Health Law Alert: HHS Publishes Cybersecurity Best Practices Aimed at Protecting Health Care Organizations

On December 28, 2018, the U.S. Department of Health & Human Services (HHS) released a publication on voluntary health care cybersecurity best practices for all health care organizations, titled Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. The publication includes a main document that details five cybersecurity threats impacting the health care industry and two technical volumes that detail ten practices to mitigate these threats. In a letter from Deputy Secretary of Health and Human Services, Eric Hargan, contained at the beginning of the publication, Mr. Hargan states:

"This publication is the result of the collaborative work HHS and its industry partners embarked on more than a year ago—namely, the development of practical, understandable, implementable, industry-led, and consensus-based voluntary cybersecurity guidelines to cost-effectively reduce cybersecurity risks for health care organizations of varying sizes, ranging from local clinics, regional hospital systems, to large health care systems."

The Cybersecurity Act of 2015

The publication was written in response to requirements provided by the Cybersecurity Act of 2015 (CSA). Section 405(d) of the CSA calls for "Aligning Health Care Industry Security Approaches." A task group was therefore formed in May 2017 consisting of health care and cybersecurity experts from the public and private sectors. In accordance with the CSA, the publication seeks to cost-effectively reduce cybersecurity risks, support the voluntary implementation of the guidance, and ensure that the content is practical and relevant to health care organizations of all sizes and resources. More specifically, "[t]he task group's approach to the guidance document [is that it] (1) Examines current cybersecurity threats affecting the HPH [Health Care and Public Health] sector; (2) Identifies specific weaknesses that make organizations more vulnerable to threats; and (3) Provides selected practices that cybersecurity experts rank as the most effective to mitigate the threats."

Five Cybersecurity Threats Facing the Health Care Industry

The publication addresses the following five cybersecurity threats and provides various tips to avoid or reduce the threats, which are summarized as follows:

Email phishing attacks

- Email phishing is an attempt to trick you into giving out information using email
- The inbound email often contains an active link or file, and appears to come from a legitimate source
- Clicking on the link or file could introduce malicious software into your technology systems

Tip: Ask yourself if you know the sender of the email and if there are any indicators that the tone or style of the email is off before opening; check with other colleagues to see if they received something similar; check your organization's policies for reporting suspicious emails.

Ransomware attacks

- Ransomware is a type of malicious software that attempts to deny access to data, often by encrypting the data with a key known only to the hacker, until the data's owners pay a ransom

Tip: *Ensure your computer and network have the proper intrusion prevention system or software; provide user awareness and compliance training to your workforce.*

Loss or theft of equipment or data

- Devices such as laptops, tablets, and smartphones are lost or stolen by hackers resulting in the unauthorized or illegal dissemination of sensitive data

Tip: *Ask whether you can travel with equipment or take equipment offsite; know your organization's policies on removing equipment from the workplace; report lost or stolen equipment immediately.*

Insider, accidental or intentional data loss

- Insider threats may be accidental (honest mistakes) or intentional (malicious loss or theft) caused by an employee, contractor, or other user of the organization's technology systems

Tip: *Conduct regular security training sessions, including "See something? Say something" training.*

Attacks against connected medical devices that may affect patient safety

- Example: A cyber attacker gains access to a provider's computer and takes command of a file server to which a heart monitor is attached

Tip: *Knowledge of protocols for potential attacks on medical devices should be shared at new hire orientation or security training; share protocols with patients when they are given medical devices.*

Ten Practices to Mitigate These Threats

HHS stresses that threats to cybersecurity is not simply an IT problem. "The most effective combination of safeguards and cybersecurity practices must be determined based on the organization's needs, exposures, resources and capabilities." The publication addresses the following ten practices to mitigate these threats:

- Email protection systems
- Endpoint protection systems
- Access management
- Data protection and loss prevention
- Asset management
- Network management
- Vulnerability management
- Incident response
- Medical device security
- Cybersecurity policies

How We Can Help

Cybersecurity breaches threaten patient care and safety, put patients at risk of identity theft and financial abuse, and result in business interruption and financial and reputational harm to health care providers. HHS reports that $6.2 billion was lost by the U.S health care system in 2016 alone due to data breaches, and that the average cost of a data breach to health care organizations is $2.2 million

HHS recommends a variety of actions to mitigate the risks and reduce the impact of a cybersecurity threat. The HHS publication also provides a method for assessment in accordance with National Institute of Standards and Technology (NIST) guidance to help organizations implement and prioritize the best practices set forth by the task force.

If you would like more information or assistance with developing, updating, or implementing your HIPAA compliance program, staff training, or adopting cybersecurity best practices, contact:

Lani M. Dornfeld | 973.403.3136 | ldornfeld@bracheichler.com