Hospitals In The Crosshairs: Managing Cybersecurity Risk (Part 1)

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

07/30/2018

From the recent headline-grabbing attacks on hospitals and municipalities, the specter of cybersecurity threats looms large. As a result, spending on cybersecurity initiatives is expected to reach $96 billion this year.[i] Hospitals have been specifically targeted because of their perceived wealth and the urgent need for access to patient data.

Reading the headlines, you may be tempted to throw up your hands in frustration, but don’t despair. There are steps to be taken to manage your risks, and these steps can help you regardless of where you are in your cybersecurity risk management efforts.

All hospitals need a cybersecurity risk management program integrated into their overall risk management and compliance structure. Whether you are just starting to establish a program or you have an existing plan in place, the steps below can guide you moving forward. Because the threat landscape is constantly evolving, coming back to these steps will be helpful to assure that your risk management efforts also evolve to address new threats, legal duties and solutions.

In this first article, we help you identify where your organization sits on the landscape of readiness and preparedness. In our next article, we walk you through concrete steps you can immediately employ to move your organization into compliance.

Understand the Legal Landscape

There is no single overarching set of “cybersecurity laws.” Notification requirements and liability for a cybersecurity intrusion can stem from a variety of authorities, such as the Office for Civil Rights in the Department of Health and Human Services for violations of the Health Insurance Portability and Accountability Act (HIPAA), the Centers for Medicare and Medicaid Services, the Federal Trade Commission, and even the Equal Employment Opportunity Commission. State authorities may also play a role.

So, when drafting and implementing a cybersecurity risk management program, you must first understand all the activities you perform and the data gathered during each activity. Then, determine which laws and regulations govern that data so that you can draft cybersecurity solutions, including a Cybersecurity Breach Response Plan, which comply with your specific legal requirements.

Perform Regular Vulnerability Assessments

Identify possible avenues of cybersecurity risk by performing a vulnerability assessment. Your goal is to identify areas where data is at risk of unauthorized access. These risk areas may include cloud-based data storage solutions, patient monitoring devices, insecure mobile devices or even an unencrypted laptop.

Several state and federal agencies have issued guidance for performing risk assessments, including the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity,[ii] and the Federal Trade Commission's guidance for testing for common vulnerabilities and using industry-accepted methods and technical and practice standards for securing data.[iii]

A vulnerability assessment will help you understand the potential risks posed by your operation. Repeat assessments should be done regularly as well because new threats are constantly appearing, leading to new and additional potential weaknesses in your data infrastructure.

Now that we have identified where you are, it's time to help you get where you need to go. Next week, we'll identify concrete steps you can immediately employ to move your organization into compliance.

Republished by permission. This article was originally written for and published in the Summer 2018 issue of Arkansas Hospitals magazine.

---

[i] Schick, Shane. https://securityintelligence.com/news/cybersecurity-spending-poised-to-rise-in-2018-gartner-reports/

[ii] https://iapp.org/media/pdf/resource_center/Krasnow_model_WISP.pdf

[iii] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf