OCR Releases Tool to Help Organizations Safeguard Health Data

March 02, 2016

Health data is among the most attractive targets for cybersecurity attacks. To help ward off attacks, health care organizations and their subcontractors subject to the Health Insurance Portability and Accountability Act (HIPAA) must continuously strive to improve their protection of health data as required by the HIPAA Security Rule. Looking beyond the HIPAA Security Rule, however, to other cybersecurity frameworks is increasingly becoming a standard of practice for many organizations as they implement and update information security policies and procedures. Indeed, the U.S. Department of Health & Human Services, Office for Civil Rights (OCR), has recognized the utility of taking a broader accounting of cybersecurity standards and, on February 24, 2016, released a tool to assist HIPAA regulated entities with mapping HIPAA Security Rule standards to other cybersecurity frameworks. Security Officers and C-Suite executives will find the tool of great help in understanding expectations and what may be considered "industry standard" for organizations moving forward.

The tool is a crosswalk that maps each administrative, physical and technical safeguard standard and implementation specification in the HIPAA Security Rule to a relevant subcategory of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). The crosswalk was developed in conjunction with NIST and the Office of the National Coordinator for Health IT (ONC). In addition to mapping standards between the HIPAA Security Rule and the NIST Cybersecurity Framework, the crosswalk also maps to other commonly used frameworks, such as the Council on Cybersecurity Critical Security Controls (CCS CSC), Control Objectives for Information and Related Technology Edition 5 (COBIT 5), International Organization for Standardization (ISO) 27001, and NIST SP 800-53 Rev. 4.

NIST has developed security guidance and specific standards that organizations in the health care industry have relied on for years, so the crosswalk between the NIST Cybersecurity Framework and the HIPAA Security Rule is a logical next step. NIST released the Cybersecurity Framework in February 2014 as a voluntary framework (based on existing standards, guidelines and practices) for reducing cyber risks to critical infrastructure. The NIST Cybersecurity Framework can help any organization understand and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

The crosswalk provides a roadmap for health care organizations subject to HIPAA to recognize how the NIST Cybersecurity Framework, the HIPAA Security Rule and other security frameworks overlap. In a time of increasing risks, understanding this overlap can help organizations safeguard health data. In order to comply with the HIPAA Security Rule, covered entities and their business associates must implement robust data security safeguards to ensure the confidentiality, integrity and availability of all of the electronic protected health information (ePHI) they create, receive, maintain or transmit. Despite substantial efforts to protect ePHI, for many covered entities and their business associates, ePHI remains vulnerable to unauthorized access and breach. The crosswalk is another tool for organizations to use to strengthen their information security programs.

For organizations that have implemented information security programs that meet the HIPAA Security Rule requirements or follow the NIST Cybersecurity Framework, the crosswalk can be used to identify potential gaps in their security programs. Organizations can then take specific actions to address these gaps, which will improve their ability to safeguard ePHI from a multitude of cybersecurity threats and strengthen compliance with the HIPAA Security Rule. For other organizations, the crosswalk can be used to develop and implement a comprehensive information security program based on existing standards. Organizations can also use the crosswalk to update their policies and procedures to incorporate references to applicable sections of the HIPAA Security Rule, NIST Cybersecurity Framework and other security frameworks, which helps an organization show that it has done its homework, followed known standards and has adequate policies and procedures in place to address cybersecurity risks.

It is important to note that integrating the NIST Cybersecurity Framework into an information security program does not assure compliance with the HIPAA Security Rule. On the other hand, the HIPAA Security Rule does not require covered entities and their business associates to integrate the NIST Cybersecurity Framework into their information security programs. Rather, covered entities and their business associates must perform their own security risk assessment to identify and mitigate threats to the ePHI they create, receive, maintain or transmit.

The crosswalk provides a tool organizations can use to inform their decision making and assist with comprehensive management of cybersecurity risks. The crosswalk also encourages covered entities and their business associates to increase cybersecurity awareness, enhance their information security programs and implement appropriate safeguards to protect ePHI.

Organizations should review the crosswalk and consider using it to identify potential gaps in their information security programs, revise and refine their policies and procedures in light of the crosswalk, or develop and implement a comprehensive information security program if they have yet to do this.

For more information about the crosswalk and how it may help your organization, contact any member of Baker Donelson's Privacy and Information Security Team.