medcrypt

APRIL 2022 UPDATE

Published September 2022

TOOLS AND PROCESSES FOR MEDICAL DEVICE CYBERSECURITY

Complying with FDA premarket cybersecurity guidances requires a variety of processes and technologies. For manufacturers, this means finding a balance between building their own or relying on commercial offering.

BACKGROUND

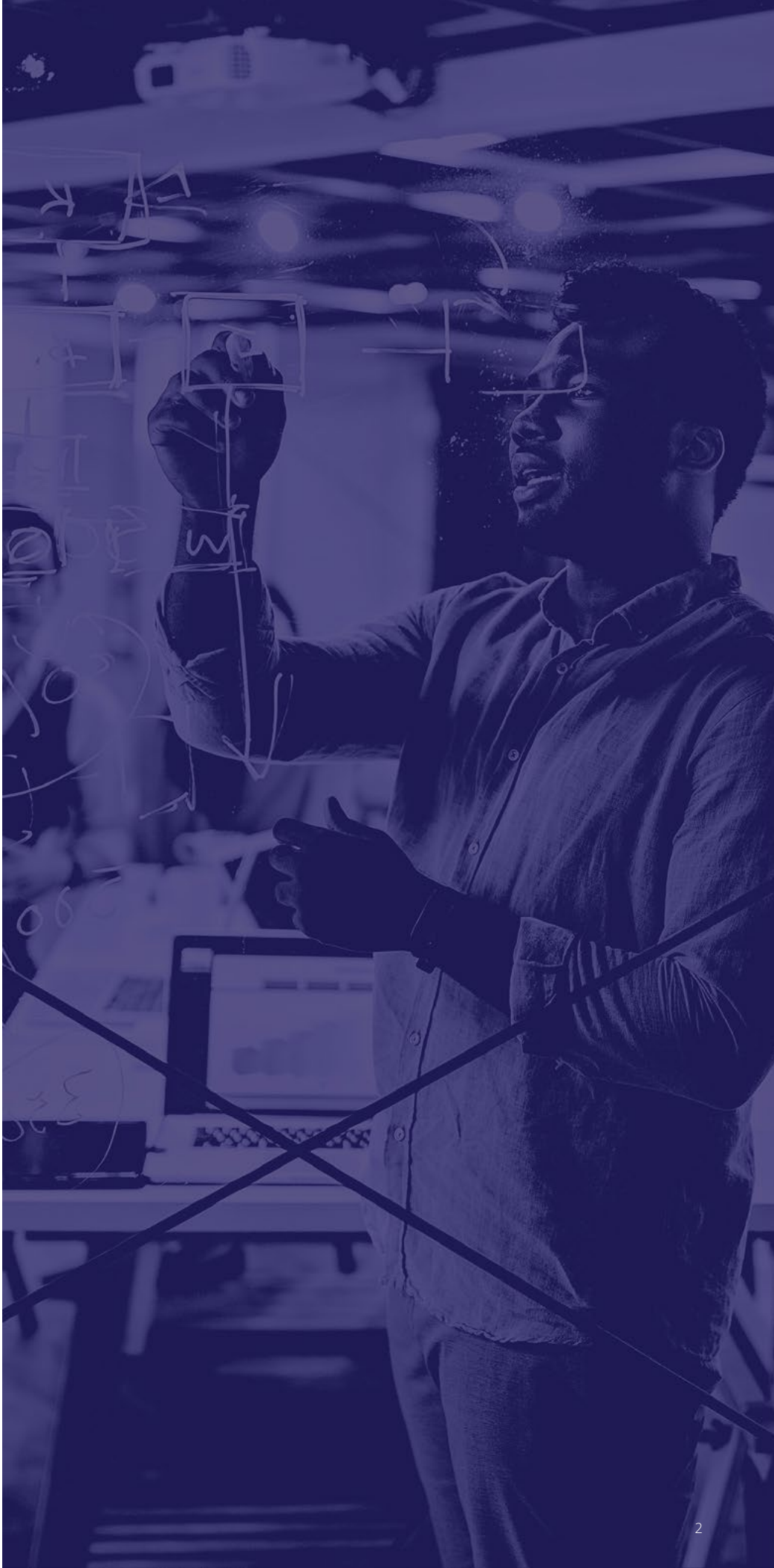
The Food and Drug Administration (FDA) issued an updated draft of the Premarket Cybersecurity Guidance in April 2022 which, when combined with existing finalized Postmarket Management of Cybersecurity in Medical Devices Guidance, specifies process and technical requirements to ensure medical devices are "secure by design" and that their security posture can be maintained over the lifetime of the device.

In this paper we propose a hypothetical medical device vendor's mature cybersecurity program that complies with FDA guidances, and we will analyze the processes and tools that aid in their success.

READERS WILL LEARN

Whether you're a research & development leader, engineer or engineering manager, quality regulatory analyst, or anyone else involved in medical device cybersecurity, this whitepaper will inform decisions around product cybersecurity.

- Quality management systems need to include cybersecurity considerations during all product lifecycle phases
- Both internal and external cybersecurity signals need to be analyzed during the operational life of the product
- Devices with security features at their core will minimize the overall cost of cybersecurity over the life of the product
- A variety of commercial tools exist that can help address medical device cybersecurity



SECTION I: CYBERSECURITY INTEGRATES INTO DEVICE LIFECYCLE

FDA Guidance Requires Both Processes and Tools

The recent release of the FDA's Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance (formerly known as the Premarket Cybersecurity Guidance) roots cybersecurity deep into the lifecycle processes for medical devices and does so from an early stage.

The guidance consists of both processes (processes through which security is managed) and tools (technologies that support security processes and controls) that must be implemented to meet both the regulator and customer expectations.

EXAMPLE PROCESS

"A Secure Product Development Framework (SPDF) is a set of processes that help reduce the number and severity of vulnerabilities in products. An SPDF encompasses all aspects of a product's lifecycle, including development, release, support, and decommission."

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, section IV.A Line 153.

EXAMPLE TOOL

"...manufacturers should also describe how the known vulnerabilities... were discovered to demonstrate whether the assessment methods were sufficiently robust."

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, section V.A.2,(a) Line 443.

While there are millions of medical devices in the field that have been designed without these considerations in mind, the guidance introduces an expanded scope for cybersecurity requirements, for a broad range of device types, including those covered under 510(k) applications, De Novo requests; Premarket Approval (PMAs); Product Development Protocols (PDPs); Investigational Device Exemption (IDE); and Humanitarian Device Exemption (HDE); as well as devices for which a premarket submission is not required (e.g., for 510(k)-exempt devices).

Premarket Cybersecurity Requirements

The FDA's premarket guidance suggests the following be incorporated throughout the device development lifecycle:

	AREA	REFERENCE TO GUIDANCE	PROCESS / TOOL
1	Quality system inclusive of cybersecurity	Device manufacturers must establish and follow quality systems to help ensure that their products consistently meet applicable requirements and specifications.	Process
2	Utilize a secure product development framework (SPDF) or similar	The primary goal of using an SPDF is to develop and maintain secure devices for their entire lifecycle. From a security context, these are also trustworthy and resilient devices. These devices can then be managed (e.g., installed, configured, updated, review of device logs), as supported through the device design and associated labeling, by the device manufacturers and/or users (e.g., patients, health care providers).	Process & Tool
3	Demonstrate authenticity, including integrity, in device design	FDA will assess the adequacy of the device's security based on the device's ability to provide and implement the security objectives below throughout the system architecture. Security Objectives: • Authenticity, which includes integrity • Authorization • Availability • Confidentiality; and • Secure and timely updatability and patchability.	Tool
4	Device designed with failure mode for system consideration	As cybersecurity is part of device safety and effectiveness, cybersecurity controls should take into consideration the intended and actual use environment.	Tool
5	Transparency	...it is important for device users to have access to information pertaining to the device's cybersecurity controls, potential risks, and other relevant information.	Process & Tool

	AREA	REFERENCE TO GUIDANCE	PROCESS / TOOL
6	Security risk management	FDA recommends that manufacturers establish a security risk management process that encompasses design controls (21 CFR 820.30), validation of production processes (21 CFR 330 820.70), and corrective and preventive actions (21 CFR 820.100) to ensure both safety and security risks are adequately addressed.	Process & Tool
7	Threat modeling	Threat model should capture cybersecurity risks introduced through the supply chain, manufacturing, deployment, interoperation with other devices, maintenance/update activities, and decommission activities that might otherwise be overlooked in a traditional safety risk assessment processes.	Process
8	Third-party software components	Device manufacturers are expected to document all software components of a device and to mitigate risks associated with these software components.	Process & Tool
9	Software bill of materials	...an SBOM or an equivalent capability should be maintained as part of the device's configuration management, be regularly updated to reflect any changes to the software in marketed devices, and... how the known vulnerabilities were discovered...[and] an assessment of the anomaly's impact on safety and effectiveness...	Process & Tool
10	Security architecture	FDA recommends that an adequate set of security controls will include, but not necessarily be limited to, controls from the following categories: • Authentication; • Authorization; • Cryptography; • Code, Data, and Execution Integrity; • Confidentiality; • Event Detection and Logging; • Resiliency and Recovery; and • Updatability and Patchability.	Process & Tool
11	Security architecture views	DA recommends providing, at minimum, the following types of views in premarket submissions: • Global System View; • Multi-Patient Harm View; • Updatability/Patchability View; and • Security Use Case View(s).	Process
12	Cybersecurity testing	FDA recommends the following types of testing, among others, br provided in the submissions a. Security requirements b. Threat mitigation c. Vulnerability testing d. Penetration testing	Process
13	Labeling recommendations	When drafting labeling for inclusion in a premarket submission, a manufacturer should consider all applicable labeling requirements and how informing users through labeling may be an effective way to manage cybersecurity risks and/or to ensure the safe and effective use of the device. Any risks transferred to the user should be detailed and considered for inclusion as tasks during usability testing (e.g., human factors testing) to ensure that the type of user has the capability to take appropriate actions to manage those risks.	Process
14	Vulnerability management plans	Vulnerability communication plans should include the following elements: a. Personnel responsible; b. Sources, methods, and frequency for monitoring for and identifying vulnerabilities (e.g., researchers, NIST NVD, third-party software manufacturers, etc.); c. Periodic security testing to test identified vulnerability impact; d. Timeline to develop and release patches; e. Update processes; f. Patching capability (i.e., rate at which update can be delivered to devices); g. Description of their coordinated vulnerability disclosure process; and h. Description of how manufacturer intends to communicate forthcoming remediations, patches, and updates to customers	Process & Tool

SECTION II: MEDCRYPT FEATURES AND FUNCTIONS

Medical device cybersecurity is complicated and spans a wide range of technologies, requiring technical and procedural actions by multiple parts of the ecosystem. There will never be a single product that will guarantee 100% coverage of all security risks. Instead, processes and tools work together to form an overall security strategy that results in a device with minimal risk in the context of its technology capabilities and use case. MedCrypt solves a specific set of cybersecurity challenges and is taking a healthcare-first approach.

Our products are designed to make it **scalable and sustainable** for software engineers building medical devices to **implement cryptography**, without needing to build an entire framework and ecosystem from scratch. We also monitor what MedCrypt-enabled devices are **impacted by new vulnerabilities**. We enable the collection of **device behavior data**, including information related to security events, and preserve forensic data for further analysis.

MedCrypt provides the experience and technology to efficiently address the FDA Guidance requirements.

MedCrypt's Product Features are Designed to Satisfy FDA Guidance Requirements

MedCrypt tools and technology help address a wide range of these requirements, and remains philosophically aligned with expected final guidance requirements.

Cryptography

A unique private key per device (think serial number) is generated from a key management server. Sensitive data and/or commands are encrypted at the application layer, preventing exposure of data and creating redundancy against network security compromise or poor network security implementation.

Digital Signatures

MedCrypt enables the cryptographic signing of commands to enforce communication and/or configuration authentication. Using MedCrypt's approach means the cryptography algorithm can easily be updated in the future to adapt to evolving requirements.

Monitor Device Behavior

Enabling devices to collect and transmit security metadata (without any sensitive PHI) in real-time. Monitoring device metadata will "baseline" device class behavior, allowing detection of changes that could indicate intrusion, enabling threat sharing.

Vulnerability Management

MedCrypt tools enable tracking versions of component libraries to specific product and SBOM versions, identifying disclosed vulnerabilities that affect an SBOM. Serving as a centralized repository to track mitigations/fixes, and share with stakeholders, this also allows integration with our Vulnerability Management as a Service (VMaaS) to enable scaled assessment and mitigation management.

SECTION III: RATIONALE FOR IMPLEMENTING SECURITY EARLY

Some organizations may feel that investing in a "Secure by Design" development process is overly expensive, and that it may be cheaper to deal with cybersecurity issues that may arise only when absolutely necessary, and as part of a regular software update. However it is becoming increasingly clear that addressing certain types of vulnerabilities once a device is in the field can be prohibitively expensive, and in some cases impossible. Devices that have security considerations as part of their design inputs will face fewer objections from customers' CIOs and CISOs, will face fewer recalls, and face fewer regulatory hurdles.

Some of the security considerations that should be part of the design process can be achieved through organizational processes. For example, code reviews can find many security issues before they make it to the final product, and don't require additional tools or equipment; only additional engineering time. Other considerations may be best addressed by commercial products. As vendors determine how to design and maintain their device security posture, a build, buy, partner assessment should be completed to accomplish efficient and effective security interventions.

For example, MedCrypt's whitepaper analyzing ICS-CERT medical device vulnerability alerts found that two classes of vulnerabilities accounted for 61% of disclosures: user authentication, and code defects. Vendors may choose to use commercial user authentication tools in order to decrease the likelihood of these vulnerabilities. Static Code Analysis tools may be helpful in identifying code issues or bugs during the development phase.

Other vulnerabilities may be prevented by adding encryption into various areas of the product. Public Key Infrastructure tools allow devices to authenticate other endpoints. Cryptography tools like those offered by MedCrypt make it easy to deploy a secure root of trust, as well as verify the integrity of commands/data received from these devices.

SECTION IV: CONCLUSION

As medical devices incorporate connectivity into their essential functionality, vendors face increasing cybersecurity challenges. These challenges range from new regulatory requirements, to unsolicited vulnerability disclosures by members of the community. Vendors need both Processes and Product features geared toward ensuring their devices function safely and effectively, regardless of the security of the environment in which the devices function.

There exist several commercial software tools and services offerings to help medical device vendors succeed in this new era of medical device connectivity. Manufacturers should identify functions and features that are best accomplished through proprietary means, and rely on commercial offerings for the rest. Our industry's products will benefit from the "communal knowledge" that comes from shared technology tools and platforms.

Disclosures

The authors of this paper are employed by MedCrypt Inc, a medical device cybersecurity software developer and service provider.

medcrypt

MedCrypt provides proactive security for healthcare technology. MedCrypt's platform brings core cybersecurity features to medical devices with just a few lines of code, ensuring devices are secure by design. MedCrypt announced a $5.3 million Series A funding round in May of 2019, bringing the total funds raised to $9.4 million with participation from Eniac Ventures, Section 32, Y Combinator, and more. The company is based in San Diego, California.

For further details, please visit and contact:

Website: www.medcrypt.com
Email: info@medcrypt.com
Twitter: @MedCrypt