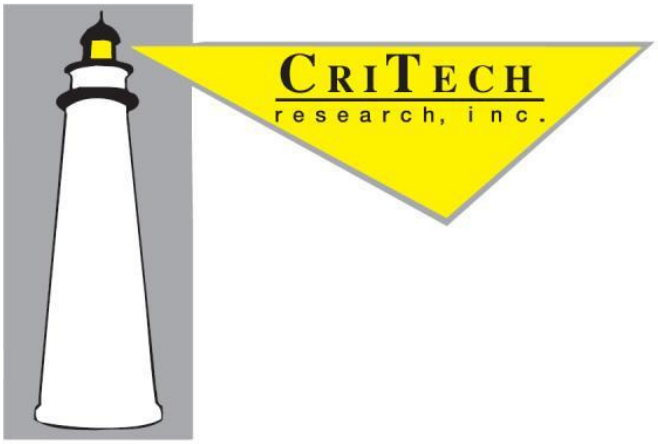

Cybersecurity for Medical Device Software

The FDA is serious about compliance.

By Bob Rajewski,

Founder and President of CriTech Research

Abstract

Cybersecurity for medical devices is **required** according to the U.S. Food and Drug Administration (FDA). Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality systems regulations (QSRs), requires that medical device manufacturers address risks, including cybersecurity risk. [1]

Medical device manufacturers are **required** to make risk-based decisions and conduct risk management activities as a part of the design, manufacture, and production of medical devices or in general as part of the quality system. In addition, the regulation of medical devices incorporates risk-based decisions to assure devices are safe and effective. [2]

Now, because of the rapidly evolving nature of cyber threats, the FDA is updating its guidance to make sure it reflects the current threat landscape so that manufacturers can be in the best position to proactively address cybersecurity concerns when they are designing and developing their devices. This is part of the total product lifecycle approach to device safety, in which manufacturers must adequately address device cybersecurity from the design phase through the device's time on the market to help ensure patients are protected from cybersecurity threats. [3]

On December 29, 2022, President Biden signed a new statute that will significantly impact medical device cybersecurity regulation. Section 3305 of the Consolidated Appropriations Act of 2023 ("Section 3305") authorizes the Food and Drug Administration (FDA) to establish cybersecurity standards for medical devices.

With the passing of this new law, the FDA now has the authority and funding to establish security requirements for pre-market medical devices. The new law **requires** the manufacturers of internet-connected medical machines to reasonably ensure that their equipment and related systems are cybersecure. [4]

Introduction

In recent years, the rapid advancements in medical device software have resulted in a significant increase in the complexity of medical devices. With this complexity, the risks of cybersecurity breaches and attacks on medical devices have also increased. The Food and Drug Administration (FDA) is responsible for ensuring that medical devices are safe and effective for their intended use, which includes addressing cybersecurity risks. Medical device manufacturers must comply with FDA regulations before their products can be marketed and sold in the US.

This white paper will discuss the importance of medical device software cybersecurity and the regulatory requirements imposed by the FDA on medical device software

cybersecurity. It will also provide guidance for medical device manufacturers on how to ensure that their medical device software is secure and meets the FDA's requirements.

Overview of Medical Device Software Cybersecurity

Medical device software cybersecurity refers to the protection of medical devices and their software from unauthorized access, modification, or disruption that could lead to patient harm. As the healthcare industry increasingly adopts digital communication technologies, cyber-attacks have become more common, leading to a rise in patient safety risks. Medical devices, particularly those connected to the internet, are prime targets for cyber-attacks due to their high value, the sensitive data they handle, and their potential to disrupt healthcare operations.

Importance of Medical Device Software Cybersecurity

Medical device software plays a crucial role in the diagnosis, treatment, and management of many medical conditions. Cybersecurity threats can take various forms, such as malware, hacking, unauthorized access, denial of service attacks, and others. Cybersecurity risks associated with medical device software can have severe consequences, including compromising patient privacy, affecting patient safety, and disrupting the availability of critical medical services. Cybersecurity breaches can result in patient harm, financial loss, reputational damage, and regulatory penalties.

Medical devices have a typical lifespan of seven or more years, during which they may become more vulnerable to cybersecurity threats as technology and the threat landscape evolves. Therefore, it is essential to ensure medical device software cybersecurity risk control measures are continually monitored, updated and improved to address new and emerging threats.

FDA Regulatory Requirements for Medical Device Software Cybersecurity

The FDA has issued key guidances to medical device manufacturers on the cybersecurity of medical devices. The guidances, entitled "**Content of Premarket Submissions for Management of Cybersecurity in Medical Devices**" and **Postmarket Management of Cybersecurity in Medical Devices**," outline the recommended steps for manufacturers to address cybersecurity risks.

The FDA recommends that medical device manufacturers consider cybersecurity risks throughout the device's entire lifecycle, including design, development, production, distribution, deployment, and maintenance. They should also establish and maintain a comprehensive cybersecurity risk management program, which should include the following components:

1. Identify cybersecurity risks - Identify and assess the potential cybersecurity risks associated with the medical device, including risks associated with network connections and third-party software.
2. Protect against cybersecurity risks - Develop and implement controls to protect the medical device from cybersecurity risks, including controls to limit access to the device, to detect and prevent unauthorized access, and to limit the impact of a cybersecurity incident.
3. Detect cybersecurity incidents - Establish procedures for detecting cybersecurity incidents and analyzing their potential impact.
4. Respond to cybersecurity incidents - Develop and implement procedures for responding to cybersecurity incidents, including identifying the cause of the incident, assessing the impact on the device and patient safety, and taking appropriate action to mitigate the risk.
5. Recover from cybersecurity incidents - Develop and implement procedures for recovering from cybersecurity incidents, including restoring the device to its intended function, and implementing measures to prevent a recurrence of the incident.

Risk Management

The FDA requires medical device manufacturers to develop, implement and document a risk management program to identify, assess, and mitigate cybersecurity risks associated with their devices. The risk management program should follow a structured process that includes the identification of cybersecurity risks, the assessment of the likelihood and impact of those risks, the development of risk control measures, and the monitoring and updating of the device throughout its lifetime. The risk management plan needs periodic updating to address changing threats.

The risk management program should also include an evaluation of the potential impact of a cybersecurity incident on patient safety and the continuity of healthcare operations. Manufacturers should identify and assess potential vulnerabilities in their devices and take measures to address those vulnerabilities. They should also implement appropriate cybersecurity controls to prevent unauthorized access, modification, or disruption of the device's operation.

The FDA also requires medical device manufacturers to document their cybersecurity risk management program in the premarket submission. The documentation should include a summary of the cybersecurity risks and the risk management program, including the controls implemented to protect against cybersecurity risks and the procedures for detecting, responding to, and recovering from cybersecurity incidents.

In addition to the recommended steps outlined in the guidance, the FDA has also issued regulations related to security of medical devices. The regulations, found in 21 CFR

Part 820, require medical device manufacturers to establish and maintain procedures for addressing non-conformities and taking corrective and preventive actions. The procedures must include addressing cybersecurity issues that could affect the device's safety and effectiveness.

Quality System Regulation

The FDA's Quality System Regulation requires medical device manufacturers to establish and maintain a quality system that ensures their products meet regulatory requirements and are safe and effective. The Quality System Regulation applies to all aspects of medical device manufacturing, including design, production, labeling, packaging, and distribution.

The Quality System Regulation requires manufacturers to establish and maintain procedures for design controls, which ensure that medical devices are designed to meet their intended use and user needs. Design controls also include risk management activities, such as the identification of hazards and the development of risk mitigation strategies.

Conclusion

The FDA's guidance on pre-market submissions and post-market surveillance for medical device software recommends that manufacturers follow a software development life cycle (SDLC) that includes specific cybersecurity activities. The SDLC should include the following cybersecurity activities:

- Threat modeling: The identification of potential cybersecurity threats to the device and its software. This includes cybersecurity risk analysis and control activities.
- Cybersecurity testing: The evaluation of the device's software for vulnerabilities and weaknesses.
- Software updates and patches: The development of a process to address updating the software to reduce cybersecurity vulnerabilities which may arise within the device over time.

Call to Action

As a medical device company CEO, company CXO, Program Manager, or Engineering Manager, it is your responsibility to ensure cybersecurity is a key part of your device’s design.

If you have not implemented a plan which addresses cybersecurity in your medical device(s) software, CriTech is here to help you.

Please contact CriTech today at 734-668-0005 and mention White Paper response. Additionally, the White Paper can be downloaded from CriTech's website at *www.critech.com*.

About CriTech Research

CriTech has provided efficient and cost-effective medical device software solutions, tailored to meet customer specific needs since 1994. We have worked on more than 500 projects and have an exceptional track record – **100% of our submissions have received FDA or EU approval.**

CriTech makes sure your medical device uses rigorously tested, fully compliant software. CriTech provides software engineering services for safety-critical software and systems. Our customers range from large, established companies to startups, with products from all FDA device classes (I, II, III), software classifications (major, moderate, minor), and IEC 62304 software safety classifications (A, B, C).

CriTech is an objective, independent third-party who's determined to make sure your software is safe and who are experts in medical device software. In addition to software cybersecurity solutions, CriTech provides software testing, software remediation, and software development. A detailed list of services is provided on CriTech's website at www.critech.com.

About Bob Rajewski

Bob Rajewski is Founder and President of CriTech Research and is a recognized industry expert in the field of medical device software engineering. He has been involved in the medical device business since 1994 and has served as an instructor for AAMI/FDA courses on software regulations and software verification and validation. Bob has been an active and excited participant in cybersecurity conferences and working groups.

References:

[1] FDA.gov, “FDA Fact Sheet – THE FDA’S ROLE IN MEDICAL DEVICE CYBERSECURITY,” [Online]. Available: https://www.fda.gov>cybersecurity-fact-sheet [Accessed 16 March 2023].

[2] FDA.gov, "Workshop & Conferences (Medical Devices)>CDRH Industry Basics: Understanding Risk with Medical Devices," 15 November 2022. [Online]. Available: https://www.fda.gov/medical-devices/workshops-conferences-medical-devices/virtual-public-workshop-cdrh-industry-basics-understanding-risk-medical-devices-11152022 [Accessed 16 March 2023].

[3] Caccomo, Stephanie, "FDA in Brief," 17 October 2018. [Online]. Available: https://www.fda.gov/news-events/fda-brief/fda-brief-fda-proposes-updated-cybersecurity-recommendations-help-ensure-device-manufacturers-are [Accessed 16 March 2023].

[4] R. Hattersley, "Campus Safety Magazine," 19 January 2023. [Online]. Available: https://www.campussafetymagazine.com/news/enables-fda-regulate-medical-device-cybersecurity/ [Accessed 16 March 2023].