American Hospital Association

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

May 31, 2018

The Honorable Greg Walden
Chairman
Energy and Commerce Committee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone, Jr.
Ranking Member
Energy and Commerce Committee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Gregg Harper
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Diana DeGette
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
2125 Rayburn House Office
Washington, DC 20515

RE: Supported Lifetimes Request for Information.

Dear Chairman Walden, Ranking Member Pallone, Chairman Harper and Ranking Member DeGette:

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 respond to the Energy and Commerce Committee's request for information (RFI) on how best to keep medical devices secure over their useful lifetimes and, specifically, "legacy technology challenges, opportunities, considerations and suggestions in the health care sector."

Hospital and health system leaders recognize that the information and resources held by health care organizations are highly sensitive, as well as valuable, and are taking cybersecurity challenges extremely seriously. The vast majority of hospitals are taking important security steps to safeguard clinical technologies and information systems while they continue to enhance their data protection capabilities (details on the steps hospitals are taking can be found at www.aha.org/cybersecurity). However, last year's global WannaCry ransomware attack underscored the cybersecurity risks hospitals and health systems face, including 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. Medical devices are vital to patient care, can hold and transmit sensitive data, and also may serve as an

entry point to expose the entire environment of a health system to a security risk. This could impact not just the security of sensitive information, but also the performance of medical devices that are life-sustaining, such as anesthesia machines and ventilators, as well as therapy-delivering devices such as infusion pumps.

Legacy Devices. The RFI centers on the security of legacy technologies, or those capital investments from prior years that were designed to last over a period of time and are still clinically useful. As noted in the RFI, many devices, such as sophisticated imaging equipment, are intended to last for a significant period of time, sometimes decades. A health system can have tens of thousands of devices from hundreds of manufacturers connected to its network, leading to significant security management challenges. For most hospitals and health systems, replacing these technologies is not financially feasible, with many hospitals only able to replace about 10 percent of devices in a given year.

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.

Too often, such supports are lacking and end-users must create their own custom security controls, many of which are expensive, inefficient, do not scale, and create operational challenges. For example, installing a firewall around a device entails additional technology and staff expenses. Or, disconnecting a piece of imaging equipment from the network means that radiologists cannot read images remotely. While there is recognition of “shared responsibility” for security, the reality today is that the end-user carries a much heavier load for securing devices. Security tools and procedures provided by medical device manufacturers should limit burden for the end-user and integrate, as much as possible, into standardized practices and tools already employed by hospitals and health systems. While not the topic of the RFI, many of these security concerns also apply to new products on the market today and are not solely limited to legacy devices. Today’s new product is tomorrow’s legacy device.

Supported Lifetimes. In considering the “supported lifetime” of a device, the useful life of a product should be the base consideration. Device security during its useful life should be assumed, with the manufacturer responsible for ensuring the device is secure. Beyond the expected useful life, a provider may reasonably be expected to develop wrap-around solutions, based on a risk-cost-benefit analysis. Unfortunately, with most devices, this is not the norm, and end-users are forced to undertake significant work to secure devices during their useful life. Many of these mitigating steps (firewalls, network segmentation, taking devices offline) do not completely resolve the security concerns and also can impact clinical workflows and patient care.

It would be useful for manufacturers to provide guidance to end-users at the time of purchase about the expected supported lifetime. This would allow for better planning and risk management activities. During the supported lifetime, manufacturers should be providing ongoing security updates, software patches, and needed hardware upgrades on a timely basis, after testing to ensure that the updates do not negatively impact device performance or the ability to send and receive data. If not included in the original purchase price, these upgrades should be provided at a reasonable cost. For example, upgrading a device from Windows 7 to Windows 10 should be anticipated by the device manufacturer, be a part of planned maintenance, and be done at a reasonable cost. To support the manufacturers, the Food and Drug Administration (FDA) must be clear about when these types of upgrades require additional review by the agency and fast-track any required reviews.

To support the end-users, device manufacturers should provide security tools as part of a device (logs, whitelisting, vulnerability scanning, software bill of materials, separation of privileges, intrusion detection systems, change control systems, etc.), provide devices with secure configurations based on a reference technical standard, and communicate with hospitals about how and when the manufacturer plans to remotely support a device. They also should provide best practice guidance that allows the provider to integrate a device into its enterprise security without excessive cost and effort. There is a significant contrast between the ease and efficiency of updating network and PC software for security and updating software embedded in medical devices. Software companies have generally prioritized creating a systematic approach for sharing timely updates and providing guidance on how to complete them. Similar approaches have yet to be deployed by medical device manufacturers.

Furthermore, manufacturers should provide coordinated disclosures and timely patches and updates during an attack. Health care providers need a single source of information on what steps to take to secure devices. It is challenging to work with each company separately, and possibly with multiple parties within each company. One possibility could be for the FDA to create and maintain a coordinated home for this information.

The FDA's Role. The FDA provides oversight to ensure that medical devices are safe and effective. Recently, the agency has come to appreciate the extent to which cybersecurity is a key safety and efficacy issue. While the FDA has released both pre- and post-market guidance to device manufacturers on how to secure systems, the concerns outlined above have yet to be resolved, particularly for the large number of legacy devices still in use. Given that legacy devices have already been sold, there is little incentive for manufacturers to address the security of their installed base of products. The FDA must make clear that security measures to protect legacy devices are required, not optional. Unfortunately, the health care sector, including the device sector, continues to be confused as to whether FDA guidance on post-market cybersecurity is binding.

As a regulator, the 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 the FDA to improve the security of legacy and new medical devices will aid in reducing significant sources of vulnerability. We were pleased to see the FDA include cybersecurity steps in its recent Medical Safety Action Plan. These included considering 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 the FDA's oversight of medical device manufacturers with respect to the security of their products and offered suggestions for improvement. The AHA also urged the FDA to move as quickly as possible to implement these steps and make public its timeline for the benefit of all stakeholders.

Thank you for your consideration of our comments. Please contact me if you have questions or feel free to have a member of your team contact Kristina Weger, executive director of executive branch relations, federal relations, at kweger@aha.org or (202) 626-2369.

Sincerely,

/s/

Thomas P. Nickels
Executive Vice President