Pepper Hamilton LLP
Attorneys at Law

Health Sector Cybersecurity Guidance Provides Best Practices Applicable Across Industries

ALERT | February 21, 2019

Sharon R. Klein | kleins@pepperlaw.com
Alex C. Nisenbaum | nisenbauma@pepperlaw.com
Karen H. Shin* | shink@pepperlaw.com

**Karen H. Shin is a law clerk in the Health Sciences Department. She is not admitted to practice law.*

While cyberattacks continue to increase in number, health care organizations face some of the greatest risks. According to the Health Sector Coordinating Council (HSCC) — a coalition of industry associations that operates in in public partnership with the government — 95 percent of health care organizations have been targeted for a cyberattack. And these attacks are particularly costly. In the health care industry, the cost per record breached is $408, nearly double the cost in other industries. In 2017 alone, breaches cost the health care industry more than $6 billion dollars.

But the U.S. government is trying to help the health care industry protect the data and security of its patients. In partnership with government agencies like the Department of Health and Human Services and the Food and Drug Administration, the HSCC has released two guidance documents that provide best practices and helpful tips for organizations seeking to increase their cybersecurity protections or organizations responding to a data breach. While the guidances are designed to assist the health care industry, they have broad applicability to any organization looking for guidelines to develop a cybersecurity framework.

'Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients'

Released in December 2018, the first of HSCC's guidance documents was created in partnership with HHS in response to a mandate in the Cybersecurity Act of 2015 section 405(d).[1] The Cybersecurity Practices guidance, which was two years in the making, sets forth a comprehensive, user-friendly "set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes." Its goal is to cost-effectively reduce cybersecurity risks for health care organizations of all sizes, ranging from small physician practices to large university hospital systems. It also provides technical implementation recommendations for IT and information security professionals.

The centerpiece of the Cybersecurity Practices guidance is a 36-page document (available at: https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf) that provides practical examples of how to incorporate privacy and security by design, as well as how to respond to different potential cybersecurity threats. The document identifies the five most common cybersecurity threats faced by the health care industry and provides a definition, real-world example, and tips on how to address the risk, ranging from best practices that all employees should use to enterprisewide policies and procedures.

The Cybersecurity Practices guidance also contains three other documents that provide a deeper dive for organizations that need more assistance in implementing a cybersecurity program: Technical Volume 1 (for small health care organizations, available at: https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol1-508.pdf), Technical Volume 2 (for medium and large health care organizations, available at: https://healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol2-508.pdf), and Resources and Templates (available at: https://healthsectorcouncil.org/wp-content/uploads/2018/12/resources-templates-508.pdf).

The technical volumes present 10 cybersecurity practices to mitigate the top threats identified in the primary document, with subpractices and advice on implementation specific to the size of the health care organization.

‘Medical Device and Health IT Joint Security Plan’

In January 2019, the HSCC released the second of its guidance documents. The Joint Security Plan (available at: https://healthsectorcouncil.org/the-joint-security-plan/)was produced in partnership with the FDA and other governmental agencies in response to the 2017 recommendations of the Health Care Industry Cybersecurity Task Force, which urged strong efforts toward increasing the security and resilience of medical devices and health IT.

The Joint Security Plan is tailored to medical device manufacturers, health information technology vendors and health care providers. It aims to serve as a reference guide for the total life cycle of a product (including concept, design, development, qualification, launch and end of life), and provides guidance on how to develop, deploy and support cybersecure technology solutions in the health care industry.

The Joint Security Plan address four major topics:

1. Risk Management – From product concept to product launch, the Joint Security Plan recommends that health care organizations implement risk registers, have a cybersecurity management plan in place, maintain an inventory of all software-enabled products and services, secure supply chains, and ensure third parties are also committed to the cybersecurity of medical devices and health IT.

2. Design Control – From product concept through product qualification, the Joint Security Plan recommends that health care organizations employ policies and procedures to ensure that product design inputs will allow for cybersecurity protection. These include establishing high-level security requirements, periodically scanning for vulnerabilities, maintaining system hardening standards, securing coding standards, periodically performing static and dynamic code analyses, maintaining system-patching, conducting robustness and penetration testing, adhering to customer information security policies, ensuring password security, and documenting security information for customers.

3. Complaint Handling and Reporting – After the product launches, the Joint Security Plan recommends that organizations gather feedback on the cybersecurity performance of their products. To do this, the Plan recommends having systems for escalating customer complaints and properly investigating them, notifying other potentially affected customers, reporting these cybersecurity vulnerabilities to stakeholders, having a vulnerability and patch management plan to allow customers to download and install patches, and having procedures in place for when the product's security can no longer be supported or when the vendor discontinues support and maintenance of the product.

4. Evaluating Joint Security Plan Progress and Maturity – The Plan provides a reference model for organizations to measure and track progress of a vendor's cybersecurity program for its medical technology.

Pepper Points

1. While neither of the HSCC's guidance documents are binding authority, they do provide an industrywide standard for cybersecurity protections that will likely be relied on by regulators and courts.

2. Plaintiffs in cybersecurity lawsuits are also likely to rely on the HSCC's guidance in filing suit after a data breach. If an organization's cybersecurity practices and policies fell short of those outlined in the HSCC's guidance, it is likely that plaintiffs will note these areas as contributing to the breach in any filed lawsuit.

3. The HSCC's guidance is consistent with the National Institute of Standards and Technology Cybersecurity Framework, and organizations relying on the NIST guidelines will already find themselves closely following the HSCC's identified best practices.

4. Health care organizations of all sizes and disciplines, including pharmaceutical and medical device manufacturers and health care providers, should evaluate their cybersecurity policies and procedures in light of the HSCC's guidance. If any gaps are identified, organizations should implement the suggested frameworks in the HSCC documents.

5. Organizations outside the health care industry, particularly those with limited cybersecurity resources, should also review the HSCC's guidance, and the Cybersecurity Practices document in particular. These best practices are applicable to any organization seeking to enhance its cybersecurity practices and can be used as a first step to protecting against potential cyberattacks.

Endnotes

1 Pepper Hamilton partner Sharon R. Klein, one of the authors of this article, was a member of the task force that developed this guidance document.

Sharon R. Klein and Alex C. Nisenbaum are members of Pepper Hamilton's Privacy, Security and Data Protection Group and the firm's Health Sciences Department, a team of 110 attorneys who collaborate across disciplines to solve complex legal challenges confronting clients throughout the health sciences spectrum. Karen H. Shin is a law clerk in the Health Sciences Department. She is not admitted to practice law.