VIEWPOINT

Cybersecurity—A Serious Patient Care Concern

Mark P. Jarrett, MD, MBA, MS
Northwell Health, New Hyde Park, New York; and Hofstra Northwell School of Medicine, Hempstead, New York.

The world of paper medical records has almost disappeared, ushering in a new era of electronically stored, analyzed, and shared medical information that offers exciting opportunities for improved patient care. However, this major shift in information management has introduced unintended and unfavorable consequences, such as theft of patient-protected health information, wide-scale sequestering of medical records by ransomware (malicious software—malware—that permanently blocks the access to records unless a ransom is paid), and the ability for hackers to directly harm patients. For example, the recent global WannaCry ransomware attack resulted in more than 48 National Health Service organizations in the United Kingdom being forced to cancel surgical procedures and outpatient appointments. This virus also affected several intravenous contrast power injectors in the United States.[1] In addition to health care organizations, more than 230 000 computers in 150 countries were infected.

Health care practitioners and institutions are learning about new terminology and jargon: WannaCry and Petya, the 2 most recent malware viruses that have affected clinicians and health care institutions globally. The potential consequences of these cybersecurity risks on the health care industry (1 of the 16 critical infrastructure sectors defined by the Department of Homeland Security) prompted Congress to establish the Health Care Industry Cybersecurity Task Force (HCIC) as part of the *Cybersecurity Act of 2015*.[2] To meet the increasing challenges of cybersecurity to the health care industry, the HCIC was charged with 6 specific tasks that resulted in the publication of the *Report on Improving Cybersecurity in the Health Care Industry* in June 2017.[3] The HCIC consisted of 21 members representing the federal government, hospitals, insurers, patient advocates, information technology (IT) specialists, clinicians, medical device manufacturers, and software developers. As part of the background, information briefings were held for the task force by other industry sectors, such as finance, transportation, and energy.

> On the individual level, clinicians must practice cyber hygiene.

In the comprehensive report, the HCIC outlined the following 6 critical recommendations (with additional subrecommendations):

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.
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.

Physicians, as well as others in the health care industry, have historically considered IT issues as an IT problem. Problems such as connectivity, usability, and even short-term down times are events that affect efficiency and satisfaction, but they are usually not viewed as major risks to patient care. However, the era of electronic health records has now created the possibility of new significant risks for patients. Theft of patient medical information is a potentially valuable commodity on the dark web, a group of websites that allows anonymous access to sites often associated with illegal activities. This stolen information not only can be sold for financial gain, but also can be used by other individuals to receive medical care, providing an opportunity for intermingling of medical information that can alter an allergy history, medication list, or other critical elements of a patient's history. This vulnerability can undermine public trust and prompt patients to withhold sensitive but needed information about medical history.

Ransomware also can sequester huge data files, making patient care difficult for extended periods. A large-scale denial of service attack, in which a network is purposefully overloaded with false requests, can substantially interfere with health care clinicians' activities by preventing access to electronic health records. Coupled with a mass casualty event, such as the Boston Marathon bombing, a denial of service cyber attack that prevents access to medical records, laboratory reports, and radiology results could amplify the disaster, possibly contributing to increased morbidity and mortality. Outdated software in an infusion pump or implantable device can allow hacking of these devices and potentially lead to patient harm or possibly death. This was highlighted in a recent report that used a simulation scenario to demonstrate the risk to patients.[4] The scenario revealed what could occur if an infusion pump was illegally accessed and medications were delivered in potentially lethal doses. Cybersecurity is clearly a patient care issue.

Health care is an industry that can be described as a mosaic with many components fitting together with a goal to ensure seamless delivery of high-quality, safe health care. The components differ more than just by the services delivered. The US health care system consists of large health systems, academic medical centers, stand-alone hospitals, small critical access hospitals, long-term care facilities, large- and medium-sized

Corresponding Author: Mark P. Jarrett, MD, MBA, MS, Northwell Health, 2000 Marcus Ave, New Hyde Park, NY 11042 (mjarrett@northwell.edu).

physician practices, and small practices of 1 to 3 physicians. In addition, the health care system includes nonclinical organizations such as the pharmaceutical industry and medical device manufacturers. Recent events have underscored the vulnerabilities of larger health care institutions, many of which scrambled for days to protect themselves from WannaCry. With the subsequent Petya malware attack several weeks later, many hospitals were unable to use the Nuance-based dictation service, some hospitals were forced to revert to paper records, and Princeton Community Hospital in rural West Virginia has replaced its entire computer system.[5]

The HCIC did address issues related to small hospitals and physician practices. These organizations have neither the resources to prepare for a cyber attack nor a robust ability to respond to one. The HCIC had extensive discussions regarding this issue and made recommendations for Congress to modify antikickback and similar statutes to allow the sharing of expertise by larger systems (perhaps as regional consortiums) with smaller health care organizations without the risk of being accused of inurement. There is already a precedent with health systems supplying electronic health record software for a reduced cost if there was to be future sharing of data for meaningful use and performance improvement. Even if physicians or small hospitals could afford to buy the level of security expertise needed, which they cannot, there is a national shortage of that expertise. This resource gap was also addressed in the HCIC report.

What should clinicians do to help protect patients? On the individual level, clinicians must practice cyber hygiene.

They should not object to having to change passwords on a regular basis, and they should use passwords that are strong. They should be wary of email phishing, a common portal of entry for hackers. Vulnerabilities, such as nonupdated software, must be mitigated; cybersecurity software must be deployed; and suspicious network activity needs to be reported. Clinicians should never assume that because their practice or organization is small, they will not be a target of hackers and malware. Advocating for adequate resources is also important. It is the professional duty of physicians to be advocates for patients and comprehensively address this situation. The promise of improved care from a digital world will be broken and patients could be placed at risk if cybersecurity is not made a priority issue.

ARTICLE INFORMATION

Published Online: September 25, 2017. doi:10.1001/jama.2017.11986

Conflict of Interest Disclosures: The author has completed and submitted the ICMJE Form for Disclosure of Potential Conflicts of Interest and none were reported.

Disclaimer: This Viewpoint does not necessarily reflect the views of the Health Care Industry Cybersecurity Task Force or others who served on the group for this report.

Additional Information: Dr Jarrett served as the physician representative for the Report on Improving Cybersecurity in the Health Care Industry.

REFERENCES

1. Fox-Brewster T. Medical devices hit by ransomware for the first time in US hospitals. *Forbes*. http://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#2aa061d7425c. Accessed June 15, 2017.

2. US Department of Homeland Security. Critical infrastructure sectors. https://www.dhs.gov/critical-infrastructure-sectors. Accessed June 1, 2017.

3. Health Care Industry Cybersecurity Task Force: report on improving cybersecurity in the health care industry. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf. Published June 2, 2017. Accessed June 11, 2017.

4. Fears of hackers targeting hospitals, medical devices. ABC News. http://abcnews.go.com/Nightline/video/fears-hackers-targeting-hospitals-medical-devices-48343190. Accessed July 17, 2017.

5. Davis J. West Virginia hospital replaces computers after Petya cyberattack. *Healthcare IT News*. http://www.healthcareitnews.com/news/west-virginia-hospital-replaces-computers-after-petya-cyberattack. Accessed July 17, 2017.