2017

Cybersecurity Report Identifies Unique Challenges to Tackling Cybersecurity in Health Care

Deborah R. Farringer
Belmont University - College of Law

Recommended Citation

11 J. Health & Life Sci. L. 117 (2017)

AHLA

Journal of Health & Life Sciences Law

VOLUME 11, NUMBER 1 | OCTOBER 2017

FEATURED ARTICLES

NOTES AND COMMENTS

PRACTICE RESOURCE

BRIEF INSIGHTS

OFFICIAL JOURNAL OF AMERICAN HEALTH LAWYERS ASSOCIATION

Brief Insight

Cybersecurity Report Identifies Unique Challenges to Tackling Cybersecurity in Health Care

Deborah R. Farringer

After a year of deliberation, the Health Care Industry Cybersecurity Task Force (Task Force) issued a report regarding the preparedness of the health care industry to respond to ever increasing cybersecurity threats.[1] Formed under Section 1533 of the Cybersecurity Information Sharing Act of 2015 (CISA),[2] the Task Force was charged with examining cybersecurity risks specifically within the health care industry and further identifying who will lead and coordinate efforts, how divisions and subdivisions[3] will divide responsibilities, and how they will communicate amongst one another.[4]

With increasing incidents of large-scale data breaches due to hacking and growing occurrences of ransomware attacks across all industries, the U.S. Congress enacted the CISA to encourage the sharing of cyber threat information across various sectors in an effort to thwart, or at least diminish, the

[1] Health Care Indus. Cybersecurity Task Force, Report on Improving Cybersecurity in the Health Care Industry (June 2017), *available at* www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf [hereinafter Report].

[2] Cybersecurity Information Sharing Act (CISA) was passed as part of the Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (Dec. 18, 2015).

[3] HHS has eleven operating divisions, eight agencies within the U.S. Public Health Service, and three human services agencies. For a complete list, see *HHS Agencies & Offices*, HHS.gov, www.hhs.gov/about/agencies/hhs-agencies-and-offices/index.html (last visited July 3, 2017).

[4] 6 U.S.C. § 1533(b).

incidence of data breaches. While the sharing of information under the CISA is entirely voluntary, the CISA encourages sharing by preempting existing laws that stood as a barrier towards sharing by making such sharing ostensibly illegal, including privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).[5] Realizing the complexity and unique challenges of the health care industry, the Task Force brought together experts from various areas of the industry, including members who represent hospitals, insurers, patient advocates, security researchers, pharmacy and pharmaceutical companies, medical device manufacturers, health information technology developers and vendors, and laboratories.

Issued on June 5, 2017, the 96 page report identifies threats to the industry and provides a number of recommendations, along with accompanying action items, for what can be done to ensure the security of patient data and electronic health systems. The report acknowledges from the start that certain aspects of the industry are challenging. Regardless, the report states unequivocally that "health care cybersecurity is a key public health concern that needs immediate and aggressive attention."[6]

Among the challenges, the report identifies the following potential barriers: the expense of in-house information security personnel or IT staff; lack of infrastructure related to identification, tracking, and ability to prevent threats; lack of information regarding new technology threats; unsupported legacy systems (replete with vulnerabilities); lack of awareness regarding vulnerability; and historic low prioritization of cybersecurity. In response, the report identifies what it refers to as "six high-level imperatives by which to organize its recommendations and action items . . . :

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT.

[5] The Privacy Rule and Security Rule are combined in the HIPAA Administrative Simplification Regulations found at 45 C.F.R. §§ 160, 162, and 164.

[6] Report, at 2.

3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. Increase health care industry readiness through improved cybersecurity awareness and education.
5. Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.
6. Improve information sharing of industry threats, weaknesses, and mitigations."[7]

In preparation for the report, the Task Force consulted with sectors in the financial services, transportation, and energy industries. While there were some similarities, the Task Force quickly realized that health care organizations could not adopt wholesale any of these approaches due to existing infrastructure challenges. In addition, the "unique culture" of health care,[8] the manner in which the industry has adopted a digital platform, the complicated regulatory environment of the industry, the exceedingly variable size (and wealth capacity) of organizations, the vast amounts of patient data collected purposes unrelated to patient care, and the complex reporting vulnerabilities and breaches all serve as major barriers and reasons why the health care industry is unlike any other industry when it comes to combatting cybersecurity.

What then does the report recommend for health care entities given all of these unique barriers? First and foremost, the Task Force believes that the health care sector requires its own single source for sharing cybersecurity threats and a single reporting framework. The health care industry is simply too complex and too distinct from other industries to contemplate that cybersecurity could be addressed by a leader or frameworks across multiple industries. Importantly, the report identifies the Stark Law and the Anti-Kickback Statute as potential barriers to success and "strongly encourage[s]

[7] *Id.* at 21.

[8] *Id.* at 9. The report characterizes the culture as both a benefit because sharing information is already a vital and primary part of the culture of health care, and also a hindrance because the need for rotating staff to immediately access data on a 24/7 basis make the protection of such data difficult in clinical environments.

Congress to evaluate an amendment to these laws specifically for cybersecurity software that would allow health care organizations the ability to assist physicians in the acquisition of this technology, through either donation or subsidy."[9] Other specific recommendations include securing legacy systems; increasing lifecycle (from concept generation through disposal) security for electronic health records and medical devices; increasing training and education; establishing a Medical Computer Emergency Readiness Team; increasing IT staffing; creating more low-cost shared-savings program models to encourage more interface and collaboration across organizations; developing more assessment and evaluation tools; dedicating more research and development in this area; and simplifying and tailoring information for easier consumption when sharing.

The number of recommendations and the various areas for increased readiness makes it clear that cybersecurity in the health care sector will not be an easy task. Implementation will be extremely difficult to coordinate; the report makes clear that no one sector of the industry can begin the process of increasing readiness on its own. The report calls on lawmakers and policymakers, including the U.S. Congress and Centers for Medicare & Medicaid Services (CMS), to change laws and regulations to enable greater integration and provide greater protections. The report also calls on health care IT vendors to make certain improvements and updates regarding security of existing systems and legacy systems, medical device manufacturers to make improvements to existing devices to provide better security and integration, and providers and suppliers (among others) to increase training and IT support and dedicate more resources to achieve the constant vigilance required for cybersecurity.

Indeed, part of what the Task Force identified as why the health care industry needs a different approach to cybersecurity than in other industries—namely the complexity of the health care industry and its existing infrastructure—creates challenges in implementation of an effective cybersecurity response. Given that reality, what is the take away for anxious hospital administrators or insurance executives trying to figure out how best to prevent the next ransomware attack or massive medical records data breach? First, imple-

[9] *Id.* at 27.

mentation will require significant time and resources. Health care entities will need to acknowledge and plan for the "new normal" to include a robust IT staff and a larger percentage of the budget dedicated to maintenance and operation of electronic health records. Additionally, there must be a more concerted effort on the part of entities across the industry to think about IT and cybersecurity, approaching the challenge not as an individual issue—how can I protect *my* data—but as a coordinated effort. Entities will have to work together to make necessary structural and technical changes and adjustments and, given the current political environment, may have to make those changes independent of legal and regulatory amendments. The report is a helpful tool for identifying the areas that will require attention, but the difficult task of industry working across sectors to try to implement change has just begun. J

Deborah R. Farringer is Assistant Professor of Law at Belmont University College of Law where she teaches health law, business associations, health care fraud and abuse, health care business and finance, and biomedical ethics. Prior to joining Belmont University College of Law, Professor Farringer served as Senior Associate General Counsel in the Office of General Counsel at Vanderbilt University, where her practice focused primarily on transactional matters for Vanderbilt University Medical Center, including analysis of contracts for compliance with applicable health care laws such as the Stark law, Anti-Kickback Statute, civil monetary penalties law, the False Claims Act, physician practice acquisitions, joint ventures, general corporate governance and corporate maintenance issues, hospital operations, and real estate leasing and purchasing issues. Prior to joining Vanderbilt University, Professor Farringer was an associate at Bass, Berry & Sims PLC where she practiced in the firm's Healthcare Industry group. She also completed a judicial clerkship for Judge H. Emory Widener, Jr. of the United States Court of Appeals for the 4th Circuit in Abingdon, Virginia. Contact her via email at deborah.farringer@belmont.edu.