HSCA
HEALTHCARE SUPPLY CHAIN ASSOCIATION
Innovators In Evidence-Based Sourcing

March 15, 2019

U.S. Food and Drug Administration
Attention: Dockets Management Staff (HFA-305)
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Re: Comments of the Healthcare Supply Chain Association (HSCA) on FDA Request for Comments on the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices [Docket No. FDA-2018-D-3443]

On behalf of the Healthcare Supply Chain Association (HSCA), we appreciate the opportunity to provide comments on the U.S. Food and Drug Administration (FDA) on the management of cybersecurity in medical devices.

HSCA represents the nation's leading healthcare group purchasing organizations (GPOs), 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. We help our healthcare provider partners leverage their purchasing volume to negotiate competitive prices on healthcare products and services, helping to lower costs for patients, hospitals, payers, Medicare and Medicaid, and taxpayers. GPOs deliver critical cost savings that allow healthcare providers to focus on their core mission: providing first-class patient care.

HSCA and its Committee for Healthcare eStandards (CHeS) support FDA's direction in updating and enhancing its guidance to manufacturers relative to the importance of effective cybersecurity in medical devices. We refer the FDA to HSCA's "Medical Device and Service Cybersecurity: Key Considerations for Manufacturers & Healthcare Providers", "Recommendations for Medical Device Cybersecurity Terms and Conditions" and our comments to the House Committee on Energy and Commerce on Supported Lifetimes and Legacy Medical Devices for additional detail and information regarding HSCA's thoughts and position regarding cybersecurity in medical devices. 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 medical devices. Moreover, 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.

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

Improvements in the interoperability of healthcare information systems in combination with advances in information technology and medical devices are improving patient care and creating efficiencies in the healthcare system. Medical devices frequently deliver life-sustaining, vital clinical functions that cannot be compromised without diminishing direct patient care. Accordingly, the availability, reliability, and safety of these devices are essential. Unfortunately, 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 at both the device and network level.

As the FDA notes in the "General Principles and Risk Assessment" section, a compromised device exposes the network and other connected devices to security threats. Network compromise of a healthcare provider can pose significant risk to multiple patients. Accordingly we suggest that the scope of the FDA's guidance be expanded to include risks to patient harm arising not just from "device exploitability" but also from network compromise via an exploited device, i.e. "Effective cybersecurity management is intended to decrease the risk of patient harm by reducing device exploitability which can result in intentional or unintentional compromise of device safety and essential performance and/or unauthorized network access." We also suggest that the definition of cybersecurity in the guidance be modified to clarify that the intent of cybersecurity is to protect any information or system in the network to which the medical device is protected from being compromised, i.e. "Cybersecurity – is the process of preventing unauthorized access, modification, misuse or denial of use or, or the unauthorized use of information that is stored, accessed or transferred from a medical device to an external recipient or from any device or system on a network to which that medical device is connected." The definition of Patient harm should be also modified to reflect the risks associated with network compromise, i.e. "Cybersecurity exploits of a device, or of a system or network to which the device is connected, may pose a risk to health and may result in patient harm."

The guidance notes that manufacturers of devices automated with computer software establish and maintain procedures to ensure that the design requirements relating to the device are appropriate and address the ***intended use*** of the device. While the limitation to intended use may be reasonable for some factors in the use of the device, cyber criminals cannot be expected to limit their efforts to intended use nor are there significant practical reasons to limit device cybersecurity measures to a device's intended use. Accordingly we believe that cybersecurity requirements should apply to any use of the device.

The FDA notes in the draft guidance that medical devices connected to a network are more vulnerable than devices not connected. It also defines Tier 1 "Higher Cybersecurity Risk" devices as those capable of being connected to another product, network or the internet; AND where a cybersecurity incident affecting the device could directly result in patient harm to multiple patients. As noted earlier, we

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

believe that any device connected to a healthcare provider's network poses a risk to multiple patients due to network compromise and suggest that second condition of posing patient harm to multiple patients should be removed. Any device that can potentially be used to compromise a healthcare provider's network poses risks to multiple patients.

It is important that devices be designed to prevent both unauthorized use and unauthorized access. We suggest that the heading for Section A.1. be revised to "Prevent Unauthorized Use or Access". Further, the use of encryption can not only be used to prevent data from being read but also from being modified in transit, i.e., "Devices should have appropriate protections in place that prevent sensitive information from being read or modified by unauthorized parties either in storage or in transmission. Encryption should be used as appropriate, as it can protect sensitive information from unauthorized disclosure and modification."

In Section A.1.(a) the FDA provides good recommendations regarding limiting access to trusted users and devices only. However, these could be enhanced by adding a recommendation to not store passwords unprotected on the device (i.e. store passwords hashed as opposed to plain text). In addition to physical controls, authentication should be required when connecting to communication ports.

Within Section A.1.(b) we suggest adding a recommendation to utilize secure boot security standards whenever feasible We also recommend that the Manufacturer Usage Description (MUD) protocol detailed in IETF RFC 8520 be encouraged as part of electronic device identification in paragraph A.1.(b)(v) "The goal of MUD is to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function."

Labeling and documentation requirements should include a description of systematic procedures for users to follow to wipe or sanitize device media of any sensitive (e.g., Protected Health Information) that may be stored on the device before retiring or otherwise removing the device from use.

We support the draft guidance calling for manufacturers to design trustworthy devices and encourage the FDA to retain this concept in the final guidance. These thoughts are consistent with our comments in "Key Considerations" that healthcare providers prefer to purchase devices that adhere to FDA guidelines and meet the QSRs. We also encourage manufacturers to view rapid adoption of the guidelines and strong cybersecurity measures as an opportunity to develop competitive position.

HSCA appreciates the opportunity to provide our perspective. HSCA supports the FDA's efforts to provide guidance to manufacturers that strengthens the security of medical devices and the healthcare provider systems and networks to which they may be connected.

Please do not hesitate to contact me directly should you have any questions. I can be reached at cwmilleriii@gmail.com or (401) 225-9389.

HSCA
HEALTHCARE SUPPLY CHAIN ASSOCIATION
Innovators In Evidence-Based Sourcing

Sincerely,

Curtis W. Miller
Executive Director
Committee for Healthcare eStandards

HSCA MEMBERS

acurity · CAPSTONE HEALTH ALLIANCE · HEALTHTRUST · HPS · HRS Health Resource Services · innovatix · INTALERE · MMCAP · PREMIER · PROVISTA · TPC · vizient · YANKEE ALLIANCE *Common goals. Uncommon results.*

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