THOMSON REUTERS
Westlaw®

Task force report hopes to galvanize cybersecurity efforts in the health care industry

By Jodi Daniel, Esq., and Brandon C. Ge, Esq., ***Crowell & Moring***

JULY 25, 2017

In early June, the Health Care Industry Cybersecurity Task Force issued its final report to Congress titled Report on Improving Cybersecurity in the Health Care Industry. The long-anticipated report describes the task force's findings regarding health care cybersecurity, which it describes as a "key public health concern that needs immediate and aggressive attention."

The report outlines six imperatives to bolster cybersecurity in the health care industry, citing the lack of security talent and the rampant use of legacy technologies as two of the top cybersecurity issues in the industry. According to the report, achieving these imperatives will require action from both the government and industry stakeholders.

Given recent high-profile incidents affecting the health care industry, we strongly advise health care clients to review their cybersecurity practices and align them with those recommended in the report where practicable.

THE TASK FORCE

The task force was formed to identify and make recommendations regarding challenges in the health care industry in securing and protecting itself against cybersecurity incidents. The task force is composed of various government and private stakeholders ranging from device manufacturers to hospitals, including the Chief Information Security Officer of the Centers for Medicare and Medicaid Services.

Established in accordance with the Cybersecurity Act of 2015, the task force has been directed to:

- Analyze how other industries have implemented strategies and safeguards to address cybersecurity threats.
- Analyze challenges and barriers private entities in the health care industry face securing themselves against cyberattacks.
- Review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record.
- Provide the Secretary of HHS with information to disseminate to the health care industry for purposes of improving their preparedness for, and response to, cybersecurity threats.
- Establish a plan for creating a single system so that the federal government and health care industry stakeholders may share actionable cyber threat indicators and defensive measures in real time.
- Report to Congress on the findings and recommendations of the task force.

THE ISSUES

According to the report, the health care industry suffered more breaches stemming from cyberattacks than any other industry in 2015. Cybersecurity has been particularly challenging in the health care industry for a myriad of reasons.

For one, as described in the report, availability of information is paramount to support the primary mission of health care — patient treatment — but allowing easy, prompt access to patient information may come at the expense of security measures implemented throughout other industries.

> Hospitals do not know which kind of surgery might be proper for a given patient or when it might be appropriate to use a specific medical device.

Implementing security measures that slow down access, such as dual-factor authentication, means lost time that could be spent treating patients, according to the report.

This, the report explained, may lead to health care facilities with workstations left unattended, virtually unfettered physical access to workstations, and passwords written down on paper.

The dearth of resources is another major reason for the cybersecurity problem in health care. A large portion of the health care industry consists of small- and medium-sized organizations with limited or non-existent funding and staffing devoted to cybersecurity.

Such organizations do not have the resources to address cybersecurity threats, and many such organizations may not even know that they have experienced an attack until long after it has occurred.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Larger organizations suffer from insufficient staffing as well, as noted in the report. The larger the organization, the more security staffing is needed to protect the larger attack surface area. In particular, affiliate sites of larger organizations often lack sufficient IT resources.

According to the report, there is also a "multiplicity of actors" in health care cybersecurity, each with its own rules, creating a "significant legal and technical burden on health care organizations" when instead there should be a "single source for industry to go for authoritative clarification, explanation, and guidance."

Although many health care workers assume that their level of cybersecurity vulnerability is low, recent high-profile incidents have demonstrated this to be false. For example, the WannaCry ransomware attack in May put a bright spotlight on the susceptibility of health care organizations across the globe to cyberattacks and especially highlighted the shortcomings of legacy systems, which unfortunately are still prevalent in the U.S. health care industry.

Such vulnerabilities can dramatically interrupt patient care and therefore need to be a higher priority for the health care industry. The task force expressed its goal that the report galvanizes both the public and private sectors to comprehensively address cybersecurity challenges in order to protect patients.

IMPERATIVES AND RECOMMENDATIONS

The report outlines six overarching imperatives that the task force believes must be achieved to improve security in the health care industry:

- Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
- Increase the security and resilience of medical devices and health IT.
- Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
- Increase health care industry readiness through improved cybersecurity awareness and education.
- Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
- Improve information sharing of industry threats, risks, and mitigations.

The report is incredibly comprehensive and includes over 100 recommendations and action items to address the six aforementioned imperatives.

These recommendations target a variety of entities, including the federal government, regulatory and legislative entities, health care industry stakeholders, and public-private partnerships. While some recommendations apply only to certain health care subsectors, others have value for the entire industry.

Some notable recommendations include the following:

- HHS should create a centralized position within the agency to coordinate health care cybersecurity efforts.
- Together, HHS and NIST should establish a health care-specific version of the NIST Cybersecurity Framework.
- Congress should scale back constraints imposed by the Stark Law, Anti-Kickback Statute, and other fraud and abuse laws that discourage larger health care organizations from assisting physicians in acquiring cybersecurity resources.
- Legacy systems should be phased out.
- The FDA and other stakeholders should encourage security and privacy by design in medical devices.
- Stakeholders should strengthen their authentication controls for health care workers, patients, medical devices, and electronic health records.
- The industry should make more concerted efforts to develop and support the cybersecurity postures of smaller and under-funded entities.

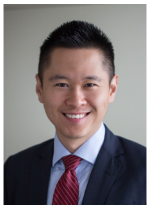
The report contains valuable observations on the state of health care cybersecurity. Many of the report's recommendations have been well-received, especially the recommendations to develop a health care-specific cybersecurity framework, encourage greater threat information sharing, and address the shortage of cybersecurity professionals.

As the industry trends towards more interoperability, the frequency and impact of cyberattacks will only grow. Thus, we advise our health care clients to review the report and consider implementing its recommendations.

More importantly, health care cybersecurity incidents are likely to increase. We recommend that health care entities review their cybersecurity policies and practices, and make improvements in light of recent cybersecurity incidents and guidance from government.

This article appeared in the July 25, 2017, edition of Westlaw Journal Medical Devices.

ABOUT THE AUTHORS



Jodi Daniel (L) is a partner at **Crowell & Moring** in Washington and leads the digital health practice. Previously, Daniel was the founding director of the Office of Policy in the Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. She helped spearhead important policy changes in health information privacy and health information technology and was one of the key drafters of the original HIPAA privacy rules. **Brandon C. Ge (R)** is an associate in Crowell & Moring's privacy and cybersecurity group and health care group in Washington. Ge advises clients on a wide range of privacy and cybersecurity laws, regulations, and standards. His practice has a particular focus on advising clients — from startup digital health companies to large health plans — on all aspects of compliance with the HIPAA privacy and security regulations. This expert analysis was first published on the firm's website June 28. Republished with permission

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.