New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 60
TUESDAY, SEPTEMBER 26, 2017

HEALTH LAW

Expert Analysis

Cybersecurity in the Health Care Sector

By **Francis J. Serbaroli**

As if it were not facing enough challenges, the health care industry is now becoming a more frequent target for hacking and ransomware by miscreants both domestic and foreign. Health care organizations have lagged behind other business sectors in protecting data, which is hard to understand given the extreme sensitivity of the data in their possession: personal and health information on individual patients; confidential information on internal quality assurance, risk management and utilization; results of clinical research on drugs, medical devices, and therapies; personal information on employees; sensitive internal financial information; confidential information on potential partnerships and deals with other organizations; and so on. Of even greater concern is the reality that hackers can interfere with web-connected medical equipment and devices and physically harm patients.

The Health Care Industry Cybersecurity Task Force, which was established by Congress in 2015, is comprised of representatives from both the government and private sector, and is charged with analyzing and making recommendations regarding securing and protecting the health care sector against cybersecurity incidents. S.754—114th Congress: Cybersecurity Information Sharing Act of 2015. The Task Force recently issued its "Report on Improving Cybersecurity in the Health Care Industry" (Report). The Report highlights the vulnerabilities to cyberattacks of organizations involved directly or indirectly in providing health care services and products, and makes recommendations to both the government and the industry to enhance awareness and improve protections.

Industry

The Report begins by describing the industry as a "mosaic" of large health care systems, physician practices, public and private payors (e.g., Medicare, Medicaid, private insurers and plans), research institutions, medical device developers and manufacturers, software companies, as well as a large and diverse population of patients. It observes that the continuing evolution of electronic health records and the health care industry's extensive connectivity to the Internet have led to major improvements in both the quality and timeliness of patient care. The Report notes that the downside to these advances is that they have resulted in an increased attack surface for health care providers, medical device companies, and many other parts of the health care industry. The Report emphasizes that securing health care data as well as securing the operation of medical devices is essential to protecting patients and providing them with the highest level of medical care.

The Report makes recommendations to both the government and the industry to enhance awareness and improve protections.

Turning to the reality of cybersecurity and preparedness in the industry, the Report found that many health care organizations

> lack the infrastructure to identify and track threats, the capacity to analyze and translate the threat data they receive into actionable information, and the capability to act on that information. Many

FRANCIS J. SERBAROLI *is a shareholder in Greenberg Traurig and the former vice-chair of the New York State Public Health Council.*

organizations also have not crossed the digital divide in not having the technology resources and expertise to address current and emerging cybersecurity threats. These organizations may not know that they have experienced an attack until long after it has occurred.

As to regulatory oversight, the Report finds that multiple federal agencies play a role in establishing and policing how health care organizations secure the privacy of their health care information, which has the potential to create complications:

Some entities may be subject to regulation and oversight by multiple federal government entities, each with their own rules, which may be difficult to reconcile. Product and technology innovations for medical devices and health IT outpace the development and creation of regulations.

Then there is the cost of compliance: While many regulations that apply to cybersecurity in health care are well-meaning and individually effective, taken together, they can impose a substantial legal and technical burden on health care organizations. These organizations must continually review and interpret multiple regulations, some of which are vague, redundant, or both. In addition, organizations must dedicate resources to implement policy directives that may not have a material impact on reducing risks.

Recommendations

The Report includes six "high-level" imperatives, for each of which the Task Force provides a number of recommendations.

Imperative 1: "Define and streamline leadership, governance, and expectations for health care industry cybersecurity." To bring this about the Task Force recommends:

- creating a cybersecurity leader role within the U.S. Department of Health and Human Services (HHS) to align industry efforts for health care cybersecurity;
- establishing a consistent, consensus-based Cybersecurity Framework that is health-care specific, and includes standards, guidelines, and best practices;

The inherent vulnerabilities in the health care sector, together with the fact that health care will soon account for 20 percent of this country's gross domestic product, make it all the more attractive to cyberattackers, and virtually guarantee that the problem will only get more serious and more complicated.

- requiring federal regulatory agencies to harmonize existing and future laws and regulations that affect health care cybersecurity;
- identifying scalable best practices for governance of cybersecurity across the health care sector; and
- exploring potential changes to the Stark Anti-Referral Law (42 U.S.C. §1395nn), the Anti-Kickback Statute (42 U.S.C. §1320a-7b(b)), and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners (e.g., physician practices).

Imperative 2: "Increase the security and resilience of medical devices and health information technology." Specifically the Task Force recommends:

- securing legacy systems through compensating controls, device update, device retirement, network segmentation, etc.;
- improving manufacturing and development transparency among software developers and users;
- increasing the adoption and rigor of the secure development lifecycle (from concept generation through end of life recycling or disposal) in the development of medical devices and electronic health records;
- requiring strong authentication to improve identity and access management for health care workers, patients, medical devices and electronic health records;
- employing strategic and architectural approaches to reduce the attack surface for medical devices, electronic health records, and their interfaces; and
- establishing a Medical Computer Emergency Readiness Team to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures.

Imperative 3: "Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities." To that end, the Task Force recommends:

- requiring every health care organization to identify the cybersecurity leadership role (e.g., chief information security officer) for driving more robust cybersecurity policies, processes and functions, with involvement of senior executives;
- establishing a model for adequately resourcing the cybersecurity workforce with qualified individuals, and determining an acceptable ratio of health care cybersecurity expertise to the size

of the organization, complexity of care, degree of interconnectedness with other organizations, etc.;
- creating managed security service providers (MSSP) models to support small and medium-sized health care providers so they can have state-of-the-art security monitoring, defensive and reporting capabilities; and
- evaluating options for small and medium-sized health care providers to migrate patient records and legacy systems to secure environments such as hosted, cloud, and shared computer environments.

Imperative 4: "Increase health care industry readiness through improved cybersecurity awareness and education." The Task Force believes this can be accomplished by:
- developing education programs targeting executives and boards of directors about the importance of cybersecurity education;
- ensuring existing and new products/systems' risks are managed in a secure and sustainable fashion through "cybersecurity hygiene" (i.e., an evaluation of each individual's security practices and precautions when conducting activities online);
- establishing an assessment model for evaluating a health care organization's conformity with cybersecurity hygiene that regulatory agencies and industry can rely upon;
- customizing the Baldridge Cybersecurity Excellence Builder, a cybersecurity self-assessment tool created by the National Institute of Standards and Technology, for use by health care organizations;
- increasing outreach and engagement for cybersecurity across all levels of government and the private sector through a cybersecurity education campaign involving both HHS and the Department of Homeland Security; and
- providing patients with information on how to manage their health care data to enable them to make educated decisions when selecting services or products from non-regulated entities (e.g., fitness trackers, devices and other consumer health care/lifestyle products).

Imperative 5: "Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure." The Task Force recommends:
- developing guidance for industry and academia on creating economic impact analysis and loss for cybersecurity risk for health care research and development; and
- pursuing research into protecting health care "big data" sets.

Imperative 6: "Improve information-sharing about industry threats, risks, and mitigations." The Task Force outlined the following steps to accomplish this:
- make information-sharing on threats and risks easier among small and medium-size health care organizations that rely on limited or part-time cybersecurity staff;
- create more effective mechanisms for disseminating and utilizing data about threats, vulnerabilities and incidents; and
- encourage cybersecurity annual readiness exercises by the health care industry to prevent uncoordinated and ineffective responses to cyberattacks.

Conclusion

The Task Force's Report is a wake-up call to every organization in the health care sector, large or small. Cyberattacks are increasing and becoming even more dangerous. The inherent vulnerabilities in the health care sector, together with the fact that health care will soon account for 20 percent of this country's gross domestic product, make it all the more attractive to cyberattackers, and virtually guarantee that the problem will only get more serious and more complicated.

Health care organizations that do not recognize these dangers or take effective steps to mitigate them are not only doing a disservice to their patients or customers, they are risking their reputations and subjecting themselves to costly notification processes and remediation expenses, as well as regulatory crackdowns, class action lawsuits, significant penalties and legal liabilities, and the potential separation from employment of the senior executives on whose watch the problem occurred. Placed in that context, expenditures on appropriate cybersecurity protections look like a wise investment.