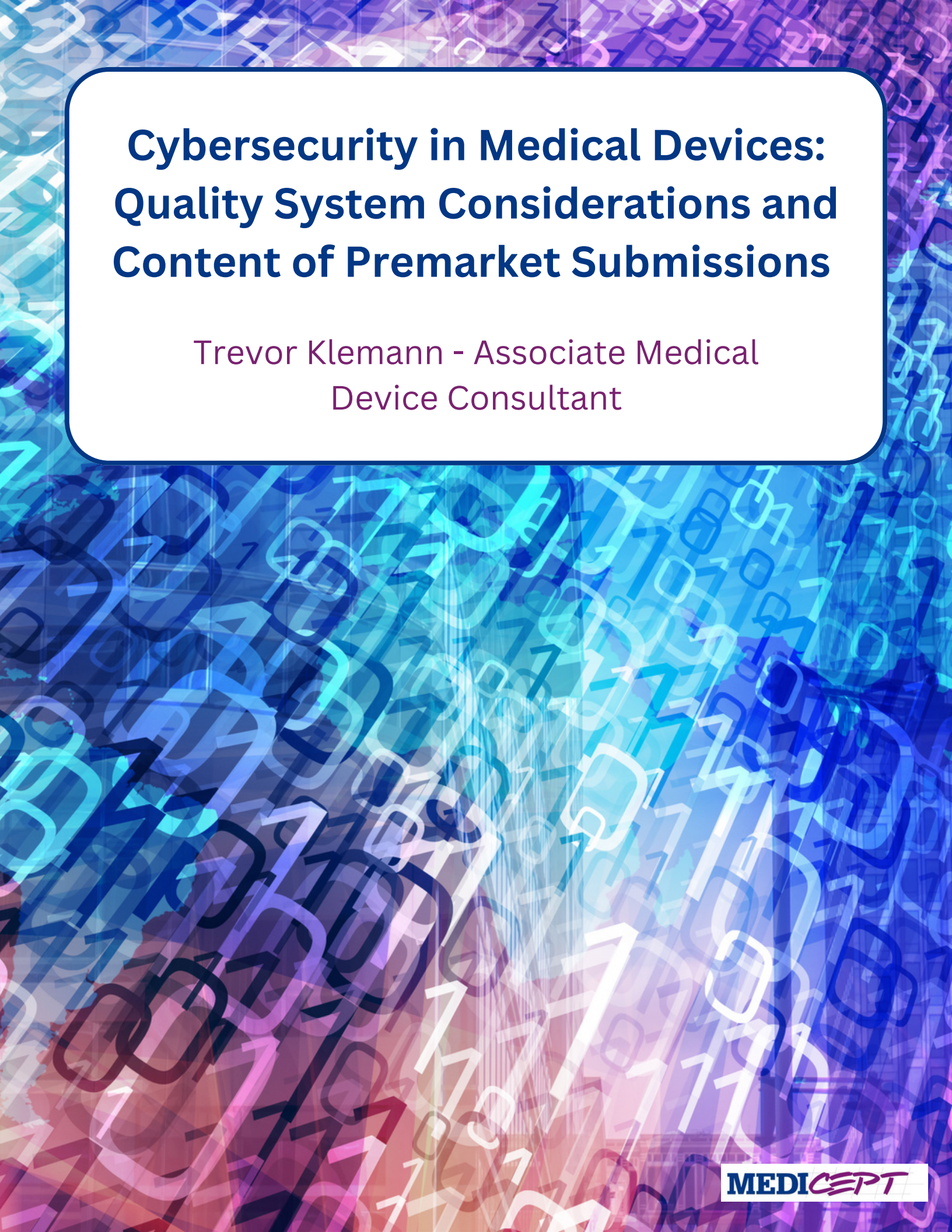
Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Trevor Klemann - Associate Medical Device Consultant



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Introduction

The new FDA Guidance document "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" discusses the increasing importance of cybersecurity controls in the context of medical devices due to the growing integration of wireless and network-connected capabilities, as well as the exchange of health information. The guidance is applicable to devices with cybersecurity considerations, including but not limited to devices that have a device software function or that contain software (including firmware) or programmable logic. The guidance highlights that medical devices are now part of larger interconnected systems, emphasizing the need for comprehensive cybersecurity considerations. The guidance clarifies that FDA recommendations are not legally binding but provide guidance on cybersecurity for devices, including those that contain software or have network connectivity. It applies to various premarket submission types and all types of devices under the Federal Food, Drug, and Cosmetic Act as well as certain drug and biologic combination products.

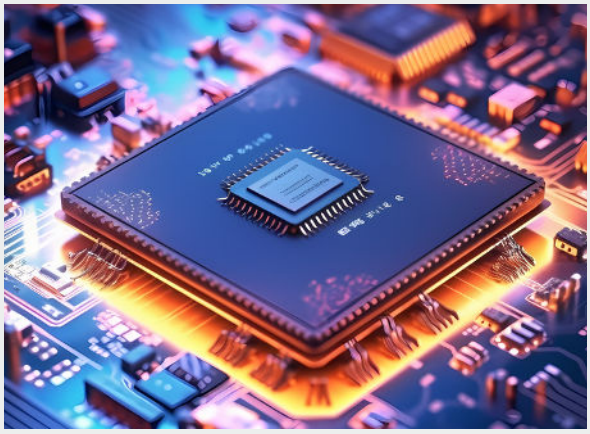
Background

Stakeholders shared responsibility premarket cybersecurity guidance in 2014 and postmarket cybersecurity guidance in 2016 but recognize the need for an updated approach to address evolving threats and emphasize secure design and mitigation throughout a device's lifecycle. This guidance introduces the concept of a Secure Product Development Framework (SPDF) and highlights the importance of risk management in device manufacturing, referencing related regulations and guidance. The guidance also aligns with international recommendations and mentions the Consolidated Appropriations Act of 2023, which adds cybersecurity requirements for certain device submissions under section 524B of the FD&C Act, defines "cyber device" and aims to help manufacturers meet these obligations.

Cybersecurity is Part of the Quality System Regulation

Device manufacturers are obligated to establish quality systems to ensure their products consistently meet requirements and specifications. These quality system requirements are outlined in 21 CFR Part 820. Depending on the device, these requirements may be relevant during the premarket phase, postmarket phase, or both. In the premarket context, demonstrating the safety and effectiveness of certain devices with cybersecurity risks may involve using documentation related to the quality system regulation.

This guidance aims to explain how such documentation, which aligns with quality system regulation compliance, can also address cybersecurity concerns for a device. For instance, the quality system regulation mandates that manufacturers of software-driven devices must establish procedures for controlling device design, including software validation and risk analysis. This software validation and risk analysis process may require the establishment of cybersecurity risk management and validation procedures for software-based devices. Software validation and risk management are integral components of cybersecurity assessments, determining whether a device is reasonably safe and effective.



FDA requires manufacturers to incorporate development processes that consider and mitigate software-related risks throughout the design and development stages, incorporating cybersecurity considerations. These processes should encompass identifying security risks, defining how these risks will be managed, and providing evidence that the controls effectively ensure adequate security in the device's usage environment.

Secure Product Development Framework

Cybersecurity threats have the potential to exploit vulnerabilities in a system, which can pose risks to patient safety. The more vulnerabilities that exist or are discovered in a system a medical device operates in, the easier it is for threats to compromise the device's safety and effectiveness. A Secure Product Development Framework (SPDF) is a set of processes designed to identify and reduce vulnerabilities in products throughout their entire lifecycle, including design, development, release, support, and decommissioning. Utilizing an SPDF during the device design phase can prevent the need for significant re-engineering when adding connectivity features after marketing or addressing vulnerabilities discovered later.

An SPDF can be integrated into existing processes for product and software development, risk management, and the broader quality system. Example SPDFs include NIST's Cybersecurity Framework (NIST SP. 800-218) and international standards like IEC 81001-5-1. FDA encourages manufacturers to use an SPDF as it helps meet Quality System (QS) regulation requirements and enhances cybersecurity. However, FDA also acknowledges that alternative approaches can satisfy the QS regulation.

When FDA reviews premarket submissions for medical devices, they evaluate device cybersecurity based on several factors, including the device's capacity to achieve and maintain specific security objectives across its architecture. These security objectives, relevant to various devices, encompass authenticity (including integrity), authorization, availability, confidentiality, secure and timely updatability and patchability.

Premarket submissions should include information detailing how these security objectives are addressed and integrated into the device's design. The extent of security requirements, architecture, supply chain considerations, and implementation will vary based on factors such as the device's intended use, electronic data interfaces, environment of use, cybersecurity risks, exploitability of vulnerabilities, and the potential harm to patients from vulnerability exploitation. The use of Secure Product Development Framework (SPDF) processes is recommended to reduce the number and severity of vulnerabilities, thereby decreasing the risk of medical device systems being exploited and causing patient harm. By incorporating SPDF into the design, a medical device system is more likely to be inherently secure, designed to remain secure within its system and network throughout its lifecycle.

The absence of essential cybersecurity information, such as details needed to integrate a medical device into its operating environment and instructions for users to maintain its cybersecurity over time, can have a detrimental impact on the device's safety and effectiveness. To address these concerns, it is crucial for device users to have access to information regarding the device's cybersecurity controls, potential risks to the device system, and other pertinent details.

Providing this information and other relevant details helps users comprehend a device system's resilience to cybersecurity threats, the specific threats it may face, and strategies for prevention and mitigation. Without this information, cybersecurity risks may remain undisclosed, improperly identified, or inadequately addressed, potentially compromising the safety and effectiveness of the device. FDA believes that cybersecurity information is essential for the safe and effective use of devices and should be included in device labeling to ensure user awareness and proper device management.

Risk Management

Device cybersecurity measures should align with the device's cybersecurity risk, which can vary based on factors like the device's intended use and its connection to networks or other devices. Manufacturers should document these cybersecurity measures, and this documentation can support FDA premarket submissions. Cybersecurity controls must also consider the device's use environment, as cybersecurity risks evolve over time.

The FDA evaluates cybersecurity information in premarket submissions to ensure device safety and effectiveness. Inadequate cybersecurity information in device labeling can result in misbranding, and non-compliance with section 524B requirements for cyber devices is considered a prohibited act. The guidance provides recommendations for cybersecurity information in premarket submissions, focusing on the specific cybersecurity risk assessed during device development, and these recommendations apply broadly to support FDA's safety and effectiveness assessments.

The guidance is based on FDA's experience in evaluating devices with cybersecurity vulnerabilities but allows sponsors flexibility in their approach and documentation, provided they meet premarket submission requirements. Given the growing interconnectedness of medical devices, addressing cybersecurity risks during device design is essential. The use of a Secure Product Development Framework (SPDF) is recommended to create safe, effective, trustworthy, and resilient devices that can be managed by manufacturers and users. Manufacturers are encouraged to utilize device design processes outlined in the Quality System regulation or consider alternative frameworks that align with FDA's recommendations for SPDF.

The guidance offers recommendations for SPDF processes and required documentation for premarket submissions, though it does not encompass a complete SPDF, and it does not suggest discontinuing existing effective processes.

Assessing safety and security risks in medical device systems is crucial, considering the evolving cybersecurity landscape. Security risk management processes should be integrated into a manufacturer's quality system throughout the device's lifecycle. Security risk management differs from safety risk management due to its broader scope and consideration of indirect and direct patient harm. Manufacturers should conduct both safety and security risk assessments for a comprehensive understanding of risks.

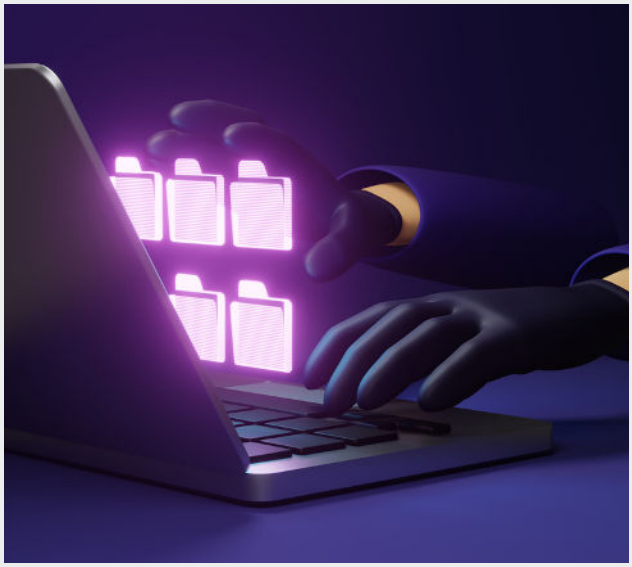
Devices should be designed to mitigate known vulnerabilities, with compensating controls considered when full mitigation isn't feasible. When vulnerabilities remain, they should be addressed as foreseeable risks, either through additional controls or user/patient risk transfer. Manufacturers should create security risk management plans and reports, following guidelines like AAMI TIR57, and include them in premarket submissions to demonstrate device safety and effectiveness. These reports should detail risk assessment methods, residual risk conclusions, risk mitigation activities, and traceability between relevant documentation. In essence, security risk management is vital for addressing cybersecurity risks in medical devices, and thorough documentation supports device safety and effectiveness.

Security

Manufacturers are responsible for identifying and mitigating cybersecurity risks in their devices and related systems, including those associated with hospital networks and cloud infrastructure. A well-defined security architecture is essential, encompassing high-level definitions and detailed implementations. FDA recommends that manufacturers incorporate security considerations into their design and development plans and procedures, covering design processes, requirements, and acceptance criteria related to the security architecture.

Premarket submissions should include documentation on the security architecture, helping FDA understand the device's context and trust boundaries, including interactions with external entities. Manufacturers should analyze system-level risks, supply chain considerations, and deployment scenarios. FDA outlines specific Security Architecture Views to document security controls and the resulting security architecture in premarket submissions.

Testing is essential to demonstrate the effectiveness of cybersecurity controls in medical devices. While related to software development, cybersecurity controls require specific testing to ensure device safety and effectiveness. Manufacturers should include security testing documentation in premarket submissions, covering aspects like security requirements, threat mitigation, vulnerability testing, penetration testing, and more. Penetration test reports should detail testing methods, results, and testers' independence. Testing should identify vulnerabilities and anomalies, and manufacturers should assess their security impacts as part of the security risk management process. Future software releases should address issues identified during testing, with plans outlined in premarket submissions. FDA recommends cybersecurity testing throughout the device development lifecycle, from early development to post-release testing, performed at regular intervals.



Cybersecurity Transparency

FDA regulates device labeling to ensure it provides adequate directions for use and does not mislead users. For devices with cybersecurity risks, informing users through labeling can help comply with requirements and mitigate risks. Manufacturers should include security information in labeling, considering the user's technical knowledge. Information may include cybersecurity controls, network interfaces, infrastructure requirements, security event responses, and more.

Manufacturers should provide machine-readable Software Bill of Materials (SBOM) information to users, describe procedures for software and firmware updates, and explain how the device responds to security events. Additionally, labeling should cover backup and restore features, secure configurations, forensic evidence capture, end-of-support information, and secure decommissioning. A Manufacturer Disclosure Statement for Medical Device Security (MDS2) and Customer Security Documentation can address many of these recommendations.

Cybersecurity Management Plans

FDA recommends that medical device manufacturers establish a plan for identifying and communicating vulnerabilities that arise after a device's release. This plan should be included in premarket submissions and outline how the manufacturer will maintain the device's safety and effectiveness post-authorization.

The cybersecurity management plan should cover personnel responsible for monitoring and identifying vulnerabilities, sources and methods for vulnerability identification like the NIST National Vulnerability Database, addressing vulnerabilities from authoritative sources like CISA Known Exploited Vulnerabilities Catalog, periodic security testing, patch development and release timelines, update processes, patching capabilities, coordinated vulnerability disclosure, and communication of remediations, patches, and updates to customers. Further guidance on coordinated vulnerability disclosure plans is available in FDA's Postmarket Cybersecurity Guidance.

Conculsion

Navigating cybersecurity device design, labeling and documentation for premarket submissions can be a complex challenge for manufacturers. This MEDIcept White Paper investigates the new FDA guidance that discusses the increasing importance of cybersecurity controls in the industry.

This White Paper discussed a few important aspects such as secure product development framework, risk management and security architecture and provides manufacturers with an understanding of how to navigate cybersecurity controls, especially when it comes to quality system considerations and premarket submissions.

Call to Action

If you are curious about additional ways to improve your cybersecurity controls, MEDIcept has quality engineering experts who stand ready to help. Reach out to us today at sales@medicept.com.

About MEDIcept

MEDIcept is an international medical device, IVD, combination product, and biotechnology compliance consulting firm. For over 27 years, our unique consulting practice has assisted thousands of companies of all sizes with cost-effective Regulatory, Quality, Clinical, Auditing, and Educational Services. Our experienced team of former FDA, Notified Body, and industry experts will work with you to efficiently develop or remediate a quality system, create a regulatory strategy, or establish a clinical trial, to meet your specific needs.

References

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions