Cybersecurity and U.S. FDA Medical Device Regulation

An overview of FDA cybersecurity control requirements in support of marketing submissions

Linda Chatwin, Esq, RAC
Lead Quality and Regulatory Consultant
linda.chatwin@ul.com

EMERGO
by UL

June 2024

The U.S. Approach to Cybersecurity of Medical Devices

The proliferation of wireless, internet, networked and interconnected medical devices and technologies has placed cybersecurity issues front and center for manufacturers and developers of such products. As this has and continues to evolve, we see regulators work to maintain requirements that will meet the security challenges presented by these devices. The U.S. Food and Drug Administration (FDA) has issued multiple guidance documents to this end.

They include:

- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, issued Jan. 14, 2005[1]
- Content of Premarket Submissions for Device Software Functions, issued June 14, 2023 – supersedes Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 2005[2]
- Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, issued Sept. 27, 2023 – supersedes Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Oct. 2, 2014[3]
- Postmarket Management of Cybersecurity in Medical Devices, issued Dec. 28, 2016[4]

In November 2021, under the sponsorship of the FDA, MITRE Corporation and the Medical Device Innovation Consortium, MDIC issued the ***Playbook for Threat Modeling Medical Devices*** using funds from the FDA. This is an educational resource for the medical device sector to help demonstrate how to effectively threat model[5]. Many private and public sector organizations recommend threat modeling to help manage and respond to cyber threats and risks.

In November 2023, MITRE released a white paper contracted by the FDA, *Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks*[6]. Because legacy devices were put on the market with cybersecurity controls that may have been effective at the time, these controls may no longer be effective due to evolving cyber risks. The MITRE white paper gives recommendations on how to address these cyber concerns. In addition, the FDA maintains a website to keep evolving cybersecurity issues updated[7].

In keeping with the FDA's expectations for cybersecurity controls, the eStar template for 510(k) submission involving software or devices with software in them includes the following requirements[8]:

- Cybersecurity risks
- Risk management report detailing separate, parallel and interconnected security risks in addition to the safety risk management process
- Threat model – identifying methodology (e.g., STRIDE, Attack Trees, Kill Chain, DREAD)
  - Include Architecture Views (global system, multi-patient harm, update ability/patch ability and security use case)
- Cybersecurity risk assessment – using exploitability versus using probability for likelihood
- Software Bill of Materials (SBOM), including software level of support and end of support date for each software component (e.g., OTS software)
  - Justification for any component where this is not available
- Listing of supported operating systems and associated versions the device/system uses
- Safety and security assessment of cybersecurity vulnerabilities in component software used by the device for all components in the SBOM
  - Description of controls that address the vulnerabilities
- Assessment of any unresolved anomalies for cybersecurity impact
- Data from monitoring cybersecurity metrics or justification where unavailable
- Information on security controls categories:
  - Authentication controls
  - Authorization controls
  - Cryptography controls
  - Code, data and execution integrity controls
  - Resiliency and recovery controls
  - Firmware and software update controls
- Architecture
- Cybersecurity testing performed with test reports:
  - Security requirement testing
  - Threat mitigation testing
  - Vulnerability testing
  - Penetration testing
  - Third-party test reports with company assessment
- Cybersecurity management plan
- Patch timelines and cycles
- Interoperability interfaces

There are a magnitude of cybersecurity concerns and control demands that companies need to navigate. Companies contemplating placing either software as a medical device (SaMD) — standalone software that fulfills one or more medical purposes without being part of a hardware medical device — or devices containing software on the market, must engage with subject matter experts to prepare the documentation required to gain market access.

FDA views

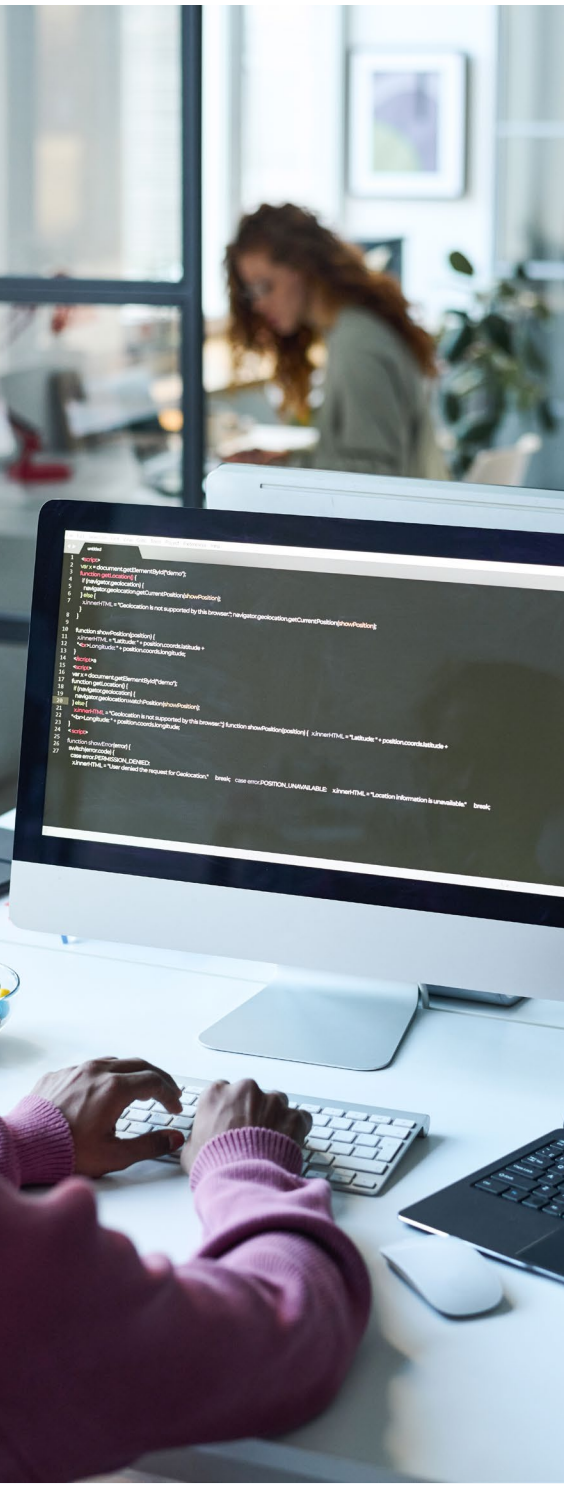
Device manufacturers are responsible for the safe and effective performance of medical device software, whether it is a SaMD or devices incorporating software. The FDA states explicitly in the guidance on networked medical devices containing OTS software that the device manufacturer bears responsibility for the continued safe and effective performance of devices including the performance of OTS software that is part of the device. Maintaining vigilance and being responsive to cybersecurity vulnerabilities are obligatory under 21 CFR 820.100 Corrective and preventive action.[9] This requires systematic analysis of sources of information and implementation of actions to correct and prevent problems. Design validation requires that devices conform to defined user needs and intended uses. This includes software validation and risk analysis. Software changes to address cybersecurity vulnerabilities must be validated before approval and issuance[10]. The FDA also notes that premarket review is not generally required prior to implementing a software patch to address a cybersecurity vulnerability.[11]

In its guidance document *Content of Premarket Submissions for Device Software Functions*, issued June 14, 2023, the FDA expects the determination of a risk-based documentation level for software to consider the likelihood of compromised device functionality as a result of inadequate cybersecurity controls. FDA may also request additional architecture diagrams to address cybersecurity risks associated with a device.[12]

FDA declares in *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, issued Sept. 27, 2023[13] that cybersecurity is part of device safety and therefore the Quality System Regulation. This is captured in the design control requirements, including risk analysis and design validation, as well as complaint handling, corrective and preventive action, and servicing. These processes can help determine the scope of vulnerability. Where multiple vulnerabilities exist, there also exists a greater threat of compromising the safety and effectiveness of the device. The guidance document recommends a Secure Product Development Framework (SPDF) as one approach that can be used to satisfy cybersecurity concerns in the Quality System Regulation. An SPDF is a set of processes that help identify and reduce the number and severity of vulnerabilities and encompasses all aspects of the product lifecycle. These processes may be integrated with existing quality systems. The guidance document includes information regarding:

- Designing for security – Confirming that security objectives for authenticity, authorization, availability, confidentiality and secure and timely updates and patches are provided, and that these are implemented throughout the device architecture.
- Transparency – Information necessary to integrate the device into its use environment, as well as information necessary to maintain the cybersecurity of the medical device over its lifecycle must be sufficiently and effectively communicated to device users.
- Submission documentation – Providing documentation to demonstrate assurance of safety and effectiveness, including cybersecurity information.
- Security risk management – Distinct from risk management as described in ISO 14971, this focuses on harms that can occur due to compromise of the device's security, taking into account the larger system within which the medical device operates. The FDA recommends implementing a risk management plan and report such as that described in AAMI TIR57.
- Threat modeling – Identification of system risks, mitigations, and consideration of pre- and post-mitigation of cybersecurity issues. This includes risks introduced in the supply chain, manufacturing, deployment, interoperability, maintenance and update activities and decommissioning.
- Software Bill of Materials (SBOM) – Includes in-house developed and third party-components with dependencies identified.
- Security assessment of unresolved anomalies – The impact of anomalies on safety and effectiveness.
- Total product life cycle security risk management – Continuous update of control processes as new threats, vulnerabilities, assets or adverse impacts are discovered.
- Security architecture – Defining the software, any internal and external connections, as well as any interactions. This includes information on how the system is secured and a demonstration that risks have been considered and are sufficiently controlled, giving assurance of the safety and effectiveness of the medical device system.
- Cybersecurity testing – Showing threat mitigation, robust vulnerability testing and penetration testing.
- Labeling to identify the relevant security information to users.

Proactive post-market evaluation is vital, as cybersecurity risks are continually evolving. A comprehensive cybersecurity risk management process must be implemented to address these emerging issues during the life cycle of the device. A structured and systematic approach to updates, patches and monitoring can include methods to identify vulnerabilities during the life of the device, and methods to detect, analyze and assess threats. The guidance *Postmarket Management of Cybersecurity in Medical Devices*, issued Dec. 28, 2016, provides references to tools that can be considered. In addition, there are evolving methods to identify and analyze cybersecurity threats; therefore, it is important to stay vigilant in identifying these.



Components of a cybersecurity framework

The *Playbook for Threat Modeling Medical Devices* cited above calls attention to the Threat Modeling Manifesto. An organization of individuals with years of experience in threat modeling for security or privacy have distilled their collective threat modeling knowledge to inform, educate and inspire adoption of threat modeling and to improve security and privacy during development. The website, threatmodelingmanifesto.org offers a plethora of available information[14]. The model asks four key questions:

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good enough job?

The Playbook recognizes controls such as the National Institute of Standards and Technology (NIST) Special Publication 800-53 and ANSI/AAMI/IEC 80001 for confirming baseline security capabilities but fails to address ways that medical devices are used, interface in the healthcare ecosystem and how security risks can result in unacceptable safety issues.[15]

The Playbook presents ways to approach threat modeling and includes examples of how to incorporate the threat modeling methods. Using data flow diagrams to represent entities involved with the function of the medical device, the relationships involved, and defining trust boundaries can be useful tools in threat modeling. The Playbook addresses the question of what can go wrong with the use of the STRIDE method (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege). Another method for identifying threats involves attack trees. This involves identifying a specific threat and then determining ways it could occur. In addition, the Playbook discusses the use of kill chains and cyberattack lifecycles. The idea is to disrupt the attacker so that the end goal is not reached. Additional methods of identification and controls are discussed in the document. We highly recommend downloading this document as a resource within the organization.

In addition to the Playbook, we recommend reading and implementing the suggestions in the white paper publication cited above, *Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks*, where the organization has legacy devices in the field. Managing risks in legacy devices is important over the lifecycle of devices to safeguard patient safety from growing and evolving cyberattacks.

Using NIST's framework Version 1.1 "Identify, Protect, Detect, Respond and Recover" concept, the following core functions can be incorporated into a viable cybersecurity framework:

- Identify and protect – Manufacturers should identify security controls best suited to their devices' intended uses, electronic data interfaces, intended operating environments and specific cybersecurity vulnerabilities.
  - Examples – Limiting device access to trusted users via authentication and timed sessions; supporting trusted content through restricted software and firmware upgrades, secure data transfers and encryption methods.
- Detect, respond, recover – Manufacturers should implement features that enable users to detect security breaches, as well as instruct users on what to do if such breaches occur. Additional features should be in place to support a device's critical functioning even in the event of a security compromise.
  - Examples – These may include a data backup process that can timestamp the information and recover valid data after an incursion. The software program should not be inert, meaning that it should have the capability to check certain parameters to detect malicious content.

The NIST updated version 2.0 has been released (Feb. 26, 2024)[16]. This framework involves looking at the core, tiers and profile of systems. This updated framework maps to resources that provide additional guidance on practices and controls to achieve acceptable outcomes. A draft of the updated version is available on the NIST CSF website[17]. The update provides increased guidance on CSF implementation, emphasizes cybersecurity governance and supply chain risk management, and clarifies understanding of cybersecurity measurement and assessment.

Cybersecurity and FDA premarket submissions

Once a manufacturer has implemented adequate cybersecurity measures and controls for the design and development phases of its device, that firm must provide documentation of those efforts in premarket submissions to the FDA.

Post-market shared responsibilities

Of course, cybersecurity issues do not end once a networked or connected device leaves a manufacturer and is sold to an end-user. The FDA released the post-market guidance cited above to help address cybersecurity challenges for marketed devices.

The guidance makes clear that U.S. regulators consider manufacturers to be responsible for monitoring and mitigating cybersecurity risks for their devices as part of their overall post-market obligations. The FDA characterizes cybersecurity as a shared responsibility between industry, health technology developers and vendors, users, patients, and government, but demarcates particular tasks to device manufacturers.

Post-market cybersecurity efforts should be carried out according to 21 CFR Part 820 mandates such as complaint handling, corrective and preventative actions, quality audits and software validation and risk analysis, according to the guidance. These activities are managed through established procedures in the quality system that should link these activities together to confirm any issues identified are managed through the systems. As an example, if customer feedback is raised about cybersecurity, the organization should review risk analyses and initiate corrective action as needed. A well-established post-market system will allow cybersecurity issues to be identified, evaluated, corrected, and effectively communicated to the relevant users, designers, regulatory agencies and other stakeholders.

Exploitability and severity concerns

The FDA recommends that manufacturers establish risk management processes focusing on the exploitability and severity of device cybersecurity vulnerabilities.

Assessing the exploitability of a cybersecurity vulnerability can prove highly challenging, according to the agency. Furthermore, conventional risk management tools for medical devices often fail to provide an accurate measure of exploitability. Thus, the FDA recommends tools such as the Common Vulnerability Scoring System[18], which provides numerical ratings according to four metric groups: Base, Threat, Environmental and Supplemental, with each set providing descriptions of possible metric values: not defined, high, medium, low, negligible and no (none) likelihoods of exploitability. This tool also includes supplemental metrics for safety, automatable, provider urgency, recovery, value density, vulnerability response effort, and descriptions of qualitative severity rating scales.

Conclusion

Cybersecurity must be implemented in the design process, the quality system, and post-market activities of medical device companies to support medical device functionality and safety. The use of wireless, networked, and other connected devices exchanging healthcare information is increasing and will continue with the application of technology to traditional medical devices.

Organizations should utilize the tools that have been published, such as the FDA guidance documents and risk management standards and tools that are incorporated into design controls to start analyzing the need for cybersecurity with software. Effective implementation of cybersecurity measures will enable operational and safe products in the medical device industry.

End Notes

1. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software
2. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-device-software-functions
3. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
4. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
5. https://www.mitre.org/news-insights/publication/playbook-threat-modeling-medical-devices
6. https://www.mitre.org/news-insights/publication/next-steps-toward-managing-legacy-medical-device-cybersecurity-risks
7. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
8. https://www.fda.gov/medical-devices/how-study-and-market-your-device/estar-program
9. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm
10. 21 CFR 820.30(i) https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm
11. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software
12. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-device-software-functions
13. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
14. https://www.threatmodelingmanifesto.org/
15. https://www.mitre.org/news-insights/publication/playbook-threat-modeling-medical-devices
16. https://www.nist.gov/cyberframework
17. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf
18. https://www.first.org/cvss/specification-document

Learn more

Need help with bringing a medical product to market? Emergo by UL helps medical technology developers bring their medical devices to market in the U.S. and other markets worldwide. Here's how we help:

- FDA 510(k) and de novo submissions
- Quality management system compliance
- QMS internal and supplier inspections

Learn more about global market access for medical devices at **EmergobyUL.com**.

About the author

Linda Chatwin, Esq, RAC is Lead Quality and Regulatory Consultant at Emergo by UL. She has over 35 years of experience with medical products. Through years of watching regulations evolve and change, she knows how to navigate the global regulatory maze and bring products to market. Ms. Chatwin has helped manufacturers obtain approvals for a wide range of products, and she remains involved in changing requirements for medical devices worldwide. She has navigated many FDA inspections, including those focused on pharmaceuticals and Part 11 compliance, and other regulatory authority audits, and negotiated favorable outcomes with the FDA. Currently, she assists clients with regulatory issues and challenges, including implementation of UDI processes, mock audits, in-depth training on regulatory requirements, and consulting on quality system development and improvement, CFR Part 11 compliance, combination products (21 CFR Part 4), and the MDSAP audit model. She has also conducted numerous training sessions and gap assessments for the EU Medical Device Regulations, as well as SaMD requirements.

EMERGO

by UL

CS1626827