OCTOBER 11, 2023

FDA Finalizes Premarket Cybersecurity Guidance for Medical Devices

For more information, contact:

Lisa Dwyer
+1 202 626 2393
ldwyer@kslaw.com

Igor Gorlach
+1 713 276 7326
igorlach@kslaw.com

Eric Henry
+1 302 312 9772
ehenry@kslaw.com

Jessica Ringel
+1 202 626 9259
jringel@kslaw.com

Kyle Sampson
+1 202 626 9226
ksampson@kslaw.com

Elaine Tseng
+1 415 318 1240
etseng@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
Tel: +1 202 737 0500

On September 27, 2023, FDA finalized its guidance entitled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" (the "2023 Final Guidance").[1] The Final Guidance replaces guidance issued in 2014 (and the draft guidance issued in April 2022, the "2022 Draft Guidance") and outlines three primary changes to the Agency's current thinking, as compared to the 2014 Guidance:

1. Introduction of the "Secure Product Development Framework," implemented through comprehensive risk management, security architecture, and cybersecurity-specific testing;

2. Recommendations for implementation of cybersecurity transparency, including modified cybersecurity-specific labeling, and a vulnerability management plan; and

3. An appendix providing cybersecurity documentation requirements for Investigational Device Exemption (IDE) submissions.

The 2023 Final Guidance is largely consistent with the 2022 Draft Guidance, but there are differences that may require additional or altered approaches; these differences are the focus of this Client Alert. Please see our Client Alert on the 2022 Draft Guidance for a detailed overview of FDA's current thinking on medical device cybersecurity requirements, outside of the changes discussed here.

INCORPORATING AI/ML AND CLOUD-BASED DEVICES

The 2023 Final Guidance includes FDA's current thinking on cybersecurity requirements for artificial intelligence and machine learning (AI/ML) enabled devices and cloud-based services by adding AI/ML and the cloud into the scope of defined security objectives for medical device software. The inclusion of AI/ML-based medical devices is neither surprising nor unexpected, and medical device manufacturers should view

this guidance from FDA as a nudge to ensure that AI/ML algorithms are addressed within the device's software architecture that drives cybersecurity requirements and risk management.

Cloud-based systems are also not a surprising addition to the scope of enumerated device security objectives, as they were included in discussions of security architecture in the 2022 Draft Guidance. The means for addressing cybersecurity risks in cloud-based systems, however, will continue to be challenging, as the use of public cloud services removes control of certain cybersecurity risks from of the hands of the medical device manufacturer and puts them into the hands of the cloud service provider. To address this concern, manufacturers using public cloud computing services should comply with both the 2023 Final Guidance and AAMI/CR510:2021 ("Appropriate Use of Public Cloud Computing for Quality Systems and Medical Devices"). Doing so will help manufacturers address some of the loss of control inherent in the use of third-party cloud services.

CYBERSECURITY RISK MANAGEMENT

The 2023 Final Guidance emphasizes the difference between cybersecurity risk management and safety risk management. Referencing AAMI TIR57 ("Principles for medical device security – Risk management"), the 2023 Final Guidance adds recommendations for a risk management plan and expands content elements for a risk management report that address cybersecurity risks exclusively, while also clarifying that cybersecurity risks impacting safety will be linked to safety risk management. The cybersecurity risk report should include (or reference) the threat model, cybersecurity risk assessment, the software bill of materials (SBOM), component support information, vulnerability assessments, and unresolved anomaly assessments. The finalization of the requirement to submit vulnerability and penetration testing reports is notable in that such reports typically contain potential security gaps, which is information that is sensitive from a security perspective and legal perspective.

When addressing cybersecurity risk assessment, the 2023 Final Guidance reinforces the non-probabilistic nature of assessing cybersecurity risk (i.e., no likelihood or probability in calculating cybersecurity risk) and points instead to exploitability as the opportunistic measure that should be used. FDA recommends that acceptance criteria measures and thresholds used in cybersecurity risk assessment be included in regulatory submissions.

The 2023 Final Guidance dedicates an entire section to interoperability considerations, and it references FDA's guidance entitled "Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices" as a guide for evaluating interoperability risks throughout the cybersecurity risk management process.

In addressing third-party software components, the 2022 Draft Guidance stated: "While source code is not provided in premarket submissions, if this control is not available based on the terms in supplier agreements, the manufacturer should include in premarket submissions a plan of how the third-party software component could be updated or replaced should support for the software end."[2] The 2023 Final Guidance maintains this language but adds that "device manufacturers should establish and maintain custodial control of device source code (the original 'copy' of the software) throughout the lifecycle of a device as part of configuration management. This may be accomplished through different methods, such as source code escrow or source code backups, among others." FDA acknowledges that third-party suppliers may be reluctant to provide this level of access to source code and recommends incorporating custodial control to purchasing controls, in the event the third-party software reaches end of life prior to the end of life of the medical device. This language is potentially problematic when considered in the context of defending configuration management practices to the FDA, where manufacturers substantially rely on third-party software. The handling of third-party source code within configuration management may be viewed as an addition to FDA's general configuration management requirements, which are set forth in FDA's recent guidance entitled "Content of Premarket Submissions for Device Software Functions."

SOFTWARE BILL OF MATERIALS (SBOM)

In the December 2022 "Consolidated Appropriations Act, 2023," Congress added Section 524B ("Ensuring Cybersecurity of Medical Devices") to the Federal Food, Drug, and Cosmetic Act (FDCA). New FDCA section 524B(b)(3) requires SBOMs in marketing applications for cyber devices, including 510(k)s, PMAs, and Humanitarian Device Exemptions.[3] The 2023 Final Guidance therefore provides that SBOMs are a required component of marketing applications for cyber devices, and a recommended component of marketing applications for all other devices. The 2023 Final Guidance also recommends that SBOMs be submitted in IDEs as well as marketing applications. The 2023 Final Guidance applies its SBOM provisions to both "device manufacturer-developed components and third-party components (including purchased/licensed software and open-source software)." This is a significant expansion beyond most existing SBOM standards set forth in the literature, which focus only on third-party software components. The guidance provides that an SBOM should contain the elements set forth in the National Telecommunications and Information Administration (NTIA) publication "Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)." In addition, the SBOM should contain the software level of support and an end-of-support date for each component.

In support of the SBOM, the 2023 Final Guidance includes a recommendation that manufacturers identify all known vulnerabilities associated with their device and its software components. The Cybersecurity and Infrastructure Security Agency (CISA) "Known Exploited Vulnerabilities" (KEV) catalog should be a good source for manufacturers.

POSTMARKET MONITORING

The 2023 Final Guidance alters how postmarket monitoring is to be communicated in a product submission.

First, what the 2022 Draft Guidance called Vulnerability Management Plans, the 2023 Final Guidance renames Cybersecurity Management Plans.

Second, the recommended content of a Cybersecurity Management Plan, as described in the 2023 Final Guidance, is identical to the content of a Vulnerability Management Plan, with one exception. Complementing the inclusion of CISA's KEV as an input to an SBOM, FDA recommends that the same vulnerability database be incorporated into the Cybersecurity Management Plan to reflect more extensive ongoing vulnerability monitoring.

SECURITY CONTROL CATEGORIES

Like the 2022 Draft Guidance, the 2023 Final Guidance includes the following recommended categories of security controls to be identified in cybersecurity risk management:

- authentication;
- authorization;
- cryptography;
- code, data, and execution integrity;
- confidentiality;
- event detection and logging;
- resiliency and recovery; and
- firmware and software updates.

In addition to a general statement recommending the use of the National Institute of Standards and Technology (NIST) standard for cryptography, the 2023 Final Guidance includes the following qualifier:

> Manufacturers should not implement cryptographic algorithms that have been deprecated or disallowed in applicable standards or best practices (e.g., NIST SP 800-131A, Transitioning the Use of Cryptographic Algorithms and Key Lengths). Implementation of algorithms with a status of "legacy use" should be discussed with FDA during a pre-submission meeting.[4]

This already is FDA's practice, implemented in its reviews of cybersecurity elements in product submissions. In our view, it should be interpreted as a mandate to use "state-of-the-art" cryptographic algorithms in devices subject to premarket submissions unless FDA agrees that the manufacturer may use "legacy" algorithms.

In addressing code integrity, the 2023 Final Guidance adds a recommendation to deploy hardware-based security solutions where possible.

ARCHITECTURE

Where the 2022 Draft Guidance focused its architectural recommendations on call-flow diagrams, the 2023 Final Guidance takes a broader approach and allows for a wider variety of architectural views (e.g., data flow diagrams, state diagrams, swim-lane diagrams, call-flow diagrams, etc.).

GENERAL PREMARKET SUBMISSION DOCUMENTATION ELEMENTS

Appendix 4 of the 2023 Final Guidance provides a list of recommended documents for IDE and premarket submissions. The appendix emphasizes that the list of recommend documents should not be used as a checklist but should instead be scaled with the level of cybersecurity risk using the threat model and architecture as a guide. Inevitably, firms will be tempted to ignore FDA's advice and use the recommended documentation table as a checklist, but we advise that firms carefully consider the extent to which each document in the appendix applies to their device and also consider whether additional supporting documents may be helpful to include in their submissions.

CONCLUSION – A SENSE OF URGENCY

As noted, 2023 Final Guidance is very similar to the 2022 Draft Guidance. Firms that have begun to implement the 2022 Draft Guidance, however, should analyze the unique aspects of the 2023 Final Guidance we describe above and consider how those differences may influence cybersecurity risk and regulatory submission processes. Where firms have not yet implemented the 2022 Draft Guidance, we encourage conducting an expedited gap analysis of the firm's current cybersecurity risk and submission processes against the 2023 Final Guidance.

The 2023 Final Guidance is immediately in effect, except for applications that were pending with FDA when the guidance was issued. Additionally, after the expiration of FDA's grace period on October 1, 2023, FDA will now issue Refuse to Accept decisions if cybersecurity information in premarket submissions is incomplete. Firms therefore should have a sense of urgency in closing any identified gaps.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 23 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MIAMI	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	

[1] We provided an overview of the draft version of this guidance, issued on April 8, 2022. See King & Spalding, Client Alert, FDA Issues Draft Guidance on Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (May 6, 2022). The 2022 Draft Guidance was the second draft revision of the 2014 Guidance, with the first draft revision having been published in 2018. Our Client Alert on the 2022 Draft Guidance provided both an overview of the document at that time and a comparison to the 2014 Final Guidance and the 2018 Draft Guidance.

[2] "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff" (Section V(A)(2))

[3] A "cyber device" is defined as "a device that— (1) includes software validated, installed, or authorized by the sponsor as a device or in a device; '(2) has the ability to connect to the internet; and '(3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats." FDCA sec. 524(c).

[4] "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions: Guidance for Industry and Food and Drug Administration Staff" (Appendix 1(C))