HSCA
HEALTHCARE SUPPLY CHAIN ASSOCIATION
Innovators In Evidence-Based Sourcing

May 31, 2018

The Honorable Greg Walden
Chairman
House Committee on Energy
and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
House Committee on Energy
and Commerce
322A Rayburn House Office Building
Washington, D.C. 20515

Re: Comments of the Healthcare Supply Chain Association (HSCA) on Supported Lifetimes and Legacy Medical Devices

Dear Chairman Walden and Ranking Member Pallone:

We thank the Committee for its interest in medical device cybersecurity and for the opportunity to add our insights to this critical conversation.

The Healthcare Supply Chain Association (HSCA) is a broad-based trade association whose members include for-profit and not-for-profit corporations, purchasing groups, associations, multi-hospital systems and healthcare provider alliances. As the sourcing and purchasing partners to virtually all of America's 7,000+ hospitals, as well as the vast majority of the 68,000+ long-term care facilities, surgery centers, clinics, and other healthcare providers, HSCA and its member group purchasing organizations (GPOs) have a unique line of sight over the entire healthcare supply chain and an important perspective on medical device cybersecurity.

Advances in information technology and medical devices, and increasing interoperability of information systems, devices and services are improving patient care and creating efficiencies in the healthcare system. Medical devices are often life-sustaining or provide vital clinical functions that cannot be compromised without diminishing direct patient care. Accordingly, the availability, reliability, and safety of these devices is essential. As the Committee has noted, medical devices and services are vulnerable to cybersecurity threats that could jeopardize patient health, safety and privacy. The increased use of connected medical devices and software as a service (SaaS), adoption of wireless technology, and overall increased medical device and service connectivity to the internet, significantly increase the risks of cybersecurity threats.

On April 17, 2018, HSCA released "Medical Device and Service Cybersecurity: Key Considerations for Manufacturers & Healthcare Providers," as well as "Recommendations for Medical Device Cybersecurity Terms and Conditions." These documents outline steps that organizations within the medical device supply chain can take to minimize and mitigate cybersecurity risks associated with the use of connected

1341 G Street NW, Suite 600 Washington, DC 20005 Phone (202) 629-5833 Fax (202) 466-9666
Web www.SupplyChainAssociation.org Email info@SupplyChainAssociation.org

medical devices. Further, they provide suggested terms and conditions to be used in purchasing contracts and documents to specify the parties' cybersecurity responsibilities relative to the acquisition, deployment and maintenance of these devices throughout the product lifecycle. We believe it is critical that the healthcare industry quickly address cybersecurity issues on a go-forward basis so as to minimize future risks while dealing with the challenges posed by the countless legacy medical devices in use today.

As the Energy and Commerce Committee noted in its "Supported Lifetimes Request for Information," legacy medical devices pose complex and varied challenges relative to cybersecurity. Many perform essential lifesaving clinical functions. Devices that were not designed to be networked may now be connected, many operate on now-unsupported software, and it is not uncommon for healthcare providers to use equipment well beyond its original expected life. The cost of these devices ranges from hundreds to millions of dollars and replacing and installing these devices can be costly and time consuming. Rapid replacement of all legacy medical devices to mitigate cybersecurity risk is an impractical and unrealistic expectation.

We also concur with the Committee's observation that requiring manufacturers and developers of these technologies to support them for as long as they are in circulation may be impractical and/or inefficient. This is particularly troublesome on a retrospective basis, where requiring such support may be inconsistent with the terms and conditions of sale and maintenance to which the manufacturer and provider have already agreed.

Our conclusion is that there is no simple and easy answer to mitigating risks for the broad spectrum of legacy medical devices in use today. Each situation needs to be evaluated considering:

a) the risk associated with continued use of the legacy device(s);
b) the clinical or operations benefit provided by the device(s);
c) the cost of replacing the device vs. cost of mitigation of the risk;

In the HSCA "Key Considerations," we encourage suppliers to view rapid adoption of cybersecurity measures and compliance with the FDA's Cybersecurity guidelines as an opportunity to gain competitive position and/or advantage. Healthcare providers will express a preference for secure devices. Recognizing that it is not practical or feasible for providers to retire or replace all their legacy medical devices in the short term, manufacturers who help providers maximize the value of their current investments are likely to gain competitive position relative to future sales. We further encourage providers to reward those suppliers that take responsibility for the security of legacy medical devices above and beyond contractual and regulatory requirements with new business and not purchase from suppliers who fail to take such responsibility.

1341 G Street NW, Suite 600 Washington, DC 20005 Phone (202) 629-5833 Fax (202) 466-9666
Web www.SupplyChainAssociation.org Email info@SupplyChainAssociation.org

HEALTHCARE SUPPLY CHAIN ASSOCIATION
Innovators In Evidence-Based Sourcing

A variety of methodologies can and will be used to mitigate the cybersecurity risks associated with legacy devices. These will include, but not be limited to, retirement, replacement, patching, upgrading, and network segmentation. Providers and suppliers should work cooperatively to determine the appropriate strategy for each situation, and whenever possible suppliers should provide mitigation mechanisms at no or minimal costs. Suppliers and providers should participate in one or more Information Sharing and Analysis Organizations (ISAOs), utilize risk assessment IT security methodologies, and ensure their policies and practices reflect widely-accepted standards, such as those provided by the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and/or the Federal Information Security Management Act (FISMA) recommendations and requirements for cybersecurity. Information sharing among the user community is a significant factor in battling cybercriminals and participation in ISAOs is a platform for such sharing and a factor in improving the cybersecurity of all participants.

HSCA believes that maintaining device and information security is a shared responsibility of the manufacturers and suppliers of connected devices and services, as well as the providers that use them. Providing this security is a continual effort that requires vigilance, adaptation, and ongoing communication and collaboration between the parties.

We look forward to continuing to work with all stakeholders to help ensure device and information security across the entire healthcare system. If HSCA can be a resource for you and your staff as you continue to address cybersecurity, please contact me directly at (202) 629-5833 or tebert@supplychainassociation.org.

Sincerely,

Todd Ebert, R.Ph.
President and CEO
Healthcare Supply Chain Association (HSCA)

Curt Miller
Executive Director
HSCA Committee for Healthcare e-Standards (CHeS)

cc: Members of the U.S. House Committee on Energy and Commerce

1341 G Street NW, Suite 600 Washington, DC 20005 Phone (202) 629-5833 Fax (202) 466-9666
Web www.SupplyChainAssociation.org Email info@SupplyChainAssociation.org