Published on *The National Law Review* https://natlawreview.com

New Cybersecurity Tools for The Health Care and Public Health Sectors

Article By:

Carla M. Dewberry

Jake Bernstein

Cybersecurity is not simply a technical issue of interest only to information technology departments. Cybersecurity issues create risk throughout healthcare entities and must be managed as a core business risk; at a minimum, they impact patient safety, business continuity, reputations, regulatory compliance, and economics.

On 17 April 2023, the US Department of Health and Human Services (HHS) released three cybersecurity tools specific to the healthcare and public health (HPH) sector, namely, a cyber awareness document, cyber educational tools, and an industry risk analysis. These important resources are available here and are discussed below.

A. Health Industry Cybersecurity Practices (HICP) 2023 Edition

The HICP is intended to be a starting point for use within the HPH sector to implement basic cybersecurity practices. HHS describes this document as a foundational publication that aims to raise awareness of cybersecurity risks, provide best practices, and help set standards in mitigating the most pertinent cybersecurity threats to the sector. There are two separate technical volumes appended to the core document. One of the technical volumes is for use by small health care organizations, the second is for use by medium and large health care organizations. Both versions provide recommendations relating to Health Insurance Portability and Accountability Act (HIPAA) compliance.

The HIPAA Security Rule (the Security Rule) sets out standards that a HIPAA-covered entity must comply with. The Security Rule (at 45 C.F.R. § 164.306) provides for a flexible, scalable, and technology-neutral framework to allow all covered entities to comply in a manner that is consistent with the unique circumstances of their size and environment.

The HICP provides a series of cybersecurity practices designed by HHS to help prevent, react to, and recover from cybersecurity threats. The HICP technical volumes group these practices into “Sub Practices” for different sizes of organizations and provide guidance across the following areas:

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Security Operation Centers and Incident Response
9. Network Connected Medical Devices
10. Cybersecurity Oversight and Governance Threat

B. Knowledge on Demand

The second tool provided by HHS is a new online educational platform, which provides training to improve cybersecurity awareness within health and public health organizations. This tool includes five training modules in the following five subject areas (which are intended to align with the top five cybersecurity threats discussed in the HICP):

1. Social engineering
2. Ransomware
3. Loss or theft of equipment of data
4. Accidental, intentional or malicious data loss
5. Attacks against network-connected devices

The training materials are available as PowerPoint slides (along with presenters' notes) and for use within a learning management system.

This training is intended for health care staff, security teams, and other departments that are on the front lines for protecting patient safety. The latter category may include board members charged with attention to risk issues.

C. Hospital Cyber Resiliency Initiative Landscape Analysis – Pdf (the Landscape Analysis)

This Landscape Analysis document analyzes the current state of cybersecurity preparedness by domestic hospitals. It includes a review of hospitals participating in the study, benchmarked against standard cybersecurity guidelines such as HICP 2023 and the National Institute of Standards and Technology Cybersecurity Framework.

The analysis was created through the partnership co-led by the Health Sector Coordinating Council Cybersecurity Working Group and the Centers for Medicare & Medicaid Services. This partnership was convened to conduct a review to better understand the state of cybersecurity within US hospitals.

The Landscape Analysis includes a review of the active threats attacking hospitals and the cybersecurity capabilities of US hospitals. Included within the Landscape Analysis are the results of investigations into 1) the tactics and techniques that threat actors use to compromise hospitals and 2) the current state of participating hospitals' cybersecurity resiliency (using the HICP as a framework).

The Landscape Analysis makes the following ten key observations, and provides detailed discussions with respect to the each:

1. Directly targeted ransomware attacks aimed to disrupt clinical operations are an outsized and growing cyber threat to hospitals;

2. Variable adoption of critical security features and processes, coupled with a continually evolving threat landscape, can expose hospitals to more cyberattacks;

3. Hospitals report measurable success in implementing email protections, which is a key attack vector;

4. Supply chain risk is pervasive for hospitals;

5. Medical devices have not typically been exploited to disrupt clinical operations in hospitals;

6. There is significant variation in cybersecurity resiliency among hospitals;

7. The use of antiquated hardware, systems, and software by hospitals is concerning;

8. Cybersecurity insurance premiums continue to rise;

9. Securing cyber talent with requisite skills and experience is challenging; and

10. Adopting HICP improves cyber resiliency.

CONCLUSION

Cybersecurity preparedness is a crucial component of managing risk in the modern health care system. The HICP 2023 resources should be reviewed by and incorporated into the cybersecurity programs of health care organizations of any size. We also recommend revisiting the role of your board with respect to cybersecurity in light of the 2022 comments from the US Cybersecurity & Infrastructure Security Agency, available here.

National Law Review, Volume XIII, Number 114