BEANSTOCK VENTURES

Navigating FDA Cybersecurity Requirements for Medical Devices

WHITEPAPER

This whitepaper discusses the standards and requirements needed for a successful FDA submission and clearance for a cyber medical device.

BeanStock Ventures provides resources for businesses that help to ensure regulatory compliance and prevent unnecessary costs and delays.

GUD-MKT-012-01 BeanStock Ventures © 2024

Navigating FDA Cybersecurity Requirements for Medical Devices

Written by the experts at BeanStock Ventures

Cybersecurity Requirements

Details of specific cybersecurity requirements set by the FDA and why they are important to your business

Common Pitfalls

A list of frequently encountered issues that lead to rejections or delays

Practical Strategies

Actionable steps and best practices for ensuring submissions meet all necessary criteria

Resources and Tools

Training, templates and resources that can help streamline the submission process.

What's Really Needed to Clear a Cyber Medical Device with the FDA?

BEANSTOCK VENTURES

Cybersecurity Requirements

Under section 524B of the Federal Food, Drug, and Cosmetic Act, any person submitting an application under sections 510(k), 513, 515(c), 515(f), or 520(m) for a device defined as a cyber device must provide information ensuring compliance with cybersecurity requirements. A cyber device is defined as one that:

Includes software validated, installed, or authorized by the sponsor as a device or within a device,

Has the ability to connect to the internet,

Contains technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

PRE-MARKET CYBERSECURITY REQUIREMENTS

The FDA has outlined specific pre-market and post-market cybersecurity requirements. Pre-market submissions are necessary to demonstrate that the device is safe and effective for market approval. The key design deliverables required in pre-market submissions include:

Documentation of identified risks and the measures taken to mitigate them.

Analysis of potential cybersecurity threats and their impact.

Evaluation of the risks associated with the device.

A comprehensive list of all software components used in the device.

Report on any known issues that have not been resolved.

Quantitative measures used to assess the effectiveness of cybersecurity controls.

Specific measures implemented to protect the device from cyber threats.

Diagrammatic representation of the device's architecture.

Results of tests conducted to assess the device's cybersecurity.

Information provided to end-users about managing cybersecurity risks.

Ongoing plan for managing and monitoring cybersecurity risks throughout the device's life cycle.

PRE-MARKET CYBERSECURITY REQUIREMENTS

Once devices are on the market, medical device manufacturers and other firms involved in distribution must adhere to post-market cybersecurity requirements. This involves the implementation of the Cybersecurity Management Plan, monitoring cybersecurity metrics, and maintaining cybersecurity controls. Effective post-market surveillance ensures that devices continue to be secure and helps in the timely identification and mitigation of new cybersecurity threats.

By meeting the FDA's cybersecurity requirements, manufacturers can ensure that their medical devices are both safe and effective, thereby protecting patients and maintaining compliance with regulatory standards.

Common Pitfalls

As an FDA-accredited third-party review organization and regulatory consultants, we have reviewed numerous submissions and identified common issues that frequently lead to rejections or delays. These issues can often be prevented.

INADEQUATE IMPLEMENTATION OF CYBERSECURITY TECHNICAL CONTROLS

Insufficient mechanisms for verifying the identity of users or systems. Weak controls over permissions and access levels.

Poor implementation of encryption and data protection methods.

Lack of measures to ensure that software and data remain unaltered.

Inadequate protections for sensitive information.

Insufficient logging of security events and incidents.

Weak strategies for maintaining system uptime and reliability.

Lack of robust plans for system recovery after a cybersecurity incident.

Ineffective processes for deploying security updates.

RELIANCE ON UNSUPPORTED PLATFORMS

Medical devices relying on operating systems or software platforms that have reached end-of-life and no longer receive security updates throughout the device's expected lifespan.

WEAK VULNERABILITY IDENTIFICATION

Insufficient identification and analysis of existing and potential vulnerabilities, failing to demonstrate that the product is secure against cyber threats.

INCOMPLETE TECHNICAL INFORMATION

Lack of comprehensive documentation, including use cases, architectural views of the system, and descriptions of the operational environment, making it difficult for reviewers to assess the adequacy of cybersecurity controls.

INADEQUATE LABELING

Failure to provide clear and effective labeling that informs end users about managing cybersecurity risks associated with the device.

Recent trends in cybersecurity voluntary medical device recalls highlight areas vulnerability, including:

Gaps in access controls allowing unauthorized use.

Vulnerabilities leading to service disruptions.

Changes to system settings that impact essential performance.

Transmission of sensitive information in unsecure formats.

These vulnerabilities often necessitate costly corrective actions such as customer communication, software updates, field service interventions, and specific customer actions.

Practical Strategies

Here are practical strategies for ensuring your FDA submission meets all cybersecurity criteria, based on successful clearances we've observed.

IMPLEMENTATION OF CYBERSECURITY TECHNICAL CONTROLS

Ensure that all critical device data, including settings that impact device performance, is authenticated to prevent spoofing or tampering.

Utilize robust password policies, avoid hard coded or commonly shared passwords, and implement two-factor authentication for administrative access.

Avoid storing system-critical information in simple text files. Use secure methods that restrict unauthorized access and modifications.

Apply digital signatures to software and firmware to confirm their integrity and authenticity.

Ensure that debug controls and ports are not exposed to prevent potential exploitation.

Safeguard patient privacy both during transmission and when data is at rest.

Go beyond basic operating system logging by incorporating extended logging practices for comprehensive breach investigation.

Add mechanisms to detect tampering or corruption of critical system information and provide means for restoration.

Verify that all software, including operating systems and third-party components, can be updated to address vulnerabilities.

Prevent unauthorized downgrades of software and operating systems to avoid security risks.

RELIANCE ON PLATFORMS

Ensure that your system is updated to the latest versions of operating systems and third-party software before submission. Alternatively, secure agreements with vendors for ongoing support and updates.

VULNERABILITY IDENTIFICATION

Contract with external experts for thorough testing, threat modeling, and evaluation of your submission. Utilize automated tools for vulnerability detection and review common vulnerabilities related to similar devices.

TECHNICAL INFORMATION

Organize technical design reviews with independent experts to ensure that use cases, system architecture, and operational environment descriptions are comprehensively defined for third-party reviewers.

LABELING

At the end of the development process, evaluate all cybersecurity risks and controls. Develop a risk management matrix and ensure that any controls requiring user action or awareness are clearly included in customer labeling. Verify that end-user controls are effective and enable users to manage risks appropriately.

Resources and Tools

Ensure your FDA submission meets and exceeds all cybersecurity criteria with our industry-leading resources and expert solutions. Our offerings are crafted to support and enhance your compliance efforts, drawing from our extensive track record of successful clearances.

TEMPLATES

BeanStock Ventures provides a comprehensive DIY Cybersecurity Regulatory Kit designed to streamline your FDA submission process. This all-in-one toolkit includes:

Cybersecurity Templates: Access a complete set of high-quality templates for your medical device file creation. Our templates are tailored to meet regulatory requirements and help you compile a robust SiMD/SaMD technical submission.

Guidance and Best Practices: Benefit from our step-by-step guidance and industry best practices to effectively complete your submission.

Cost and Time Savings: Save over $100k and 9 months in FDA preparation with our cost-effective kit, which includes continuously updated content to keep your team informed and compliant.

Start with a free starter version of our regulatory kits: https://grassrootsdx.beanstockventures.com/diy-software-regulatory-kit

TRAINING

Included in the DIY Cybersecurity Regulatory Kit is a 12-month subscription to Software Online Agile Regulatory (SOAR®), featuring 16 specialized 90-minute training modules on cybersecurity. This course covers:

Regulatory Requirements: Broad and specific cybersecurity regulations, including FDA guidelines and industry standards.

Practical Implementation: How to apply regulations, standards, and best practices effectively.

Agile Impact: Understanding Agile's role and application in cybersecurity.

Enroll separately for this course here: https://grassrootsdx.beanstockventures.com/course/course-16-cybersecurity/

CONSULTING

Leverage our seasoned experts to navigate FDA cybersecurity requirements with ease. Our consulting services include:

Technical File Creation: Assistance with design history file or technical file preparation.

Remediation and Review: Address and resolve compliance issues through detailed technical reviews and audits.

FDA Interaction: Support with additional information requests related to cybersecurity.

Receive personalized, expert support throughout your submission process, ensuring that your cybersecurity strategy is both effective and compliant.

DEFINITIONS

Cyber Device: A medical device that includes software validated, installed, or authorized by the sponsor as a device or within a device, has the ability to connect to the internet and contains technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

MDF (Medical Device File): A repository of all documents related to your medical device.

IEC 62304: An FDA Recognized Consensus Standard which defines the life cycle requirements for medical device software. The set of processes, activities, and tasks described in this standard establishes a common framework for medical device software life cycle processes. Applies to the development and maintenance of medical device software when software is itself a medical device or when software is an embedded or integral part of the final medical device.

ISO 13485: An international regulatory standard that specifies the requirements for Quality Management Systems (QMS) in the medical device industry.

QMS (Quality Management System): A set of policies, processes, procedures, and resources implemented within an organization to ensure that its products or services consistently meet or exceed customer expectations and comply with applicable regulations and standards.

REFERENCES

AAMI TIR57:2016 (R2019) Principles for medical device security - Risk management

AAMI TIR97:2019 - Principles for medical device security - Postmarket risk management for device manufacturers

ANSI UL 2900-1 Ed. 1-2017 - Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

FDA 21 CFR 820 Quality System Regulation

FDA-2021-D-1158 Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

FDA-2015-D-5105 Postmarket Management of Cybersecurity in Medical Devices

IEC 62304 - Medical Device Software – Software Life Cycle Processes

IMDRF/CYBER WG/N60FINAL:2020 Principles and Practices for Medical Device Cybersecurity

ISO 14971 Medical devices — Application of risk management to medical devices

ISO/IEC 27001:2013 Plus Redline - Information technology - Security techniques - Information security management systems - Requirements (includes Redline Version)

ISA/IEC 62443 Series of Standards: defines requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS).

MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices

NIST Cybersecurity Framework ver. 1.1 (April 16, 2018)

NIST EO 13636 Framework for Improving Critical Infrastructure Cybersecurity