersecurity preparedness posture. Developed in partnership with the National Institute of Standards and Technology (NIST) and the Office of the National Coordinator for Health IT (ONC), the Crosswalk allows health care organizations to quickly and easily identify the overlap between the HIPAA Security Rule and the NIST Cybersecurity Framework (as well as other security frameworks) in a manner that will both aid compliance with the Security Rule and strengthen overall cybersecurity. The full text of the OCR Crosswalk may be found here. The new Crosswalk continues the OCR trend over the past few years of publishing guidance intended to help covered entities and business associates meet their HIPAA obligations. Other helpful tools can be found here.

Background: Separate Guidelines, Similar Goals

Electronic personal health information (ePHI) stored by health care providers, plans and business associates is rapidly becoming a favorite target for criminal hackers and other unauthorized individuals. Recent reports indicate that the health care industry accounted for over 42 percent of all data breaches nationwide in the last three years—significantly more than any other single industry. More ominously, a staggering 91 percent of all health care organizations have reported at least one data breach in the past 24 months. Individual breaches can range from inappropriate access of a few records to broad-ranging security attacks, such as last year's cyberattack on Anthem, which news reports suggest involved nearly 80 million private personnel files.

The HIPAA Security Rule requires covered entities and business associates to implement strong data security safeguards to ensure the confidentiality and integrity of all ePHI records. Failure to meet these requirements can result in stiff civil fines, private liability, and substantial loss of consumer goodwill. While covered entities have been obligated to comply with the Security Rule since 2005, business associates only became directly liable for HIPAA compliance in 2013. As a result, many business associates have less experience in complying with HIPAA requirements than their covered entity counterparts. To help health care organizations cope with the cybersecurity problem, in 2014 NIST released its Cybersecurity Framework

as a voluntary framework to guide institutions in reducing risk to their critical IT infrastructure. The NIST Cybersecurity Framework, which organizes cybersecurity into five key functions and several activity categories and sub-categories, has become an increasingly popular cybersecurity standard in the health care field since its release.

Crosswalk Seeks to Bridge the Gap

In recognition of the popularity of the NIST Cybersecurity Framework, OCR's new Crosswalk seeks to help covered entities and business associates comply with their HIPAA Security Rule obligations while simultaneously reducing cybersecurity risk system-wide. The Crosswalk works by mapping each administrative, physical, and technical safeguard standard and implementation specification in the HIPAA Security Rule to a relevant NIST Cybersecurity Framework subcategory. For those organizations that have already aligned their security with the NIST Framework or the HIPAA Security Rule, the Crosswalk provides a helpful tool to highlight gaps and vulnerabilities that may exist in current programs. By addressing these gaps, organizations can bolster HIPAA compliance and improve the security of their ePHI.

Because the HIPAA Security Rule is designed to be flexible, scalable, and platform agnostic, the Crosswalk also provides guidance for organizations that rely on frameworks other than the NIST Cybersecurity Framework, or for those that are currently in the process of implementing a framework for the first time. For these organizations, the Crosswalk serves as a reference for development of a comprehensive security program aligned with Security Rule requirements and industry best practices.

While the Crosswalk serves an important purpose by integrating the HIPAA Security Rule with the NIST Cybersecurity Framework and other frameworks, it is important to note that reliance on the Crosswalk alone is insufficient to guarantee compliance with the Security Rule. OCR has noted in its guidance that some specific Security Rule standards, such as those relating to documentation and organization, do not perfectly map to NIST Cybersecurity Framework subcategories. Thus, while the Crosswalk is a valuable resource for covered entities and business associates to use in designing a comprehensive cybersecurity system, it is not a replacement for careful attention to applicable laws and regulations.

The Takeaway

As health care organizations continue to face increased risk from cybersecurity breaches, security officers and others should review the Crosswalk to identify gaps in their security programs and to revise their policies and procedures where appropriate. Implementing thorough safeguards for ePHI that comply with industry best practices is critical to avoiding serious headaches down the road.

HIPAA and health care privacy issues will be among the topics covered at Gray Plant Mooty's 20th annual Health Law Conference. The Conference will be at the Depot in Minneapolis and will provide valuable updates on current issues and recent developments in health law. Save the date and invitation forthcoming.

If you have any questions about the HIPAA Security Rule, the NIST Cybersecurity Framework, or the new OCR Crosswalk, please contact Jesse Berg at jesse.berg@lathropgpm.com (612.632.3374) or Catie Bitzan Amundsen at catherine.bitzan@lathropgpm.com (612.632.3277).