ConnectedHealth

May 31, 2018

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, District of Columbia 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives
Washington, District of Columbia 20515

Dear Chairman Walden and Ranking Member Pallone,

The Connected Health Initiative (CHI) applauds your commitment to developing a better understanding of how the healthcare sector handles the cybersecurity risks presented by legacy technologies through the Supported Lifetimes Request for Information (RFI). We are pleased to share the expertise of our member organizations on this matter. CHI represents a broad consensus of stakeholders spanning the healthcare and technology sectors with a wide range of experience and a shared interest in helping the U.S. government support a communications technology-driven healthcare system.

The RFI points out several familiar issues with legacy technologies. CHI agrees that the use of legacy technologies presents unique risks and challenges. We offer the following recommendations and observations for the Committee’s consideration:

- ***CHI members, representing providers and a range of connected health stakeholders, strive to mitigate vulnerabilities associated with legacy technologies.*** No information is more personal to Americans than their own health information. CHI members respect this importance and put extensive resources into ensuring the security and privacy of sensitive health information to earn and maintain the trust of patients. We strive to leverage dynamic risk management frameworks, such as the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework and other healthcare-specific frameworks, to make purchasing, operational, and other decisions related to the risk presented.

While we acknowledge that legacy technologies and systems present risks, we emphasize that there is no one-size-fits-all solution to the phasing out of legacy equipment with vulnerabilities (nor is there a solution for cybersecurity vulnerability risk management generally). However, CHI members take steps, both as individual organizations and within partnerships and other collaborative relationships, to address legacy technology-related vulnerabilities. These steps include:

- ***Striving to maintain up-to-date asset management inventories.*** Our members point out that if a large health system—especially one large enough to have a variety of branches—is unable to account for its many devices and software programs, managing the risks they present is a much more difficult task. Maintaining these lists can be notoriously difficult, but a worthy investment of time and resources in order to properly identify and mitigate legacy IT risks, and is a foundational step in applying risk management to their complex systems.

  CHI further notes that software bills of materials (SBOMs) can improve a health system's cyber risk management markedly. However, SBOMs are more effective in the hands of an organization that has centralized its cybersecurity approach and prioritized its asset management. We recommend that these baseline, fundamental steps be taken before or in parallel with adopting more sophisticated methods of managing cyber risks. It is worth noting, however, that for smaller practices, the notion of centralizing these functions is less applicable, because the problem it addresses arises mostly from the inherent difficulty of coordinating the widely spaced functions of a larger enterprise.
- ***Prioritizing cybersecurity at the leadership level.*** Cybersecurity is an exercise in risk mitigation rather than a focus on patient care or revenue generation. For this reason, it is inherently difficult to prioritize cybersecurity in the healthcare context. Our members have observed that if an organization's chief information security officer (CISO) is marginalized within the decision-making process, they are also unable to prevent parts of the organization from adopting technology that escapes central security reviews. This makes the effort to support devices and software purchased by a branch of a healthcare system throughout the entirety of their lifetime more challenging. CHI therefore recommends that health systems empower CISOs to conduct security approvals and reviews for IT devices or software purchased by the health system.
- ***Managing (and limiting) connectivity to legacy equipment and software.*** As the RFI notes, it is often unfeasible for health systems to simply upgrade equipment or software when recommended by a cost-benefit analysis. Just as supervisory control and data acquisition (SCADA) systems limit internet protocol (IP) connectivity, health systems could benefit from limiting IP connectivity to legacy devices. For example, if certain hospital devices require legacy operating systems, we recommend they air gap them or place them on a virtual local area network (VLAN), separately from the hospital's IP-connected computers.

- ***Providing end-user education and assistance.*** Because the vast majority of cybersecurity breaches are caused by human error and thus preventable, end-user education is a crucial aspect of improving cybersecurity, particularly with respect to legacy technology in use or being phased out.

  The federal agencies under this Committee's jurisdiction, such as the Centers for Medicare and Medicaid Services (CMS), can incent fundamental risk management practices with respect to legacy technology. For example, through the implementation of the Medicare and CHIP Reauthorization Act, CMS continues to develop the Improvement Activities (IAs) or steps a caregiver can take to avoid penalties imposed by the Quality Payment Program's (QPP's) Merit-based Incentive Payment System (MIPS). CHI has encouraged CMS to adopt IAs that reward prudent cybersecurity risk management practices and offer education on cybersecurity hygiene. Additional incentive opportunities exist within the MIPS Promoting Interoperability performance category.

  We note that the Department of Health and Human Services (HHS) Office of Inspector General (OIG) could create a safe harbor from anti-kickback laws allowing for the sharing of cybersecurity products and services. Moreover, as HHS' own Cybersecurity Task Force Report recommends, "Congress [should] . . . evaluate an amendment to [the Stark Law and Anti-Kickback Statute] specifically for cybersecurity software that would allow health care organizations the ability to assist physicians in the acquisition of this technology, through either donation or subsidy."[1] Whereas OIG has the authority under current statute to create an anti-kickback safe harbor, creating Stark exceptions is more difficult for CMS. As a result, Congress could consider creating a Stark exception as an incentive to adopt cybersecurity measures that are otherwise unavailable under the Stark statute.

- ***Regulators should facilitate timely software updates for medical technology.*** CHI urges this Committee to ensure government regulation does not inadvertently discourage the patching of vulnerabilities. For example, the Food and Drug Administration (FDA) currently requires manufacturers to manage post-market cybersecurity vulnerabilities for marketed medical devices. CHI supports the FDA's approach to routine cybersecurity software modifications. Considering the dynamic world of threats to software, the FDA recognizes the need for constant software modifications and has worked to ensure unnecessary regulatory burdens do not discourage software updates that are strictly security-themed. The FDA offers a practical and tailored approach to cybersecurity risk management in a way that removes unnecessary government intervention from an increasingly necessary activity. We discourage the FDA from extending its reach beyond medical devices to a health system's broader IT equipment.

[1] https://www.slideshare.net/dgsweigert/healthcare-sector-cybersecurity-task-force-report-6217 (recommendation 1.5).

- ***Public-private partnerships (PPPs) are a useful vehicle to confront cyber-based threats posed by legacy technology in the healthcare sector.*** PPPs can support the ability to rapidly react to ever-developing cybersecurity risks that prey on legacy technology. CHI is committed to working collaboratively with all public and private stakeholders to ensure a secure connected healthcare ecosystem. The U.S. government should increase outreach to the private sector to collaborate on the management of legacy technology-related vulnerabilities.

  For example, the voluntary and timely sharing of cybersecurity threat indicators among private and public-sector organizations is crucial to the detection, mitigation, and recovery of cybersecurity threats, particularly regarding legacy technology. Cybersecurity threat information sharing fora that utilize the open and inclusive PPP model, from the most formal to the more loosely organized, can assist those looking to improve their cybersecurity posture through the sharing of threat information. While Congress and various federal agencies have taken steps to improve threat information sharing, public and private sector stakeholders must do more. CHI is committed to facilitating more effective and timely sharing of cybersecurity threat information. We believe the U.S. government must share the available threat information in a more user-friendly way. We encourage you to review our views in more detail within a recent testimony on this issue.[2]

We thank you for your continued attention and dedication to address cyber vulnerabilities in the healthcare sector, especially those related to legacy technologies. These threats have unique characteristics within the healthcare sector and deserve dedicated attention from this Committee. We look forward to the next steps of this process, and we welcome your questions or comments.

Sincerely,

Brian Scarpelli
Executive Director
Connected Health Initiative

[2] http://actonline.org/wp-content/uploads/11152017_ACT-Small-Biz-Testimony_Cybersecurity.pdf.