Navigating Section 524B

What You Need to Know About Ensuring Cybersecurity in Medical Devices

As medical technology and medical devices have advanced with new technology and increasing connectivity, so have the threats to their cybersecurity. These threats endanger patient health, lives, and privacy. Cybersecurity is a major concern, and the U.S. government moved to address it by passing a December 2022 bill that amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding Section 524B. This gave the Food and Drug Administration (FDA) statutory authority and a mandate around cybersecurity.

SECTION 524B AND CYBERSECURITY FOR MEDICAL DEVICES

The addition of Section 524B to the FD&C Act authorized the FDA to add cybersecurity requirements through the rule-making process ("guidance"). FDA issued "Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act: Guidance for Industry and Food and Drug Administration Staff" on March 30, 2023.

WHAT DOES SECTION 524B DO?

The FD&C Act Section 524B requires that medical device applications submitted by national medical device manufacturers for premarket approval must include information to ensure that cybersecurity requirements are met on their cyber devices. The requirements were phased in during 2023 and are now fully in force.

WHY CYBERSECURITY MATTERS FOR MEDICAL DEVICES

Many new medical technologies and devices are now connected to a computer network or the internet via wireless communication. Patient and device data can be transferred to and from doctors and medical facilities, but it also makes these devices vulnerable to computer hacking that can be harmful to the patient's health and privacy and even to the medical facility and other patients. Disruptions can target medical business or operational activities.

For example, a cardioverter-defibrillator (ICD) can be implanted inside a patient's body to perform defibrillation; some types can perform cardioversion and heart pacing. These devices can be connected to a small computer known as a programmer. They retrieve data for a home docking station that can transmit that data wirelessly from the ICD to the doctor or cardiac care team. These connections make the devices vulnerable to cyberattacks, and effects on the operation of the ICD can endanger the patient's health.

WHAT IS A CYBER DEVICE?

What medical products are in the scope of Section 524B? Section 524B(c) of the FD&C Act defines a cyber device as "a device that includes software validated, installed, or authorized by the sponsor as a device or in a device; has the ability to connect to the internet; and contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats."

Medical technology or medical device manufacturers should contact the FDA if they are unsure if their equipment or devices are considered cyber devices. Final decision on whether a device falls under the cyber device definition is subject to FDA's interpretation. (Note that devices that do not directly connect to the internet may still contain cybersecurity vulnerabilities.) A medical device manufacturer should be prepared to answer detailed questions if the FDA is not satisfied with the initial application.

REQUIREMENTS IN SECTION 524B

The FDA Requirements of Section 524B (Question 4) state that "Section 524B(a) of the FD&C Act provides that the sponsor of a premarket submission for a cyber device must include information to demonstrate that the cyber device meets the cybersecurity requirements in section 524B(b) of the FD&C Act."

Specifically, the sponsor of the premarket submission must:

- Submit a plan to monitor, identify, and address, as appropriate, in a reasonable time, post-market cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures.
- Design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available post-market updates and patches to the device and related systems.
- Provide a software bill of materials, including commercial, open source, and off-the-shelf software components.

For full details, see the FDA link at www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

REGULATIONS AND STANDARDS

There are seven regulations and standards that medical device manufacturers need to consider as they implement cybersecurity features in their devices. These are:

- **IEC 62304:** Medical Device Software: Software Lifecycle Processes
- **IEC 82304:** Health Software: General Requirements for Product Safety
- **IEC 62366:** Medical Device Software: Application of Usability Engineering to Medical Devices
- **ISO 14971:** Medical Devices: Application of Risk Management to Medical Devices
- **IEC 80001-1:** Application of Risk Management for IT-Networks Incorporating Medical Devices, Part 1: Safety, Effectiveness, and Security in the Implementation and Use of Connected Medical Devices or Connected Health Software
- **21 CFR 820:** Quality System Regulation 820.30(g): Design Controls: Design Validation
- **AAMI TIR57:** Principles for Medical Device Security: Risk Management

CYBERSECURITY: GENERAL PRINCIPLES AND FRAMEWORK

Medical device manufacturers should address cybersecurity during the design and development of their devices. However, the FDA recognizes that medical device security is a shared responsibility among stakeholders, including healthcare facilities, patients, providers, and medical device manufacturers.

General Principles

Manufacturers should establish design inputs related to cybersecurity and establish a cybersecurity vulnerability and management approach for their devices that includes:

- Identification of assets, threats, and vulnerabilities
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients
- Assessment of the likelihood of a threat and of a vulnerability being exploited
- Determination of risk levels and suitable mitigation strategies
- Assessment of residual risk and risk acceptance criteria

NIST Framework for Cybersecurity

Using a cybersecurity framework can help enable a comprehensive process that strengthens cybersecurity for medical devices. The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce that created a framework to help improve the management of cybersecurity risk. The FDA suggests addressing cybersecurity core functions per the NIST framework:

- **Identify:** Develop an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect**: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond**: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

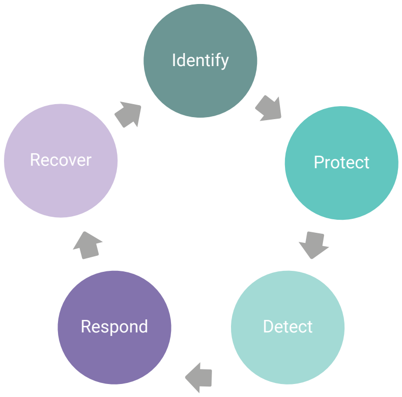

Figure 1. The NIST cybersecurity framework

PREMARKET CYBERSECURITY DOCUMENTS

The FDA has required that medical device manufacturers utilize strong cybersecurity methods and tools in the development of their products and the ongoing operation of their medical devices. In order to demonstrate that they are following these protocols, applicant manufacturers must develop and complete documents for their medical devices that cover the following topics:

- Threat modeling
- Cybersecurity vulnerability and risk assessment
- Cybersecurity control
- Traceability matrix
- Plan for continuing support
- Plan for malware-free shipping
- Cybersecurity labeling

KEY ACTIONS OUTLINED IN FD&C 524B

FD&C Section 524B requires medical device manufacturers to demonstrate these actions in their premarket application for new devices:

Monitor: Device manufacturers should have a process to monitor vulnerabilities.
Design: They should build devices that are secure by design.
Patch: There needs to be a routine patching plan that is part of the overall product lifecycle management.
Disclosure: There should be a process for coordinated vulnerability disclosure.
SBOM (CBOM): Devices should have a software bill of materials as part of a cybersecurity bill of materials.

THE INCREASING CYBERSECURITY FOCUS

As medical facilities and medical devices face daily and growing threats of hacking, viruses, and ransomware, the FDA and medical device companies have increased their focus on and priorities for cybersecurity and the implementation of strong security in device design, development, processes, operation, and updates. The FDA's role in cybersecurity is evolving as a result. Prior to FD&C Section 524B, its cybersecurity authority was tied to safety and effectiveness evaluation for devices, and security compliance was submitted along quality regulations. With the passage of the appropriations bill on March 29, 2022, the FDA was granted authority for cybersecurity in all new submissions to ensure adequate cybersecurity controls, and it published premarket cybersecurity guidance.

The role of device manufacturers is also changing. Prior to Section 524B, manufacturers had to document and justify why safety and essential performance were not impacted by known vulnerabilities. Now they must detail how to deliver patches as part of product lifecycle management, in addition to documenting why safety and essential performance are not impacted.

Software bills of materials (SBOMs) have evolved over the same time frame. Prior to the bill, manufacturers were to provide SBOMs as labeling to customers, if requested by the review branch. Since passage of the appropriation bill, medical device manufacturers are required to provide SBOMs for all defined cyber devices under review.

Since the implementation of FD&C Section 524B, the FDA and medical device manufacturers have advanced their focus on cybersecurity from initial design through development, delivery, operation, and ongoing updates and protection. Navigation of Section 524B by medical device manufacturers requires more design planning, development, and ongoing cybersecurity protection, all under strong FDA guidance and administrative authority, with the ultimate goal of protecting patient health, safety, and privacy.

WNDRVR

Wind River is a global leader of software for mission-critical intelligent systems. For 40 years, the company has been an innovator and pioneer, powering billions of devices and systems that require the highest levels of security, safety, and reliability. Wind River offers a comprehensive portfolio of software and expertise that are accelerating digital transformation across industries.

© 2023 Wind River Systems, Inc. The Wind River logo is a trademark of Wind River Systems, Inc., and Wind River and VxWorks are registered trademarks of Wind River Systems, Inc. Rev. 11/2023