American Hospital Association

800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100 Phone
www.aha.org

Statement

of the

American Hospital Association

for the

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

of the

U.S. House of Representatives

"Cybersecurity in the Heath Care Sector: Strengthening Public-Private Partnerships"

April 4, 2017

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to submit for the record our comments on information security in the health care field.

Hospital and health system leaders recognize that data held by health care organizations is highly sensitive, as well as valuable, and are taking cybersecurity challenges extremely seriously. The vast majority of hospitals already are taking many important security steps to safeguard data while they continue to enhance their capabilities. A variety of private organizations have been formed to facilitate information sharing and proactively prevent cyber attacks. Such efforts have been effective and should receive ongoing support and encouragement to develop actionable information and tools.

Hospitals and health care providers also work with a variety of federal agencies and law enforcement to respond to and prevent cyber attacks. Law enforcement should be given the resources necessary to share information proactively, to conduct investigations and to assist victims and targets, particularly those who are most vulnerable. The field also is actively regulated through the Health Insurance Portability and Accountability Act (HIPAA) Security

Rule and related enforcement actions. Although attacks will occasionally succeed, the victims should be given support and not be presumed to have been at fault.

HOSPITALS AND HEALTH SYSTEMS ARE ACTIVELY PROTECTING THEIR ASSETS

Hospitals and Health Systems Take Their Responsibility to Secure Systems Seriously

The health care field is increasingly realizing the promise of networked information technologies to improve quality and patient safety and bring efficiencies to our business systems. But with those opportunities come vulnerabilities to theft and threats to the security of personal information for patients and employees, billing records—even the function of medical devices. Increasingly, bad actors are using phishing emails, malicious malware, and other tactics to attempt to attack hospital computers, networks, and connected devices.

Recently publicized attacks include the use of ransomware—software that holds computers hostage through malicious usage of encryption until a ransom is paid. Other attacks may be motivated by a desire to steal data from a health care system, such as individual medical, financial or other identity information that can be monetized. In some cases, health care organizations may have intellectual property that is of interest to others, such as clinical trial data, medical research data or information on high-profile patients.

Recognizing that much of the data held by health care organizations is highly sensitive, as well as valuable, hospital and health system leaders take cybersecurity challenges extremely seriously and understand that protecting patients and their personal data is a 24/7 responsibility.

Hospitals and Health Systems are Taking Specific Steps to Secure Systems

As a result of the sensitive information used throughout health care organizations, hospitals are diligently working to defend and improve the security of their networks by implementing safety measures, testing, maintaining back-ups and deploying the latest upgrades. They also are encrypting networks and workstations. Many hospitals conduct annual threat assessments and work to identify vulnerabilities through extensive penetration testing. Increasingly, hospitals and health systems are conducting cybersecurity "tabletop" exercises or other simulations to assess their readiness to respond in the event of an actual attack.

Results from a 2016 AHA survey show that the majority of hospitals already are taking many important security steps while they continue to build out their capabilities.[1] For instance, more than 80 percent of hospitals have implemented intrusion detection systems; similarly, 80 percent also use encryption on their wireless networks, mobile devices and removable media. Moreover, more than 90 percent of hospitals require the use of strong passwords, require passcodes on mobile devices, encrypt laptops and/or workstations, at least annually perform a risk analysis to identify compliance gaps and security vulnerabilities, and at least annually undergo an infrastructure security assessment.

---

[1] *See* http://www.hhnmag.com/mostwired

Hospitals and Health Systems are Engaging in Information Sharing, but More Law Enforcement Assistance is Needed

Despite hospitals' concerted attempts to secure their ecosystem, individual efforts to secure systems are insufficient to prevent all attacks. Hospitals and health care providers are, therefore, working together at the national level to share information and best practices relating to cybersecurity. Information sharing allows organizations to stay ahead of emerging cybersecurity risks and contribute to collective knowledge of threats to guard against. Several private sector entities, such as the Nation's Healthcare and Public Health Information Sharing and Analysis Center (NH-ISAC) and Health Information Trust Alliance (HITRUST), provide information-sharing opportunities. In addition, the federal government has provided information-sharing resources through its cybersecurity initiatives, including health care and public health facilities. The Cybersecurity Act of 2015 provided a mechanism for information sharing among private-sector and federal government entities and provides a safe harbor from certain liabilities related to that information sharing. With that said, the increased information sharing is not yet a reality, and expedited and tailored cyber threat information sharing from the federal government would benefit all health care and public health organizations. Providers most need actionable information that identifies specific steps they can take to secure against new threats. Large volumes of more generalized information can prove challenging to interpret, and even become a distraction.

For its part, the AHA has a dedicated cybersecurity web hub that includes many resources that can help hospital leaders better understand cybersecurity threats and incorporate cyber risk reduction and response into their strategic priorities. The webpage also includes links to recent cybersecurity alerts. We also have developed audio and video resources on specific topics, such as what to do when an attack happens, the importance of staff training and ransomware.

The federal government is working to provide more educational and other resources to the health care field overall. The recently formed Healthcare Industry Cybersecurity Task Force is charged with better understanding the cyber needs of the health care field and identifying helpful resources. We look forward to hearing the task force's recommendations, which are expected to be released in an upcoming report to Congress. These steps are critically important, as are measures to identify, disrupt and apprehend the bad actors. As a nation, we must bolster the security of our ecosystem, not just place the burden on individual institutions.

Hospitals and Health Systems Will Maintain Continued Vigilance and Support

Cyber threats will continue, but ongoing vigilance by the health care field and active pursuit of bad actors by law enforcement can mitigate the problem. As the threats grow, we will need continued support for health care entities, particularly those with the fewest resources. The AHA and its members work in close partnership with the Department of Health and Human Services (HHS) Assistant Secretary for Preparedness and Response, Federal Bureau of Investigation, Food and Drug Administration, and other federal partners. These agencies must be given the resources to not only respond to attacks, but help vulnerable health care targets prevent attacks from occurring or succeeding, on an ongoing basis.

HIPAA Security Rule Provides Comprehensive Standards for Hospitals and Health Systems

From a regulatory point of view, health care entities already have significant obligations under the HIPAA security rule. That rule established a national set of security standards for protecting certain health information that is held or transferred in electronic form. The HHS Office for Civil Rights (OCR) has responsibility for enforcing the Security Rule with civil monetary penalties for violations. OCR has exercised this power in the past and remains a very active regulator. Failure to comply with HIPAA also can result criminal penalties, and OCR may refer a complaint to the Department of Justice for investigation.

Victims of Cyber Attacks Should be Given Assistance, Not Blame

Despite complying with rules and implementing best practices, hospitals and health care providers will continue to be the targets of sophisticated attacks, and some will inevitably succeed. Whether exploiting previously unknown vulnerabilities or taking advantage of an organization with limited resources, attackers will continue to be successful. The victims of attacks should be given support and resources, and attackers should be investigated and prosecuted. Merely because an organization was the victim of a cyber attack does not mean that the organization itself was in any way fault or unprepared. Similarly, a breach does not necessarily equate to a HIPAA Security Rule compliance failure. Instead, successful attacks should be fully investigated, and the lessons learned should be widely disseminated to prevent the success of similar attacks in the future.

CONCLUSION

We appreciate the opportunity to provide these comments and support the subcommittee's efforts and attention to examining the issues concerning cybersecurity in the health care sector. Hospitals and health care providers are making great strides in securing their systems and sharing information to prevent and mitigate attacks. We urge Congress to provide law enforcement and other appropriate agencies with the resources to investigate cyber attacks, and proactively prevent them.