May 31, 2018

The Honorable Greg Walden
Chairman, Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member, Committee on Energy and Commerce
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, DC 20515

Submitted electronically to: supportedlifetimes@mail.house.gov

Re: Response to Request for Information Around Supported Lifetimes

Dear Chairman Walden and Ranking Member Pallone:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) welcome the opportunity to respond to the Committee's request for feedback from stakeholders intended to inform its efforts to address cybersecurity issues in legacy devices.

CHIME is an executive organization serving more than 2,600 chief information officers (CIOs) and other senior health information technology leaders at hospitals and clinics across the nation. AEHIS, a partner organization with CHIME, represents more than 800 chief information security officers and provides education and networking for executive cybersecurity leaders within healthcare.

We agree that medical device management, particularly regarding security, is a complex and challenging topic with varying opinions and perspectives. As noted in the request for information (RFI), legacy devices are often susceptible to cyberattacks that also affect other areas of our nation's critical infrastructure. The lack of basic cybersecurity safeguards within legacy medical devices requires providers to manage undue risk as they attempt to balance patient safety against using legacy devices that are vulnerable to low-level and easily executed cyberattacks.

I. Primary Recommendations

Providers continue to encounter a series of challenges associated with securing medical devices, and in many instances, they are being required to accept more risk than is reasonably appropriate for the use of these devices. For example, during the WannaCry cyberattack cited in the RFI, several medical device suppliers (herein referred to as suppliers) elected to not provide software patches or other risk mitigations as they determined it was a "low risk," and in several instances when providers pushed for risk mitigations, they were simply informed by the supplier to disconnect the devices from the network if they felt the risk was unacceptable.

Therefore, we were pleased when the FDA outlined in their Medical Device Safety Plan the importance of cybersecurity related to medical devices. Increasingly, our members report that suppliers are taking a stronger interest in securing medical devices in ways that simply were not happening in prior years. Nonetheless, providers

perceive they are largely shouldering the risk associated with medical devices and that this disproportionate risk distribution results in an unfair and unreasonable risk to patient safety as well as an increased cost to their operations.

In many instances, providers feel as if they pay for the same medical device twice, once to purchase it and once more to secure it appropriately for cyber risks. While providers acknowledge they do own some of the risk for these legacy devices, they believe a shared responsibility between the suppliers and the providers is warranted for appropriate risk distribution compared to the current approach where one party assumes the majority of the responsibility.

Thus, in examining the numerous aspects of securing medical devices and the associated challenges, we delineated our comments into **several discrete subject areas** with subtopics that are outlined in greater detail within the body of this letter. **Our top recommendations, however, are outlined immediately below:**

1. **Industry Standard Definition(s):** What is defined as a legacy device should be simplified and defined to bring uniformity and consistency to the discussion across stakeholders. Even among providers there are varied opinions on what constituted a "legacy medical device."
2. **Industry Standard Categorization:** Given the heterogeneity of medical devices, a risk-based approach for categorizing cyber risk based on the type of device and its intended functionality would help the industry as currently the stratification of cyber risk is largely subjective.
3. **Responsible Vulnerability Disclosure:** Suppliers should provide documentation of vulnerabilities within their product(s), and this should include documentation on vulnerabilities that have not been publicly disclosed. The documentation should include a description of each vulnerability and its potential impact, as well as recommended compensating security controls, mitigations, and/or procedural workarounds.
4. **Reasonable Risk Sharing/Distribution:** Providers perceive they are unduly bearing the majority of the cyber risks associated with medical devices, many of which, they have little to no control over as they are result of the hardware and software design processes of the supplier.
5. **Supply Chain Risk Management:** Medical device risk reporting should be aligned with the newly developed portion of the supply chain risk management section released in the NIST Cyber Security Framework 1.1 version.
6. **Simplified Cybersecurity Implementation Guidance**: The amount of information available in the form of instructions for deploying medical devices varies significantly and more standardization is needed around the way this information is created and distributed.
7. **Basic Cybersecurity Hygiene**: Basic cyber hygiene is absent from a majority of medical devices sold on the market today. Therefore, we propose:

    A. **Standard set of criteria**: Suppliers should be required to follow a system with defined criteria to ascertain whether a device contains basic cybersecurity functionality, and whether or not it is functioning by default.
    B. **Costs:** Suppliers should be prohibited from charging providers after the sale of a device for additional costs to safeguard the device to meet basic cybersecurity requirements (e.g., using anti-virus).
    C. **Indemnification:** Providers should be fully indemnified against regulatory action and/or associated liability if a cybersecurity event results in patient harm or lack of ability to comply with regulatory

requirements, especially when the event is through no fault of their own and is rather a weakness or failure of the supplier to ensure their medical device incorporates basic cybersecurity safeguards.

8. **Modular Hardware/Software Design Principles:** Suppliers should be required to embrace modular design approaches to devices. Devices should be designed using standards that are aligned with industry best practices, not vendor propriety practices, protocols or designs.

II. Medical Device Lifecycle Management

A. **Medical Device Lifecycle Management Challenges:** The challenges for providers with managing medical devices throughout the lifecycle of devices varies significantly depending on the type, functionality and "smartness" of the devices. This has resulted in a fragmented approach across the industry and created a heightened state of concern among providers. After conferring across our membership base, the following represent frequent problem areas related to lifecycle management:

- **Asset Management:** The sheer volume of medical devices with different operating systems, ports, protocols, etc., on a provider's network is challenging to manage. Even for providers with robust asset management, inventory management is challenging as the software needed to maintain / patch the device related to the operating system is not routinely disclosed by the suppliers. This forces the providers to expend additional resources to even identify if a specific device is vulnerable to a specific attack.

- **Supply Chain Challenges:** Supply chain vulnerabilities and the associated cyber risk from a provider perspective is a patient safety issue. Several members reported that a persistent challenge with their suppliers is that security features are not inherently integrated into medical devices, requiring providers to add on security after the fact, which often results in the provider accepting the increased cyber risk of the device as well as the cost to safeguard it.

  While suppliers are talking about security, there is a lack of actual action on the topic to safeguard their devices. From a provider perspective, it is positive that the FDA continues to highlight the importance of cybersecurity; however, our members do not believe that the current approach of issuing guidelines to suppliers that contain non-binding recommendations is having a material impact on this issue.

  We recommend that the FDA strongly consider the use of binding guidance, while also working to link what has been outlined in the NIST Cyber Security Framework 1.1 version around the supply chain risk management with standardizing reporting related to medical device risks. CHIME & AEHIS are pleased to see that NIST heeded our suggestions for strengthening this area of the Cyber Security Framework (CSF), as our members have identified this as an area for improvement.

- **Contracts:** Providers often experience a significant challenge having suppliers agree to contracts with basic language around privacy and security related to federal regulatory obligations. A significant point of contention between providers and suppliers is that suppliers are not required to satisfy regulatory obligations under the Health Insurance Portability and Accountability Act's (HIPAA) privacy and security requirements, yet they are required to follow Food and Drug Administration's (FDA) policies. Thus, our

members are more successful getting contract language inserted around patient safety than ensuring the information their devices store, process or transmit is being reasonably protected.

- **Technical Capabilities:** Several members raised concerns related to the technical capabilities of devices and the lack of clarity on security features and functions, including understanding what is enabled by default and what is the responsibility of providers. For example, whether devices have auditing, intrusion detection or prevention, etc., is frequently unknown. In addition, many providers are unable to obtain basic updates or patches for devices. Even if patches are available, without a complete understanding of the operating system, providers are unable to easily identify what systems need updates and many have been told patches won't be released for low-risk items (which is often a point of disagreement, as discussed under the controlled vs. uncontrolled risk section below). This played out during the WannaCry cyberattack last year as many providers simply didn't know what or how many devices were impacted because they didn't have the information on the device specifications.

- **Controlled vs Uncontrolled Risk:** An issue that is now emerging following the publication of the FDA's *Postmarket Management of Cybersecurity in Medical Devices* guidance, is the introduction of the concept of controlled vs. uncontrolled risks. Several members reported substantial disagreements between providers and suppliers for determining when a cyber risk is controlled vs. uncontrolled. As this approach does not have any system for resolving these disagreements, providers were bound by supplier decisions even though they disagreed with their positions, which ultimately left the provider's accepting the residual risk. The introduction of controlled and uncontrolled risk without proper mechanisms to address concerns has only contributed to the perceived inequality of risk distribution occurring from the provider's perspective.

- **Quarantining devices:** Several members provided feedback that they are often told that a device they considered high-risk because of vulnerabilities should be taken off the network or they should install a firewall to safeguard it. These responses were received by several providers that push backed on suppliers during the WannaCry cyberattack when they were attempting to receive risk mitigations for vulnerable devices.

  As one member noted, "we are way past firewalls" in terms of what is needed to protect medicals devices and our patients. In addition, as medical devices are critical for patient safety and care as well as the fact that many of these devices feed information into the electronic health record, it is an unrealistic expectation for the suppliers to communicate that removing devices is a viable option from a provider perspective.

B. **Costs for managing medical devices:** In discussing the challenges with medical devices with our membership, it became clear that the costs of vulnerability management programs are difficult to quantify and vary widely based on the maturity of the entity's cybersecurity programs. Some providers are making good faith efforts to do this work, but identifying the true costs for managing medical devices has not been conducted.

C. **What is a reasonable lifecycle for medical devices?** Our members view the issue of lifecycle from a few vantage points. First, they believe that the lifecycle for medical devices should be based upon the lifecycle of the operating system. Therefore, we do not believe that the lifecycle should be based on a

set number or years. For instance, if a device is based on XP and XP has waned then the lifecycle should be over.

Many of our members report challenges receiving extended support for devices once the operating system is no longer being updated. Further, sometimes suppliers are aware of a known vulnerability and do not share this with providers. Thus, we believe it should be a requirement that the supplier disclose to providers any known vulnerabilities, even vulnerabilities that have not been publicly reported.

D. **Modularity:** As technology suppliers mature, they have continued to focus on a modular design approach to software and hardware. It is the providers' opinion that this approach has a lot of potential related to medical device hardware and software design to reduce costs and improve the security of medical devices. For example, a modular approach would enable providers the ability to replace components of a device without having to buy an entirely new one.

III. Medical Device Definitions & Categorizations

In discussing the issue of legacy devices with our members, it became apparent that there is no uniform definition of a legacy device nor is there a standard set of criteria used to categorize them. Further, not only is there divergency in definitions among our members of what constitutes a legacy device, but there is also disagreement between providers and suppliers.

In the RFI, the Committee notes there are questions around how a provider should expect that a device be managed. From our perspective, devices vary considerably and managing them in a unilateral manner is not practical or cost effective. For instance, medical imaging equipment is costlier and it would not be cost effective if they were managed in a short lifecycle (e.g., five years) as most providers cannot afford to replace these systems that frequently. Therefore, the cost of the device and the technology used within it must be accounted for when deducing what the lifecycle should be.

We recommend that a cross-sector work group be assembled and charged with putting together the initial groundwork on this topic that can be built upon to move the industry closer to utilizing a common taxonomy.

This taxonomy should also work to address a risk categorization system to assist providers with the risk treatment for devices with the highest risk. Some of our members with more advanced cybersecurity programs report they are beginning to quantify risk; however, this is the exception not the norm.

IV. Medical Device Implementation

There was consensus among our members that not only is more information on medical devices needed for implementation, but that there should be a more simplified and standardized approach for the dissemination of this information.

A. **Standardizing Implementation Guidance: We recommend that suppliers be required to deliver simplified and easy-to-understand implementation guidance, and that it be required to be distributed in a consistent manner. Ideally, a summary, with a lengthier set of instructions**

should be the norm. One member likened this to the manual that comes with a car compared to the shop manual; both are needed by providers because while the "owner's manual" may offer the details on how the device is typically installed, providers may need more granular instructions for implementing the device within their environment.

B. **Basic Cybersecurity Hygiene:** Several providers reported that suppliers have attempted to monetize the vulnerabilities within their products by using them as an opportunity to charge providers additional fees for cybersecurity safeguards or push providers to upgrade to new products. In several instances, it has been identified that suppliers have attempted to charge additional fees for the usage of products such as anti-virus. The installation of anti-virus even on home computers is considered a basic necessity, therefore, it is troubling to see these types of emerging business practices.

It is unreasonable and inequitable that providers be required to absorb the costs from suppliers because they are unwilling or unable to implement basic cybersecurity safeguards within their products. **Therefore, suppliers should be prohibited from charging providers after the sale of the device, for additional costs to safeguard the device to meet basic cybersecurity requirements (e.g., using anti-virus). In addition, providers should be provided legal indemnification against regulatory action and or associated liability if a cybersecurity event results in patient harm or lack of ability to comply with regulatory requirements. This should especially be the case when the event is through no fault of their own and is rather a weakness or failure of the supplier to ensure their medical devices incorporates basic cybersecurity safeguards.**

V. Conclusion

CHIME & AEHIS commend the Committee for its leadership and willingness to engage stakeholders on these critical issues. Should you have questions about our remarks or require additional information, please contact us at policy@chimecentral.org.

Sincerely,

Cletis Earle, Chair,
CHIME Board of Trustees
Vice President and CIO
Information Technology
Kaleida Health

Erik Decker
Chair, AEHIS Board
CISO and Chief Privacy Officer
University of Chicago Medicine