American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

March 22, 2019

The Honorable Mark Warner
United States Senate
703 Hart Senate Office Building
Washington, DC 20510

RE: Reducing cybersecurity vulnerabilities in the health care sector

Dear Senator Warner:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, 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 respond to your letter regarding cybersecurity in the health care sector.

Hospital and health system leaders recognize the information and resources held by health care organizations are highly sensitive and valuable, and they are taking cybersecurity challenges extremely seriously. They have implemented important security steps to safeguard clinical technologies and information systems while they continue to enhance their data protection capabilities. And hospitals and health systems have made great strides to defend their networks, secure patient data, preserve the efficient delivery of health care services and, most importantly, protect patient safety.

The AHA has focused its efforts on providing up-to-date cybersecurity information – for both technical and non-technical audiences – to our member hospitals and health systems. This information assists hospitals and health systems as they face the continuing challenges of ensuring the privacy and security of patients' health care data in an environment of increasingly networked technology and expanded connectivity that offers significant benefits for care delivery, but also increases the potential for exposure to possible additional cybersecurity threats.

As the global WannaCry ransomware attack in 2017 underscored, the cybersecurity risks hospitals and health systems continue to face include the extent to which medical devices are vulnerable to threats and, in turn, can create serious risks for the security of hospitals' overall information systems and the delivery of patient care.

Below, we discuss our efforts to assist members with cybersecurity risk reduction and mediation, as well as federal government efforts to stimulate and promote additional cybersecurity risk reduction strategies to the health field. We also offer recommendations for reducing cybersecurity vulnerabilities in health care.

AHA Efforts to Address Cybersecurity

Cyber threats are a major risk issue for hospitals and health systems. The AHA began raising awareness on cybersecurity issues in 2014 with resources directed at both hospital and health system leaders and trustees.

In 2018, the AHA expanded on its provision of educational opportunities for members, and we now also provide them with targeted and customized information, including strategic cybersecurity and risk advisory services. Specifically, the AHA created a new role, senior advisor for cybersecurity and risk, to assist the field. We hired a nationally recognized health care cybersecurity expert who has nearly 30 years of highly-accomplished service with the Federal Bureau of Investigation (FBI).

The AHA offers many cybersecurity education opportunities to hospital and health system leaders, including both in-person and web-based presentations discussing specific cybersecurity topics. We have prioritized raising awareness for board members, hospital leaders and staff, in addition to providing information to technical audiences. In addition, the AHA reviews government policy, regulation and legislation to provide analysis pertaining to cybersecurity and risk implications for hospital and health systems. We monitor pending criminal and national security investigations and liaise with law enforcement and the intelligence community, as needed. The AHA also offers support and advice to members during ransomware and extortion incidents, including communications and response to adversaries.

The AHA has worked closely with federal government partners to help increase the coordination and sharing of information to identify possible vulnerabilities and prevent attacks on hospitals. The AHA serves as both a distribution channel to disseminate threat information, as well as a conduit to federal agencies and departments highlighting hospitals' and health systems' on-the-ground experiences. This was especially important during the WannaCry attack when the AHA provided critical information to many government partners regarding the impact on the health care sector.

Federal Government and Private-sector Efforts to Address Cybersecurity

Both Congress and the Administration have worked to address cybersecurity vulnerabilities in recent years. There are numerous efforts underway in several departments and agencies. The Administration has used executive orders to name 16 critical infrastructure sectors ─ including health care and public health ─ deemed

essential to the security of the nation and directed federal agencies to prioritize securing federal systems.

The Department of Health and Human Services (HHS) is designated as the liaison for the health care sector. More broadly, the FBI has been designated as the lead authority on investigating cybercrime. Other agencies, including the Department of Homeland Security (DHS) and the Secret Service, also play key roles in combatting cybercrime and providing guidance. Coordination across these federal agencies is critical to ensure threat intelligence and defensive strategies are shared widely, effectively and in a timely manner. In addition, these agencies must be given the resources to not only respond to attacks, but help vulnerable health care targets prevent attacks from occurring and succeeding.

The Cybersecurity Information Sharing Act of 2015 (CISA) allowed for information sharing among private-sector and federal government entities and provided a safe harbor from certain liabilities related to that information sharing. Information sharing is a critical way to help prevent future attacks by allowing organizations to share real-time threat information. Several private-sector entities, such as the Health Information Sharing and Analysis Center (H-ISAC) and Health Information Trust Alliance (HITRUST), provide information-sharing opportunities for organizations. The Health Sector Coordinating Council Joint Cybersecurity Working Group, which the AHA participates in, also serves an important role in bringing stakeholders together and coordinating across public and private sectors.

In addition, the federal government has provided information sharing resources through its cybersecurity initiatives, including health care and public health facilities. With that said, the goals of information sharing have yet to be fully realized. Expedited and tailored cyber threat information sharing from the federal government would benefit all health care and public health organizations. Providers 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.

In September 2018, the Administration released the National Cyber Strategy to address the larger cyber ecosystem. Action is needed to address the cybersecurity challenges facing all sectors, including health care. As a nation, we must bolster the security of our cyber ecosystem, not just place the burden on individual institutions. The magnitude of the challenges and the growing sophistication of the attacks suggest that the federal government must provide additional resources.

Department of Health and Human Services. Under CISA, HHS is directed to work with the private sector and other federal agencies to establish voluntary, consensus-based best practices. To carry out this directive, HHS convened the Health Care Industry Cybersecurity (HCIC) Task Force in March 2016 to examine the cybersecurity challenges in the health care sector and determine recommendations to address them.

The following year, the Task Force released a report detailing six areas of focus along with recommendations for both public and private partners to increase security in the health care sector. In addition, in 2017, HHS convened the CISA 405(d) Task Group to align industry approaches by developing a common set of voluntary, consensus-based, and industry-led guidelines, practices, methodologies, procedures and processes that health care organizations can use to enhance cybersecurity. The group is comprised of more than 150 members from both the public and private sector, including the AHA.

In January 2019, the task group released the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients to help continue to raise awareness and provide best practices. The Health Industry Cybersecurity Practices provides essential guidance for organizations of varying size and resource level to mitigate cybersecurity threats. HHS also opened the Health Sector Cybersecurity Coordination Center (HC3) in October 2018 to coordinate activities across the sector and report threats, profiles and preventive strategies to DHS.

Food and Drug Administration (FDA). The FDA provides oversight to ensure that medical devices are safe and effective. As a regulator, FDA has a leadership role in creating expectations that manufacturers proactively minimize risk by building security into products by design, providing security tools to their end-users, and updating and patching devices as new intelligence and threats emerge. Manufacturers must share with end-users the responsibility for safeguarding the confidentiality of patient data, maintaining data integrity, and ensuring the continued availability and functionality of the device system itself.

While no actions can completely eliminate cybersecurity risks from health care, swift action by FDA to improve the security of legacy and new medical devices will aid in reducing significant sources of vulnerability. We were pleased to see FDA include cybersecurity steps in its May 2018 Medical Safety Action Plan and release a draft of new pre-market authority requiring manufacturers to build capability to update and patch device security into product design and providing a “Software Bill of Materials” that identifies the information technology solutions in a device so that end-users can better manage the devices. It also included consideration of new post-market authority to require manufacturers to adopt policies and procedures for coordinated disclosure of vulnerabilities when they are identified. In our comments to the agency, we noted that the outlined steps would make important improvements to FDA’s oversight of medical device manufacturers with respect to the security of their products and offered suggestions for improvement. The AHA also urged FDA to move as quickly as possible to implement these steps and make public its timeline for the benefit of all stakeholders.

FDA also has worked collaboratively with the private sector to advance medical device security. In January 2019, the Healthcare and Public Health Sector Coordinating Councils released the Medial Device and Health IT Joint Security Plan as a result of the recommendation in the 2017 HCIC Task Force report. It will be important to continue this work.

AHA Recommendations to Reduce Cybersecurity Vulnerabilities in the Health Care Sector

The AHA supports recommendations included in the HCIC report, particularly continuing to increase the security and resilience of medical devices and developing the health care cybersecurity workforce capacity. We also support the development of a safe harbor to protect HIPAA-covered entities that have complied with cybersecurity best practices and making sure victims of attacks receive support and resources while enforcement efforts are focused on investigating and prosecuting the attackers. Additional recommendations in certain areas follow.

Medical Devices. A health system can have tens of thousands of devices from hundreds of manufacturers connected to its network, leading to significant security management challenges. Legacy devices remain a key vulnerability for hospitals and health systems. Given their useful lifespans, many legacy devices were not built with cybersecurity in mind and may use outdated or insecure software, hardware and protocols, leaving them vulnerable to attack. To remediate this problem, manufacturers must support end-users in providing a secure environment for safe patient care. This support should include wrapping security precautions around these devices, adding security tools and auditing capabilities where possible, conducting regular updates and patching all software, and communicating security vulnerabilities quickly through consistent channels.

While FDA has released both pre- and post-market guidance to device manufacturers on how to secure systems, and released updated pre-market guidance for comment, there are still concerns surrounding legacy devices and supported lifetimes that have yet to be resolved. Given that legacy devices have already been sold, there is little incentive for manufacturers to address the security of their installed base of products. FDA must make clear that security measures to protect legacy devices are required, not optional. Last year, we provided detailed comments to the House Committee on Energy and Commerce with additional recommendations on the security of legacy medical devices.

Workforce. Hospitals and health systems have emphasized the challenges they face in securing their information systems, given the limited financial resources they have to devote to cybersecurity and the current cybersecurity workforce shortages. These challenges are even more acute for smaller and rural facilities. As discussed earlier, recommendations to address this concern were included in the June 2017 HCIC Task Force report. These recommendations discuss the need for the Administration and Congress to provide resources and programs to increase and improve the cybersecurity workforce in health care and to address the challenges of small and rural facilities. The AHA would support developing and promoting workforce training programs specific to cybersecurity in health care, as well as funding for targeted internships or other programs to place cybersecurity professionals in small and rural facilities.

Safe Harbor. Despite complying with HIPAA rules and implementing best practices, hospitals and health care providers will continue to be the targets of sophisticated cyberattacks, and some attacks will inevitably succeed. Whether exploiting previously unknown vulnerabilities or taking advantage of an organization with limited resources, attackers will continue to be successful. The AHA believes that victims of attacks should be given support and resources, and enforcement efforts should rightly focus on investigating and prosecuting the attackers. Merely because an organization was the victim of a cyberattack does not mean that the organization itself was in any way at fault or unprepared. Similarly, a breach does not necessarily equate to a HIPAA security rule compliance failure. Moreover, an aggressive regulatory enforcement approach could be counter-productive and hinder valued cooperation by the victims of cyberattack with other parts of the government, such as DHS, FBI and the intelligence community. Instead, successful attacks should be fully investigated, and the lessons learned should be disseminated widely to prevent successful similar future attacks.

We urge the HHS Office of Civil Rights (OCR) to consider ways to develop a safe-harbor for HIPAA-covered entities that have shown, perhaps through a certification process, that they are in compliance with best practices in cybersecurity, such as those promulgated by HHS, in cooperation with the private sector, under section 405(d) of the CISA. Those best practices were developed through broad public/private collaboration after months of deliberation and development. A safe harbor would give covered entities clarity about the level of diligence they need to exercise, including when they agree to share and exchange protected health information with other systems/organizations through tools like health information exchanges, to avoid OCR enforcement when an attacker gains access.

General Cyber Defenses. In addition to activities specific to the health care sector, the AHA supports efforts to bolster nationwide cyber defenses. These include building capacity and devoting federal resources to:

- Develop and disseminate coordinated national defensive measures, both within government and to the private sector.
- Identify and disrupt bad actors through law enforcement activities.
- Increase the consequences for those who commit cybercrimes.
- Identify and support best practices by the private sector.

CONCLUSION

Hospitals and health systems have made great strides to defend their networks, secure patient data, preserve the efficient delivery of health care services and, most importantly, protect patient safety. The AHA supports improving the cybersecurity of

medical devices to help reduce vulnerabilities, increasing the cybersecurity workforce to ensure needed experts can help prevent attacks, and the developing of a safe harbor to give reassurance to facilities with exemplary cyber practices. The AHA is pleased to continue sharing information from the field to help the federal government effectively combat cyber threats. We look forward to working with you and others in Congress to reduce cybersecurity vulnerabilities in the health care sector.

Thank you for the opportunity to comment and for your leadership on this issue. Please contact me if you have questions or feel free to have a member of your team contact Mark Seklecki, vice president of political affairs, at mseklecki@aha.org or (202) 626-2341.

Sincerely,

/s/

Thomas P. Nickels
Executive Vice President