King & Spalding
Client Alert

FDA and Life Sciences

MAY 6, 2022

For more information, contact:

Eric Henry
+1 202 661 7823
ehenry@kslaw.com

Steve Niedelman
+1 202 626 2942
sniedelman@kslaw.com

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

King & Spalding

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

FDA Issues Draft Guidance on Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

On April 8, 2022, FDA issued new, long-awaited draft guidance "*Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*" (Draft Cybersecurity Guidance).[1] This draft guidance replaces a previous draft guidance published in 2018 (the 2018 Draft Cybersecurity Guidance) and, when final, will supersede "*Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014*" (2014 Cybersecurity Guidance).[2]

The Draft Cybersecurity Guidance provides important information regarding FDA's current thinking regarding appropriate steps and precautions medical device manufacturers need to consider as they design, manufacture, and seek premarket clearance for their devices. King & Spalding recommends that device manufacturers read and become familiar with the full content of the Draft Cybersecurity Guidance, especially information contained within the Appendices which provide additional tools for executing the information contained within the draft guidance. The Draft Cybersecurity Guidance does not have the effect of law or regulation; firms may use an alternative approach if it satisfies the requirements of the applicable statutes and regulations.

FDA will be accepting comments on the Draft Cybersecurity Guidance until July 7, 2020. Comments can be submitted electronically to https://www.regulations.govor by mail to the Dockets Management Staff, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852. Identify all comments with the docket number FDA-2021-1158.

Importantly, FDA clarified in the Draft Cybersecurity Guidance its recommendations are not intended to suggest that FDA will evaluate an applicant's compliance with the Quality System Regulation (QSR) as part of a 510(k) submission. Rather, FDA explains that the "guidance is intended to explain how FDA evaluates the performance of device cybersecurity and the cybersecurity outputs of activities that are part and parcel of QSR compliance and explain how the QSR can be leveraged to demonstrate these performance outputs."[3] In our experience, we have observed comments from FDA on premarket submission deficiency letters related to cybersecurity that resulted in both significant delays in product clearance and in for-cause inspections of manufacturing facilities.

To distinguish the changes contained within Draft Cybersecurity Guidance from the 2014 Cybersecurity Guidance and the 2018 Draft Cybersecurity Guidance, we have included a comparison table as an Appendix to this client alert for your firm's information and use.

As always, King & Spalding's cybersecurity experts are prepared to provide any assistance you may need to assist with any questions or assistance in developing, designing compliant cybersecurity controls for your medical devices, as well as provide training in the growing importance of cybersecurity.

Scope

The 2014 Cybersecurity Guidance applied to most medical device premarket submissions, namely, premarket notification (510(k)) submissions, De Novo requests, Premarket Approval (PMA) applications, Product Development Protocols (PDP), and Humanitarian Device Exemption (HDE) submissions. The Draft Cybersecurity Guidance retains this scope and adds PMA supplements and Investigational Device Exemption (IDE) submissions.

Background

The Draft Cybersecurity Guidance acknowledges that increasingly advanced and connected medical device operating environments have resulted in increased cybersecurity risks to safety and/or effectiveness.

Cybersecurity threats to the healthcare sector have become more frequent and more severe, carrying increased potential for clinical impact. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the U.S. and globally. Such cyber-attacks and exploits may lead to patient harm resulting from clinical hazards, such as delay in diagnoses and/or treatment.[4]

As a result of "the rapidly evolving landscape, an increased understanding of emerging threats, and the need for capable deployment of mitigations throughout the total product lifecycle (TPLC)," FDA determined that an updated, iterative approach to device cybersecurity is needed.[5] The changes proposed in the Draft Cybersecurity Guidance are intended to "more clearly outline FDA's recommendations for premarket submission information to address cybersecurity concerns."[6]

The Draft Cybersecurity Guidance focuses on the importance of incorporating cybersecurity measures into the design of the device based upon its intended use, and the importance of ensuring adequate design controls in accordance with the QSR.

General Principles

The Draft Cybersecurity Guidance establishes four broad general principles as the basis for its recommendations:

1. **Cybersecurity is part of device safety and the QSR.** Incorporating cybersecurity protections into a medical device is inherent in complying with the QSR and other applicable guidance documents. Utilization of a Secure Product Development Framework (SPDF) (as elaborated upon in the Draft Cybersecurity Guidance) is introduced as one method for assuring quality system and cybersecurity requirements are met.
2. **Designing for security.** Using a variation on the well-known goal of cybersecurity protections known as CIA (confidentiality, integrity, and availability), the draft guidance establishes as objectives authenticity,

authorization, availability, confidentiality, and secure and timely updatability and patchability. The use of an SPDF will enable these objectives to be met by ensuring a medical device is designed for security from the outset.

3. **Transparency.** Medical device manufacturers should be transparent to device users regarding the "device's cybersecurity controls, potential risks, and other relevant information."
4. **Submission documentation.** Cybersecurity documentation outlined in the Draft Cybersecurity Guidance should be included in device submissions.

Using a Secure Product Development Framework (SPDF) to Manage Cybersecurity Risks

FDA recommends the use of a Security Product Development Framework (SPDF) to ensure effective incorporation of cybersecurity protections throughout the product lifecycle. FDA notes that devices developed with an SPDF "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, health care facilities)."[7] FDA clarifies that healthcare facilities can use their existing cybersecurity risk management frameworks to manage devices designed using a SPDF.

In the Draft Cybersecurity Guidance, "FDA recommends that manufacturers use device design processes such as those described in the QSR to support secure product development and maintenance."[8] FDA permits flexibility, however, acknowledging that

> other frameworks that align with FDA's recommendations for using an SPDF may be used, such as the medical device-specific framework that can be found in the Medical Device and Health IT Joint Security Plan (JSP). Frameworks from other sectors may also comply with the QSR, like the framework provided in ANSI/ISA 62443-4-1: 2018 Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements.[9]

An SPDF, as described by FDA, includes three major elements:

1. Security risk management
2. Security architecture
3. Cybersecurity testing

Although not explicitly mentioned in the Draft Cybersecurity Guidance, we note that the use of recognized consensus standards for medical device software development, such as IEC 62304, are complementary to the use of an SPDF and such standards already include lifecycle activities into which can be inserted these SPDF components.

1. Security Risk Management

While emphasizing the use of the recognized consensus international safety risk management standard ISO 14971:2019, the Draft Cybersecurity Guidance (in contrast to the 2014 Cybersecurity Guidance) makes clear that security risk management includes safety risk but goes beyond it to address a broader array of security risks that may not impact safety. FDA points to AAMI TIR57:2016 (Principles for medical device security – Risk management) to detail how to best integrate security risk management with safety risk management.

The Draft Cybersecurity Guidance recommends the following primary elements to ensure effective implementation of security risk management:

Threat modeling

FDA explains that "[t]hreat modeling includes a process for identifying security objectives, risks, and vulnerabilities across the system, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system throughout its lifecycle. It is foundational for optimizing system, product, network, application, and connection security when applied appropriately and comprehensively."[10]

Similar to a Failure Modes and Effects Analysis (FMEA) or traditional safety risk analysis, a threat model identifies threats that can be exploited through vulnerabilities in the device or its operating environment, assesses them as security risks, identifies appropriate mitigations, and reassesses them post-mitigation. The output of a threat model should be input to safety risk analysis.

Key to effective threat modeling is understanding the device operating environment (including the assumption, known as zero-trust, that an adversary already controls the network and has the ability to alter, drop, and replay packets) and capturing risks introduced throughout the supply chain, manufacturing, deployment, interoperation with other devices, maintenance/update activities, and decommission activities.

FDA recommends that threat models be included in premarket submissions.

Software Bill of Materials (SBOM)

Regarding SBOMs, FDA explains in the Draft Cybersecurity Guidance that:

> A robust SBOM includes both the device manufacturer-developed components and third-party components (including purchased/licensed software and open-source software), and the upstream software dependencies that are required/depended upon by proprietary, purchased/licensed, and open-source software. An SBOM helps facilitate risk management processes by providing a mechanism to identify devices that might be affected by vulnerabilities in the software components, both during development (when software is being chosen as a component) and after it has been placed into the market throughout all other phases of a product's life. [11]

FDA recommends that SBOMs be included in premarket submissions in machine-readable format, and the Draft Cybersecurity Guidance provides seven expected content elements of SBOMs.

Security assessment of unresolved anomalies

Consistent with FDA's 2005 "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices,"[12] and using ANSI/AAMI SW 91:2018 (Classification of defects in health software), the Draft Cybersecurity Guidance recommends including a risk assessment of any anomalies (i.e., defects, issues, bugs) not resolved prior to release in premarket submissions.

Risk management plan and report

Using AAMI TIR57:2016 as a guide, FDA recommends including a risk management plan and risk management report in premarket submissions. Of particular note in the risk management report is a summary of risk evaluation methods, the detailed security risk assessment (i.e., threat model), and any safety risk management mitigations. The report should also provide full traceability between risks, risk controls, and testing to ensure the effective implementation of risk controls and a reasonably secure device.

Living security risk management throughout the life of the product.

Using the idea of a Total Product Lifecycle (TPLC), FDA recommends a continuous refreshing of security risk management activities and documents to ensure timely identification and mitigation of new cybersecurity risks. Based on the activities needed to address newly identified vulnerabilities postmarket, FDA points to its 2016 guidance on "Postmarket Management of Cybersecurity in Medical Devices"[13] to determine whether a new submission or other reporting to FDA will be required.

FDA recommends three measures and metrics, at a minimum, to ensure the effectiveness of security risk management throughout the product lifecycle and recommends that manufacturers track the following:

- Percentage of identified vulnerabilities that are updated or patched (defect density).
- Time from vulnerability identification to when it is updated or patched.
- Time from when an update or patch is available to complete implementation in devices deployed in the field.

2. Security Architecture

The Draft Cybersecurity Guidance points to security architecture as a key element of implementing an SPDF. Incorporated into the security architecture should be a set of security controls in the following categories, at a minimum:

- Authentication
- Authorization
- Cryptography
- Code, data, and execution integrity
- Confidentiality
- Event detection and logging
- Resiliency and recovery
- Updatability and patchability

Appendix 1 of the Draft Cybersecurity Guidance provides specific control recommendations and implementation guidance for each of the above categories.

- FDA recommends four security several architectural views be included in premarket submissions, with detail on the level of detail to be included in the submission outlined in Appendix 2 of the Draft Cybersecurity Guidance:
- Global system view: Overall view of the system including internal and external interfaces
- Multi-patient harm view: Description of how the device / system defends against and/or responds to attacks with the potential to harm multiple patients
- Updateability/patchability view: End-to-end process permitting software updates and patches to be deployed to the device
- Security use case view(s): Diagrams, with explanatory text, describing various security scenarios in each of the operational and clinical functionality states of the system and how the system addresses each scenario architecturally

FDA explains that "[t]hese security architecture views should:

- Identify security-relevant system elements and their interfaces;
- Define security context, domains, boundaries, and external interfaces of the system;
- Align the architecture with (a) the system security objectives and requirements, (b) security design characteristics; and
- Establish traceability of architecture elements to user and system security requirements"[14]

Although not mentioned in the Draft Cybersecurity Guidance, medical device manufacturers conforming to IEC 62304 will note that security architecture can be integrated into the "software architectural design" step of the software development lifecycle defined in this consensus standard.

3. Cybersecurity Testing

FDA recommends four types of security testing, at a minimum, be conducted on medical devices during design verification and design validation.

- Security requirements: Evidence of successful implementation of each design input (security) requirement including boundary analysis and rationale
- Threat mitigation: Testing to show the effectiveness of risk controls identified in the threat model

- Vulnerability testing
    - Abuse case, malformed, and unexpected inputs
        - Robustness
        - Fuzz testing
    - Attack surface analysis
    - Vulnerability chaining
    - Closed box testing of known vulnerability scanning
    - Software composition analysis of binary executable files
    - Static and dynamic code analysis, including testing for credentials that are "hardcoded," default, easily-guessed, and easily compromised.
- Penetration testing: Tests focused on discovering and exploiting security vulnerabilities

FDA recommends documentation of cybersecurity testing, including test report, be included in premarket submissions. Reports should describe where the testing was performed and assurance of the independence of those performing the tests from the developers of the software.

Cybersecurity Transparency

As described in the general principles above, FDA recommends providing useful information regarding the state of cybersecurity risks and controls to device users. The Draft Cybersecurity Guidance breaks this principle into two primary categories:

1. Labeling

FDA modified the 14 cybersecurity-specific labeling recommendations from the 2018 Draft Cybersecurity Guidance and generated a list of 15 labeling recommendations in the current Draft Cybersecurity Guidance, including device instructions, diagrams, an SBOM, a listing of backup and restore features, description of the shipped secure configuration of the device, and a description of how the device logs events to enable forensic review.

2. Vulnerability Management Plans

To complement the ubiquitous discussion of coordinated vulnerability disclosure to internal and external stakeholders across global regulatory literature, FDA recommends submitting vulnerability communication plans in premarket submissions. According to the Draft Cybersecurity Guidance, such plans should include the following:

- "Personnel responsible;
- Sources, methods, and frequency for monitoring for and identifying vulnerabilities (e.g., researchers, NIST NVD, third-party software manufacturers, etc.);
- Periodic security testing to test identified vulnerability impact;
- Timeline to develop and release patches;
- Update processes;
- Patching capability (i.e., rate at which update can be delivered to devices);
- Description of their coordinated vulnerability disclosure process; and
- Description of how manufacturer intends to communicate forthcoming remediations, patches, and updates to customers."[15]

Submission Documentation for Investigational Device Exemptions

As described above, FDA has added Investigational Device Exemption (IDE) submissions to the scope of cybersecurity guidance. In Appendix 3 of the draft guidance, FDA recommends five cybersecurity elements be included in IDE applications.

- Inclusion of cybersecurity risks as part of the Informed Consent Form

- Global, Multi-patient, and Updateability/Patchability architectural views
- Security Use case architectural views for functionality with safety risks
- Software Bill of Materials (SBOM)
- General labeling – Connectivity and associated general cybersecurity risks, updateability process

Appendix: Comparison of FDA's 2014 Cybersecurity Guidance vs. 2018 Draft Cybersecurity Guidance vs. 2022 Draft Cybersecurity Guidance

2014 Final Guidance	2018 Draft Guidance	2022 Draft Guidance
Scope		
• Premarket Notification (510(k)) including Traditional, Special, and Abbreviated • De novo submissions • Premarket Approval Applications (PMA) • Product Development Protocols (PDP) • Humanitarian Device Exemption (HDE) submissions		Added • PMA supplements • Investigational Device Exemption (IDE) submissions
Definitions / Terminology		
Defined 14 terms	• Added 12 new terms (including Authenticity, Availability, Cybersecurity Bill of Materials (CBOM), Patchability / Updatability) • Removed the term "Harm"	• Modified five terms: ◦ Authentication ◦ Integrity ◦ Malware ◦ Patchability / Updatability (Updatability and patchability) ◦ Patient harm (Note: adopts new definition of harm from ISO 14971:2019) • Added 23 new terms (including Secure Product Development Framework (SPDF), Security architecture, Software Bill of Materials (SBOM), Threat modeling) • Removed eight terms (including Cybersecurity Bill of Materials (CBOM))
Lifecycle Requirements		
• Clarified integration of cybersecurity activities into broader Quality System Regulation (QSR) requirements for design controls • Incorporated NIST's Cybersecurity Framework (i.e., identify, protect, detect, respond, recover) into lifecycle guidance	• Introduced "Tier 1" and "Tier 2" cybersecurity risk levels • Expands guidance for incorporating NIST's Cybersecurity Framework for "Tier 2" systems only	• Removed "Tier 1" and "Tier 2" cybersecurity risk levels • Expanded guidance in the context of cybersecurity design controls • Introduced Secure Product Development Framework (SPDF) ◦ Security risk management (threat modeling, SBOM, anomaly list) ◦ Security architecture (detailed security controls guidance, detailed architectural views guidance) ◦ Cybersecurity Testing • Expanded guidance for vulnerability management / communication
Documentation		

2014 Final Guidance	2018 Draft Guidance	2022 Draft Guidance
• Hazard analysis • Trace matrix • Plan for updates and patches • Plan for integrity during delivery to customer • Cybersecurity instructions and product specifications	• Labeling (14 recommendations) • Documentation describing implementation of described NIST cybersecurity framework elements • System diagrams • Plan for updates and patches	• Modified labeling recommendations • Threat model • SBOM • List of residual software anomalies • Security risk management plan and report (ref. AAMI TIR57) • Total Product Lifecycle (TPLC) metrics • Security architecture (implementation of eight security controls, four security architectural views) • Security documentation (including test reports) • IDE documentation

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 1,200 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.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising." View our Privacy Notice.

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

[1] U.S. Food & Drug Admin., Center for Devices and Radiological Health and Center for Biologics Evaluation and Research, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff, Draft Guidance," Apr. 8, 2022 *available at* https://www.fda.gov/media/119933/download (Draft Cybersecurity Guidance).

[2] U.S. Food & Drug Admin., Center for Devices and Radiological Health and Center for Biologics Evaluation and Research, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Administration Staff," Oct. 2, 2014, *available at* https://www.fda.gov/media/86174/download (2014 Cybersecurity Guidance).

[3] Draft Cybersecurity Guidance at fn. 16.

[4] *Id.* at 1.

[5] *Id.* at 3.

[6] *Id.*

[7] *Id.* at 8.

[8] *Id.*

[9] *Id.*

[10] *Id.* at 10.

[11] *Id.* at 12.

[12] U.S. Food & Drug Admin., Center for Devices and Radiological Health and Center for Biologics Evaluation and Research, "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices," May 2005, *available at* https://www.fda.gov/media/73065/download.

[13] U.S. Food & Drug Admin, Center for Devices and Radiological Health and Center for Biologics Evaluation and Research, "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," Dec. 2016, *available at* https://www.fda.gov/media/95862/download.

[14] Draft Cybersecurity Guidance at 20.

[15] *Id.* at 27.