ROPES & GRAY

ALERT ▪ FDA Regulatory ▪ Digital Health ▪ Data, Privacy & Cybersecurity

May 11, 2022

FDA Updates Guidance on Cybersecurity Responsibilities for Medical Device Manufacturers

Attorneys
Gregory H. Levine
Edward R. McNicholas
Lauren Sager

On April 8, 2022, the U.S. Food and Drug Administration ("FDA") released a draft guidance document titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions."[1] The draft guidance, if finalized, would replace FDA's 2014 final guidance document titled, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," which was discussed in a previous Ropes & Gray Alert.

Ever since the TV show "Homeland" dramatized a terrorist remotely hacking the Vice President's pacemaker in 2012, the need to secure medical devices has captivated the attention of policymakers. The issue jumped to the headlines again with the 2017 global WannaCry ransomware attack that infected tens of thousands of computers and medical devices, including MRI machines in U.K. hospitals and Bayer's Medrad contrast agent injection devices in the U.S.[2] The present potential for a Russian cyber-weapon to impact U.S. health care infrastructure remains a possibility, particularly after the NotPetya cyber-weapon hit a global pharmaceutical company during the prior Ukraine conflict and similar weapons are reportedly being deployed during the present war.

In recognition of the increased potential and evolving nature of cybersecurity threats, FDA's draft guidance expands on its 2014 recommendations by providing more details about how device manufacturers should integrate cybersecurity considerations into their quality systems and what cybersecurity information should be included in premarket submissions (PMAs, 510(k)s, de novo classification requests, PDPs, HDEs, and IDEs) to demonstrate a reasonable assurance of safety and effectiveness. When assessing and addressing the cybersecurity risks associated with devices, the draft guidance recommends that manufacturers consider their devices in the context of the larger "medical device system," which includes all of the devices and systems—such as health care facility networks—that may use or be used with a device.

FDA's Recommendations for Device Design and the Quality System Regulation

FDA explains that certain quality system requirements related to cybersecurity will apply to the premarket and post-market stages of the device lifecycle, and applicable requirements may differ depending on the device. To satisfy FDA's Quality System Regulation ("QSR"), device manufacturers should establish design controls that include software validation and risk analysis procedures. The draft guidance recommends that device manufacturers satisfy the QSR by establishing a Secure Product Development Framework ("SPDF"), which is a set of processes designed to reduce the number and severity of product vulnerabilities throughout all aspects of the product life cycle. The guidance outlines aspects of a SPDF, including threat modeling and risk assessments, that take into account third-party software components. While the SPDF recommendation is far more specific than anything recommended in FDA's 2014 guidance, FDA acknowledges that manufacturers also may satisfy the QSR using other approaches, provided they meet the QSR's requirements.

To meet the QSR's design control requirements, FDA recommends that manufacturers design devices with features that address cybersecurity vulnerabilities from the outset, rather than adding them later in development. The guidance discusses five security objectives that manufacturers should take into account when designing devices: authenticity, including data integrity; authorization; availability; confidentiality; and secure and timely updateability and patchability.

Consistent with Executive Order 14028 (issued after the SolarWinds attack involving a nation-state injecting malicious code into a secure compiling process), FDA also recommends that a device manufacturer prepare a Software Bill of Materials ("SBOM") describing the various software components used by the device, including off-the-shelf and other software manufactured by third parties, that can be used by FDA as well as device users to understand a device's cybersecurity controls. The SBOM recommendation may result in the disclosure of the jurisdictions involved in the development of the device, which could affect the ability of medical device manufacturers to develop code in lower-cost jurisdictions.

FDA's Recommendations for Inclusion of Cybersecurity Information in Device Labeling

The draft guidance reiterates FDA's prior position that stakeholders throughout the medical device system, including health care facilities, patients, providers, and manufacturers, share responsibility for medical device security. Given this shared responsibility, FDA emphasizes the need for manufacturers to furnish device system users with information about cybersecurity risks and mitigation efforts so that they can effectively manage security risks associated with devices. FDA recommends that manufacturers include cybersecurity information in device labeling and provides a list of specific types of information that labeling should contain. Such information includes, among other things, instructions and product specifications related to cybersecurity controls, detailed diagrams to enable controls to be implemented, lists of network ports and interfaces that send or receive data, guidance on supporting infrastructure requirements, and the SBOM. Significantly, the widespread publication of this information would also potentially provide attackers with detailed information about vulnerabilities that could be exploited, requiring the exercise of considerable care in the development of such labeling.

Even after manufacturers obtain clearance or approval for a device and release the device to the market, cybersecurity vulnerabilities may arise, and FDA recommends that manufacturers establish vulnerability management plans to address potential risks as they evolve. These plans should define the steps for identifying and communicating to users regarding vulnerabilities that are discovered after the device is released to market. The guidance lists elements that vulnerability communication plans should include, such as personnel responsible; periodic testing; update processes; and communication plans for remediation efforts, patches, and updates to customers.

Although sound in principle, this implied duty to continually protect aging devices against ever-advancing threats may require considerable attention by device manufacturers. This recommendation also could create a potential liability trap as hacking techniques evolve, but devices cannot be re-engineered without undue cost and risk. While manufacturers of PMA-approved devices arguably would have statutory protection from such liability through express preemption language in the Federal Food, Drug, and Cosmetic Act (*see Reigel v. Medtronic*, 552 U.S. 312 (2008)), the vast majority of devices do not enter the market through the PMA pathway and therefore are not subject to such liability protection.

FDA's Recommendations on Cybersecurity Information in Premarket Submissions

The draft guidance explains that cybersecurity documentation to be included in a premarket submission will depend on the cybersecurity risks specific to the device that is the subject of the submission. For example, a device that is not connected to an external network and connects only through a USB interface is lower risk and will require less cybersecurity disclosures, while more complex, network-connected devices carry greater vulnerabilities, requiring more extensive documentation in the premarket submission.

The draft guidance outlines the type of documentation regarding safety and security risks that manufacturers should include in premarket submissions. This documentation includes threat modeling to identify risks and vulnerabilities across the device system and countermeasures for addressing the risks and vulnerabilities. Premarket submissions should also contain documentation related to each third-party software component, including a SBOM and supporting information such as the component's name, version, manufacturer, and end-of-support date and known vulnerabilities associated with the component. Other information that FDA recommends that device manufacturers provide in premarket submissions includes a list of software abnormalities and outputs of security risk management processes, such as plans and reports.

With regard to a device's security architecture, FDA recommends that premarket submissions include "views"—diagrams and text explaining the design. FDA also outlines in the draft guidance the types of cybersecurity testing that premarket submissions should contain, which includes threat mitigation testing, vulnerability testing, and penetration testing.

The draft guidance explains that failure to have adequate cybersecurity controls can cause a device to be misbranded. First, a device without adequate cybersecurity controls may be misbranded under section 502(f) of the Federal Food, Drug and Cosmetic Act ("FDCA") if the device's labeling does not contain adequate directions for use. Likewise, a device without adequate cybersecurity controls may be misbranded under section 502(j) of the FDCA because it is dangerous to health when used in the manner that the labeling recommends or suggests.

Legislation Addressing Medical Device Cybersecurity

Although FDA guidance is not binding, recently proposed legislation could require that premarket submissions include cybersecurity information. On March 15, 2022, the Protecting and Transforming Cyber Healthcare ("PATCH") Act was introduced to address device cybersecurity concerns.[3] If enacted, the PATCH Act would amend the FDCA to require that all premarket submissions for software and internet-connected devices include information showing that such devices meet cybersecurity requirements. The PATCH Act also would set minimum cybersecurity requirements, including that device manufacturers establish procedures for monitoring devices, addressing cybersecurity vulnerabilities, and coordinating vulnerability disclosures; and that manufacturers submit an SBOM as part of premarket submissions. While the prospects for this bill being enacted are uncertain at the present time, there is clearly a trend toward increasing cybersecurity expectations for medical device manufacturers. Manufacturers should pay close attention to developments in this area, expand their internal expertise, and otherwise invest in establishing robust cybersecurity risk assessment, design control, and risk management practices and procedures relating to their devices.

More generally, on March 15, 2022, President Biden signed into law significant new federal data breach reporting legislation that will likely expand data breach notice requirements far beyond personal data. Unceremoniously tucked as Division Y into the H.R. 2471 Consolidated Appropriations Act, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) will require "covered entities"—organizations in certain critical infrastructure sectors—to report substantial cybersecurity incidents to the Department of Homeland Security within 72 hours after the organization reasonably believes the cyber-incident has occurred. Without doubt, this issue will continue to be front-of-mind on Capitol Hill while the Russian attack on the Ukraine continues.

Comments on the draft guidance are due on July 7, 2022. Ropes & Gray will continue to monitor developments in this area. If you have any questions, please contact any member of our FDA regulatory practice or your usual Ropes & Gray advisor.

1. 87 Fed. Reg. 20873 (April 8, 2022).
2. Thomas Brewster, *Medical Devices Hit by Ransomware for the First Time in US Hospitals*, Forbes (May 17, 2017).
3. H.R. 7084, 117th Cong. (2022).

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.