CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

CHIME Cheat Sheet – October 4, 2023
FDA's Final Guidance Document
Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

The Food and Drug Administration (FDA) released their final guidance document for medical device manufacturers on how they should address cybersecurity in their premarket product submissions in order to meet new requirements – including the documentation that FDA is requiring to be included, as well as recommendations regarding cybersecurity device design, and labeling in their premarket product submissions. These recommendations are intended to promote consistency, facilitate efficient premarket review, and help ensure that marketed medical devices are sufficiently resilient to cybersecurity threats.

Background

The Protecting and Transforming Cyber Health Care Act of 2022 (PATCH Act) – supported by CHIME – was signed into law on Dec. 29, 2022 as a part of the 2023 Consolidated Appropriations Act. The bill became effective 90 days after the enactment of the law, on March 29, 2023. Importantly, this statute gave the FDA additional authority over cybersecurity of medical devices, which the agency had requested from lawmakers.

Since March, the FDA has not been enforcing the "refuse to accept" (RTA) policy regarding device submission decisions; however, beginning on Oct. 1, the Agency will begin issuing RTAs if sponsors do not include the cyber requirements in their submission. In other words, the FDA will now begin to reject premarket medical device submissions that lack the cybersecurity requirements outlined in this final guidance, as well as other previous guidance documents, as detailed below.

This final guidance replaces the document issued in 2014, and the FDA acknowledges that a "rapidly evolving landscape, an increased understanding of emerging threats, and the need for capable deployment of mitigations throughout the total product lifecycle (TPLC) warrants an updated, iterative approach to device cybersecurity." These recommendations are intended to supplement the Agency's Postmarket Cybersecurity Guidance, "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," and "Content of Premarket Submissions for Device Software Functions." Additionally, these recommendations are in general alignment with or expand upon the recommendations in the Pre-Market Considerations for Medical Device Cybersecurity section of the International Medical Device Regulators Forum

(IMDRF) final guidance "Principles and Practices for Medical Device Cybersecurity," issued in March 2020.

You can find the FDA's Cybersecurity in Medical Devices Frequently Asked Questions (FAQs) here.

Key Takeaways

This guidance document 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. It is not limited to devices that are network-enabled or contain other connected capabilities. The term "medical device system" includes the device and systems – such as healthcare facility networks, other devices, and software update servers – to which it is connected. The guidance identifies the cybersecurity information FDA recommends to help support a premarket submission for devices within its scope. While it does not affect products already on the market (i.e., legacy devices), if a manufacturer makes a change to the device necessitating a premarket review, these new cybersecurity requirements policies will apply to the device.

The recommendations included in the guidance cover all relevant cybersecurity considerations that may affect device safety and effectiveness – including but not limited to software, hardware, and firmware. Device manufacturers must establish and follow quality systems (QS) to help ensure that their products consistently meet applicable requirements and specifications. Additionally, the security objectives may apply broadly to devices within the scope of the guidance, including, but not limited to, devices containing artificial intelligence and machine learning (AI/ML) and cloud-based services.

One way the TPLC considerations for devices can be achieved is through the implementation and adoption of a Secure Product Development Framework (SPDF). An SPDF, as described in this guidance, is a set of processes that reduce the number and severity of vulnerabilities in products throughout the device lifecycle. Additionally, an SPDF includes a set of processes that help identify and reduce the number and severity of vulnerabilities in products, and encompasses all aspects of a product's lifecycle, including design, development, release, support, and decommission – among other QS regulatory requirements. The FDA notes that "cybersecurity risks to the medical device or to the larger medical device system can be reasonably controlled through using an SPDF."

The primary goal of using an SPDF is to manufacture and maintain safe and effective devices. From a security standpoint, these are also trustworthy and resilient devices. These devices can then be managed (e.g., installed, configured, updated, review of device logs) through the device design and associated labeling by the device manufacturers and/or users (e.g., patients, healthcare facilities). For healthcare facilities, these devices can also be managed within their own cybersecurity risk management frameworks, such as the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, generally referred to as the NIST Cybersecurity Framework, or NIST CSF.

However, sponsors may use alternative approaches and provide different documentation so long as their approach and documentation satisfy premarket submission requirements in applicable statutory provisions and regulations. When reviewing premarket submissions, the FDA intends to assess device cybersecurity based on a number of factors, including, but not limited to, the device's ability to provide and implement the security objectives throughout the device architecture. Additionally, device cybersecurity design and documentation are expected to scale with the cybersecurity risk of that device. Manufacturers should take into account the larger system in which the device may be used.

FDA recommends that cybersecurity testing occur throughout the SPDF. Security testing early in development can ensure that security issues are addressed prior to impacting release timelines and can prevent the need to redesign or re-engineer the device. After release, cybersecurity testing should be performed at regular intervals commensurate with the risk (e.g., annually) to ensure that potential vulnerabilities are identified and able to be addressed prior to their ability to be exploited. To document the security risk management activities for a medical device system, FDA recommends that manufacturers generate a security risk management plan and report – such as that described in AAMI TIR57, "Principles for Medical Device Security – Risk Management."

Additionally, the FDA is requiring transparency regarding cybersecurity information which has the potential to affect the safety and effectiveness of a device. The FDA states that it is "important for device users to have access to information pertaining to the device's cybersecurity controls, potential risks to the medical device system, and other relevant information."

The FDA believes informing users of security information through labeling may be an effective way to comply with labeling requirements relating to cybersecurity risks, and an important part of design and development activities to help mitigate these and help ensure the continued safety and effectiveness of the device. When drafting labeling for inclusion in a premarket submission, the FDA states that 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 – see the FDA's Guidance "Applying Human Factors and Usability Engineering to Medical Devices" here) to ensure that the type of user has the capability to take appropriate actions to manage those risks.

The recommendations provided in this guidance aim to communicate to users the relevant device security information that may enable their own ongoing security posture, thereby helping ensure a device remains safe and effective throughout its lifecycle. The depth of detail, the exact location in the labeling for specific types of information (e.g., operator's manual, security implementation guide), and the method to provide this information should account for the intended user of the information. Instructions to manage cybersecurity risks should be understandable to the intended audience, which might include patients or caregivers with limited technical knowledge. If the manufacturer chooses to employ methods to ensure certain information is available only to the user, and if it does so through an online portal, it should ensure that users have up-to-date links that contain accurate information.

Additionally, recognizing that cybersecurity risks evolve as technology evolves throughout a device's TPLC, FDA recommends that manufacturers establish a plan for how they will identify and communicate to users any vulnerabilities that are identified after releasing the device in accordance with the PATCH Act statute.[1]

For more information regarding FDA's policy on labeling changes and submission requirements, manufacturers can use the FDA Guidance Search Tool to identify relevant guidance documents for their product and submission type, available here.

If you have any questions, please email policy@chimecentral.org.

[1] 21 CFR 820.100