Medical Device and Service Cybersecurity:

Key Considerations for Manufacturers & Healthcare Delivery Organizations

***EXECUTIVE SUMMARY*: Advances in information technology and medical devices and the 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. However, 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), the adoption of wireless technology, and overall increased medical device and service connectivity to the internet significantly increase the risks of cybersecurity threats.**

Maintaining device and information security is a shared responsibility of the manufacturers and suppliers of connected devices and services as well as the healthcare delivery organizations (HDOs) that use them. Providing this security is a continual effort that requires vigilance, adaptation, and ongoing communication and collaboration between the parties.

The Healthcare Supply Chain Association (HSCA) and its group purchasing organization (GPO) members are the sourcing and purchasing partners to America's hospitals, long-term care facilities, surgery centers, clinics, and other HDOs. Given our unique line of sight over the entire healthcare supply chain HSCA suggests the following key cybersecurity considerations for medical device manufacturers, HDOs, and service providers:

GLOSSARY OF KEY TERMS

This discussion references several terms for which the reader should have a clear understanding of the meaning. Readers are encouraged to reference the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) Glossary at https://csrc.nist.gov/glossary for additional information and definitions.

Vulnerability – Weakness or deficiency in an information system, system security procedures, internal controls, or an implementation that could be exploited by a threat source or accidentally triggered.

Threat – A deliberate or unintentional activity that has the potential to harm organizational operations or an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and/or natural events.

Exploit – A threat actor taking advantage of a vulnerability to gain unauthorized access to a system or network

Cybersecurity Event – A cybersecurity or IT environment change that could have an impact on organizational operations, including mission, capabilities, or reputation. Note that most organizations experience many cybersecurity events on a daily basis. Few rise to the level of Incident or Breach.

Cybersecurity Incident – A cybersecurity event that compromises the integrity, confidentiality or availability of an information asset

Breach – A cybersecurity incident that results in the confirmed disclosure of data to an unauthorized party.

HDOs and suppliers should, at minimum, participate in one or more Information Sharing and Analysis Organizations (ISAOs) such as the Health Information Sharing and Analysis Center (H-ISAC), utilize an IT security risk assessment methodology 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)**, **The Health Sector Coordinating Council (HSCC)** and/or the **Federal Information Security Management Act (FISMA)** recommendations and requirements for cybersecurity. Suppliers and HDOs should be familiar with the May 12, 2021 **Executive Order on Improving the Nation's Cybersecurity** and ensure they are aligned with that order as required.

Key cybersecurity measures that organizations should implement are noted below; some apply to all organizations, while others are HDO-specific or supplier-specific.

CONSIDERATIONS FOR HEALTHCARE DELIVERY ORGANIZATIONS, MEDICAL DEVICE MANUFACTURES & SERVICE SUPPLIERS

- Organizations should designate an information technology and/or network **security officer** to be responsible for security of the organization, services, and products, and for maintaining communications and relationships with peers and counterparts across the industry.
- All employees with network access should receive role-appropriate **periodic training and assessments**, at least annually, on cybersecurity. Training should include periodic phishing tests with additional training provided for employees who fail tests or assessments.
- Organizations should have processes for implementing and maintaining **anti-virus/anti-malware software**.
- Organizations should have patching processes capable of aiding in prevention of a ransomware attack. ensuring all software, firmware, and third-party applications are **updated and patched promptly**. **Unsupported software should be retired** on a timely basis.
- Organizations should install **firewalls** and use **network segmentation** to provide least-privilege access to system resources and data where appropriate to further minimize risks.
- Organizations should make appropriate use of **firewalls or network access control** (NAC) to **restrict user access to systems and data based on need**. Consideration should be given to implementing IP address and/or application **whitelisting in high-risk environments,** limiting applications and services to those pre-approved.
- When practical, **data should be encrypted in transit**. Authentication Information (usernames, passwords, keys etc.), Personally Identifiable Information (PII), Protected Health Information (PHI), as well as any **confidential** or **sensitive information** should **always** be **encrypted** in **transit** and at **rest**.
- **Backup and restoration procedures**, capable of aiding in recovery from a ransomware attack, should be created, documented, and periodically tested.
- A **password policy** that complies with latest NIST and/or ISO guidelines should be enforced. **Default passwords** for operating systems, databases, and applications should be changed upon implementation and immediately whenever an employee with knowledge of them leaves the organization. Where possible, organizations should also consider **changing default usernames**. **Shared passwords are to be avoided**.
- **The expected useful life of the device or service should be specified within the purchase agreement** and security updates to the software and all supporting software components (Software Bill of Material – SBoM) should **be made available for the stated useful life** at no additional cost to the HDO, this and other recommended contract terms and conditions may be found in HSCA's *Recommendations for Medical Device Cybersecurity Terms and Conditions*.

- In cases where manufacturers are selling devices that rely on software no longer supported by a third party, the HDO should be sure to consider **any additional expenses that will be incurred to securely implement and maintain the devices.**

- **Medical device application software** (e.g., image acquisition, manipulation, reconstruction, analysis, display, etc.), **and any commercial Operating System (OS) necessary for operation and maintenance of the system** should be provided by the Supplier with a perpetual license. The most current version of a medical device should have an OS with latest the latest major release currently available for purchase in the commercial marketplace. Application software updates compatible with the system's hardware shall be kept current at no cost to the HDO for at least the expected useful life of the device.

CONSIDERATIONS FOR HEALTHCARE DELIVERY ORGANIZATIONS

- HDOs should avoid acquiring any device or service from a manufacturer that does not warrant that they **actively participate in an ISAO**. **HDOs are encouraged to participate in ISAOs** as well. 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. Terms of sale, including non-disclosure agreements, should not prohibit HDOs from participating in ISAOs or other cybersecurity information sharing initiatives.

- HDOs should avoid acquiring devices for which a supplier is unable or unwilling to provide a **Manufacturer Disclosure Statement for Medical Device Security (MDS2) utilizing the most recent template**. Where suppliers provide MDS2s, those MDS2s should be **reviewed by HDO network security teams**, or their designated third party, prior to the purchase, use, or implementation of any medical device. All medical devices and services should be installed and operated in a manner consistent with the organization's security policies and practices.

- Purchase agreements for medical devices and services should contain **appropriate liability and warranty provisions**.

- HDOs' **insurance policies should cover cybersecurity risks with appropriate minimum coverage**. HDOs should not acquire devices or services from any supplier who will not provide evidence of appropriate coverage unless no practical alternatives exist.

- HDOs should not acquire or utilize devices, software or services not **compliant with current U.S. Food and Drug Administration (FDA) cybersecurity guidance** or industry standards unless no practical alternatives exist. In these cases, HDOs should ensure devices, software and/or services are deployed in a manner that reduces the risk of a cybersecurity or information security incident or breach.

- HDOs should conduct **risk assessments, including testing when practical,** for all **devices and services to verify manufacturer claims** prior to acquiring any device or service and connecting the device or service to their network. Alternately, a third-party testing and certification service may be used to validate manufacturer's claims. Policies regarding who can approve and add devices to the network should be implemented and followed.

- HDOs should **require suppliers to identify if a device can be remotely accessed or controlled**, whether it is connected to a network, and if the device can be remotely accessed or controlled, the supplier should provide a detailed description of the measures incorporated to safeguard the security of that device

- HDOs should **implement physical security controls** to prevent unauthorized and/or unwitnessed access to any devices and servers.

CONSIDERATIONS FOR MEDICAL DEVICE MANUFACTURERS & SERVICE SUPPLIERS

- Suppliers of network-accessible medical devices, software and services should **warrant that they are compliant with current U.S. Food and Drug Administration (FDA) cybersecurity guidance documents,** industry standards and do not contain known malicious code or other known vulnerabilities.

- Medical device manufacturers should **provide an MDS2 (current version and SBoM) for any medical device that can be connected to a network** (i.e., any device that has a MAC address).

- Supplier **insurance policies should cover cybersecurity risks with appropriate minimum coverage**.

- Although compliance with current guidelines can significantly reduce the cybersecurity risks associated with medical devices and services, **legacy devices and possible future noncompliance pose ongoing risks**. HDOs have a considerable investment in connected legacy devices, software and services that may not be compliant with current guidelines and standards but that are critical to maintaining patient care. Recognizing that it is not practical or feasible in the short term to retire or replace those assets, **manufacturers should acknowledge responsibility for the security of legacy devices** and **work expeditiously to upgrade those to current security standards or provide device upgrade paths** to HDOs at the lowest possible cost.

- In addition to complying with regulatory reporting requirements, suppliers of network-accessible medical devices, software and services should, at their own expense, provide corrective actions, etc., which includes the following:

    - **Reliable and timely information** (e.g., via Cybersecurity Portals, direct communications, etc.) regarding any issues or risks identified with one of their devices or services, the firmware, software and/or any other security issues;

    - **Guidance on what should be done** to address any vulnerability, including a corrective action plan/flaw remediation process that identifies appropriate software update(s) and/or workaround(s) to mitigate all issues or risks associated with the vulnerability;

    - **Change management-based release notes** and/or HDO communications explaining the impact of changes to operating systems, databases, applications, and more.

- Suppliers should make every effort to assist HDOs in resolving cybersecurity threats and vulnerabilities in a timely manner.

- Suppliers should ensure the security of all procured or developed systems and technologies, including all subcomponents (hereinafter referred to as "Systems"), throughout the useful life including any extension, warranty, or maintenance periods. This includes, but is not limited to, workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as “Security Fixes”) which may be necessary to fix all security vulnerabilities published or known to the Supplier anywhere in the Systems, including Operating Systems and firmware. The Supplier should **ensure that Security Fixes do not negatively impact the Systems**.

- As encouraged by FDA guidance, device manufacturers should participate in an Information Sharing and Analysis Organization (ISAOs) such as the **Health Information Sharing and Analysis Center (H-ISAC** or the **Health Information Trust Alliance (HITRUST)**;

- Although the FDA’s guidance is prefaced as non-binding, the FDA has stated that medical device manufacturers must **comply with all federal regulations including quality system regulations (QSRs)**. QSRs require medical device manufacturers to address all risks, including cybersecurity risks. The FDA guidance provides recommendations on how manufacturers might address those risks. Medical device manufacturers should recognize that HDOs prefer to purchase devices that adhere to the FDA guidelines and meet the QSRs. We encourage manufacturers to view the rapid adoption of rigorous cybersecurity measures and compliance with published guidelines as a necessary precondition to marketing medical devices.