AdvaMed
Advanced Medical Technology Association

AdvaMed Medical Device Cybersecurity Foundational Principles

Safety is critical to the medical technology industry, and medical device manufacturers take seriously the need to continuously assess the security of their devices in a world where the risks, no matter how remote, evolve. Medical device manufacturers address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data. Similarly, manufacturers implement proactive measures to manage medical device cybersecurity, including but not limited to routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

This document provides the medical device industry's foundational principles for building a cybersecurity program for the development and deployment of secure medical devices. To be sure, the entire health care ecosystem that uses advanced medical technologies should be aware of the potential for cybersecurity incidents and share in the commitment to securing these technologies. This includes but is not limited to the users, healthcare professionals, providers, IT system integrators, Health IT developers, IT vendors, medical device manufacturers, and regulators. Moreover, security requirements for medical devices must take into account the intended use and use environment of the product. For example, many medical devices are required to be immediately accessible by a physician during an emergency medical procedure, and miniaturized medical devices are often constrained by limited energy storage (*e.g.*, battery life).

The medical device industry commends and supports FDA's efforts to address medical device cybersecurity. We continue to work with the agency, health care providers, the academic community, security experts and other stakeholders on ways to ensure the continued security, safety and effectiveness of medical devices.

The following foundational principles should guide the development of an effective cybersecurity program for the production and deployment of secure medical devices:

1. **Medical device development and security risk management.** An effective cybersecurity risk management program incorporates both premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to disposal.[1]

[1] Device manufacturers are expected to apply FDA's cybersecurity-related guidance documents during the premarket and postmarket lifecycle phases. *See Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act (Mar. 29, 2023);* Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (Sept. 26, 2023); Postmarket Management of Cybersecurity in Medical Devices (Dec. 27, 2016).

AdvaMed Code of Ethics CERTIFIED

Medical device security risks should be addressed through a risk management process that is based on consensus-driven recognized standards and reference documents.[2]

a. Manufacturers shall address and document cybersecurity during the design and development of the medical device. As a result, cybersecurity should be fully integrated into manufacturer quality management systems. In addition to patient safety and device effectiveness, product development processes must address privacy concerns as well as the fundamental objectives of secure design: Confidentiality, integrity (including authenticity and non-repudiation), and availability.

b. Manufacturers should work with healthcare providers, device users and patients to ensure that risk control measures intended to increase security do not degrade the intended use of the device, including requirements related to emergency access. A risk-benefit analysis may be required in certain situations. In many cases, the therapeutic benefits of a product far outweigh potential security risks.

c. Manufacturers shall have a process to monitor the ongoing security of their devices and if new vulnerabilities are revealed, they must determine whether additional security risk control measures can be implemented without compromising the safety and effectiveness of the device. These processes should operate with the quality management system creating supporting records and must operate in a timely manner to ensure healthcare ecosystem cybersecurity risks from vulnerabilities are adequately communicated and managed.

d. Manufacturers should employ mechanisms to receive relevant cybersecurity-related information from their suppliers.

2. **System-level[3] security.** Systems are only as secure as their weakest point. In order to maintain system-level security, all elements of the system must be appropriately managed and secured.[4]

---

[2] For example, manufacturers should address medical device security risks through a risk management process aligned with ISO 14971 *Medical devices — Application of risk management to medical devices*, and apply the NIST Framework for Improving Critical Infrastructure Cybersecurity in the development and implementation of their cybersecurity program.

[3] System-level security refers to the architecture, policy and processes that ensure data and system security in systems that contain connected medical devices.

[4] The ISO/IEC 80001 series of standards and technical reports support the risk management of IT-networks incorporating medical devices, including communication of product-specific security risk control measures that are the responsibility of a health care delivery organization.

a. System-level security is a shared responsibility. Device manufacturers play an important role; however, all stakeholders within the larger healthcare eco-system must work together to ensure its integrity.

b. Security incidents should be investigated in a collaborative fashion in order to, as appropriate, uncover facts, appropriately inform stakeholders including patients, health care delivery organizations, and regulators, and to employ additional security risk control measures when appropriate in the context of a device's intended use.

3. **Coordinated disclosure.** Medical device manufacturers should support a coordinated disclosure process that provides a pathway for researchers and others to submit information, including detected potential vulnerabilities, to the organization.

   a. Coordinated disclosure processes should clearly define the responsibilities of both the manufacturer and researcher.

   b. Manufacturers bear a responsibility to address submitted potential vulnerabilities in a timely and professional manner and to comply with regulatory reporting requirements.

   c. To minimize any potential impact to patient safety, researchers and other third parties should work with and submit as promptly as possible, and prior to public release of such information, potential vulnerabilities to the manufacturer and relevant government body (*e.g.*, FDA or DHS) on a coordinated basis.

4. **Information sharing.** It is important for manufacturers to continuously manage their device's cybersecurity throughout the product's lifecycle. Part of this process includes the judicious sharing of threat and vulnerability information, which enables organizations to efficiently respond to new threats.

   a. In order to facilitate the exchange of information, manufacturers should consider the use of a single information exchange body, with the understanding that other avenues of information sharing exist. If a new threat is discovered, it should be shared and, once validated, disseminated to the appropriate stakeholders.

   b. Shared vulnerability information must protect the identity and intellectual property of medical device manufacturers and disclosure of the information should not jeopardize the privacy and civil liberties of individuals. Authentication methods, non-disclosure agreements, and restricted access to information should be employed to ensure that only trusted entities receive vulnerability information.

   c. Close cooperation with local, state, and federal law enforcement agencies is necessary to ensure that information sharing does not inadvertently enable a threat source.

5. **Software Bill of Materials (SBOM).** To ensure medical device users are able to respond to cybersecurity threats, the community must coalesce around a common approach and align with standards to create and share SBOMs to ensure their consistency and usefulness.

    a. Medical device manufacturers, FDA and healthcare providers should agree to the information that is to be conveyed in the SBOM. Information required in the SBOM should be consistent with industry minimum expectations and standards including CISA minimum elements of an SBOM guidance. Only information that is necessary to support the essential cybersecurity functions of the SBOM recipient, without compromising intellectual property rights or providing information capable of misuse, should be shared.

    b. In order for an SBOM to serve as a meaningful resource, manufacturers should appropriately maintain and update the document when changes are made to the device.

    c. If required by a device manufacturer, SBOM recipients are expected to keep confidential all information shared by the device manufacturer and must not be shared with third parties outside of established confidentiality agreements. Some device manufacturers may choose to provide SBOMs in a less restrictive manner, but until practices mature it is important to establish trust between all stakeholders.

6. **Consensus standards, regulatory requirements, and education.** The development of consensus standards and regulations should be a collaborative effort between regulators, medical device manufacturers, independent security experts, academia, and health care delivery organizations.

    a. The health care industry should leverage the experiences and expertise of other critical infrastructure sectors and government agencies (*e.g.*, CISA, NIST).

    b. The involvement of academia and independent security experts is a critical factor in ensuring that new standards and regulations are current and reflect best practices.

    c. Manufacturers and health care delivery organizations should leverage principles elaborated in relevant consensus standards and technical reports.

    d. Stakeholders should be educated on the importance of coordinating privacy and security requirements so that they complement each other to further patient safety.