Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FDA Steps Up Its Focus On Medical Device Cybersecurity

By **Michael Buchanan and Joshua Furman** (November 1, 2018, 2:34 PM EDT)

Michael Buchanan

Joshua Furman

October was National Cybersecurity Awareness Month. No doubt this explains why the U.S. Food and Drug Administration stepped up its focus on the security of internet-connected medical devices.

In quick succession last month, the FDA: (1) issued a "Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook"[1] to address continued threats to medical devices that could affect patient safety; (2) announced a memorandum of agreement with the U.S. Department of Homeland Security[2] to increase coordination between these federal agencies on medical device cybersecurity threats; and (3) provided recommendations to the medical device industry regarding cybersecurity published in a draft guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."[3]

Taken together, these actions demonstrate that the FDA is prioritizing the cybersecurity risks of connected medical devices, and increasing its efforts to strengthen the agency's medical device cybersecurity program to protect patients. This article will touch briefly on the memorandum of agreement with DHS and the incident response playbook, before focusing on the draft guidance.

The memorandum of agreement with DHS, which the FDA announced in mid-October, formalizes and enhances the working relationship between the FDA and DHS to address vulnerabilities and threats involving the cybersecurity of medical devices. The agreement is meant to encourage greater coordination and sharing of information between the two federal agencies "about potential or confirmed medical device cybersecurity vulnerabilities and threats."

While not groundbreaking, this announcement continues an effort by the FDA to address medical device cybersecurity as it comes on the heels of the playbook. Like the memorandum of agreement, the playbook emphasizes the importance of collaboration — not just between government agencies, but among all stakeholders with an interest in protecting patients against the potential risks posed by cyber threats. Stakeholders include medical device manufacturers, healthcare delivery organizations, software and app designers and cybersecurity professionals.

The draft guidance, published in the Federal Register on Oct. 18, provides the FDA's non-binding recommendations for the design of medical devices that have a “cybersecurity risk,” whether the device contains software or the device is itself software. The guidance is subject to review and comment for 150 days.

When finalized, it will supersede the guidance on the same topic issued in October 2014.[4] The guidance also complements another FDA publication, “Postmarket Management of Cybersecurity in Medical Devices,” issued in 2016,[5] which addresses FDA recommendations for “managing postmarket cybersecurity vulnerabilities” for devices already on the market.

In addition to updating and expanding the design and documentation guidelines from 2014, the new guidance includes the FDA recommendations for the labeling of at-risk medical devices. Why now? The FDA says that “the rapidly evolving landscape, and the increased understanding of the threats and their potential mitigations, necessitates an updated approach” to cybersecurity.

Three maxims animate the guidance. First, medical devices can improve patient outcomes. Second, all medical devices carry a certain amount of risk. Third, cyber vulnerability of connected devices cannot be completely eliminated. As a result, the FDA expects manufacturers to engage in a cost-benefit analysis so that, as noted on the FDA website, “there is a reasonable assurance that the benefits to patients outweigh the risks.”[6]

In conducting this analysis, the FDA once again encourages manufacturers to examine: the threats and vulnerabilities and their potential impact on devices' functionality and users; the likelihood of an exploit; the acceptable levels of risk; mitigation strategies; and residual risk and criteria for levels of residual risk.

Additionally, through the guidance, the FDA sets forth a tiered approach that depends on the risks presented by the device, and moves away from the more flexible framework it previously endorsed. The FDA previously suggested that manufacturers “carefully consider the balance between cybersecurity safeguards and the usability of the device in its intended environment of use” and ensure that “security controls should not unreasonably hinder access to a device intended to be used during an emergency situation.”

The revised guidance instead divides medical devices into two tiers: connected devices with a “higher cybersecurity risk” of an incident or exploit that could directly harm a patient (“Tier 1”) and other software devices that do not present such risk (“Tier 2"). It tailors the guidance to each tier. In addition, the guidance now encourages manufacturers to leverage a cybersecurity bill of materials, or CBOM — a list of all constituent hardware and software components of a device that may themselves be subject to vulnerabilities — to better design for and address a device’s risks.

The FDA uses this framework to provide guidance for the design of medical devices with a cybersecurity risk, device labeling and documentation for the FDA for premarket approval. Each will be addressed in turn.

Design

The FDA expects manufacturers of all medical devices to provide information on how the device being submitted for approval was designed. The guidance provides specific recommendations for how the manufacturer should design the device to address cybersecurity risks associated with it.

For Tier 1 devices, the FDA recommends that premarket submissions address every design recommendation provided in the guidance. Manufacturers are given more flexibility for Tier 2: They can either follow the Tier 1 standard or "provide a risk-based rationale" explaining why certain aspects are not applicable.

Overall, and new to 2018, the FDA recommends that manufacturers design "trustworthy" devices. This means devices that:

> (1) are reasonably secure from cybersecurity intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

According to the FDA, following this guidance means that a device is more likely to meet the standards for premarket review, and is more likely to remain safe.

The FDA, following the NIST framework, suggests that a proper design should focus on identifying and protecting the device and its functionality. According to the guidance, the design of a device should include:

- Mechanisms to prevent unauthorized access by using, for example, authentication such as passwords or biometrics. Security mechanisms can differentiate between users types (e.g., caregiver, patient, administrator) and provide permissions based on the user's role;

- Strong password protection. For example, a device should not have default, hardcoded or easily guessed passwords;

- Authentication of software (including updates) to be installed on the device;

- Authorization mechanisms for commands or instructions that are to be run on the device to prevent a hacker from causing the device to run commands without the appropriate authorization — for example, to shut down or change a dose;

- A secure development environment where the code for the device is created and maintained so that it is not vulnerable to exploitation;

- Protection of the integrity of data sent to the device; the device should be designed to ensure that corrupt data cannot be loaded onto the device, and that corrupt data, if loaded, does not compromise the device's functionality;

- Mechanisms to ensure the confidentiality of data stored on the device and transmitted to and from the device by, for example, by using encryption;

- Mechanisms to detect and respond to cyberattacks in a timely manner, including features that allow for critical functionality to continue in the face of an attack;

- The ability to log and report detected events;

- Mechanisms to allow for scanning and forensic evidence capture following a cyber event; and

- The ability to provide prompt notice of an incident to users, the administrator or the healthcare provider.

Labeling

The FDA also provides guidance on how to label devices that may pose cybersecurity risks. In that regard, the FDA encourages medical device manufacturers to utilize labeling to assist in managing cybersecurity risks. The FDA includes 14 points for manufacturers to consider when labeling interconnected medical devices, including:

- Instructions on the proper network environment and infrastructure for the device to operate, including whether to use a firewall for connected devices;

- Features of the device that protect functionality even when compromised;

- A list of network interfaces that are expected to send or receive data;

- Instructions on how authorized users can download software and firmware from the manufacturer;

- A description of how evidence of attacks are captured and how users are notified;

- A full CBOM that includes a list of all software and hardware components; and

- Appropriately detailed system diagrams.

Documentation

As part of the premarket submission process, devices manufacturers are required to provide the FDA with documentation about the device and the software. For devices with a cybersecurity risk, the guidance recommends that these requirements be met by providing documentation of the design features, risk management strategies and labeling as described above.

As noted earlier, the FDA provides different guidance for Tier 1 and Tier 2 devices. Manufacturers of Tier 1 devices should provide documentation for how the device meets each requirement of the design section of the guidance. For Tier 2 devices, manufacturers should document how each requirement was met, or why it was not necessary. In addition, documentation for both tiers should include system diagrams that describe how the design requirements are incorporated into the device. This includes:

- Network, architecture and flow diagrams;

- Interfaces and protocols between components as well as network interfaces;

- Authentication mechanisms;

- User types (e.g., administrator, provider, patient) and how they interact with the device; and

- If encryption is used, a diagram of that system and how it interacts with the various aspects of the device.

The FDA also recommends including risk management documentation. Manufacturers should include a system-level threat model that includes threats identified in the design, production and deployment of the device, as well as supply chain vulnerabilities. For each of those identified threats, the manufacturer should also provide the likelihood that a vulnerability will be exploited, and a matrix that links cybersecurity design elements to the risks.

Lastly, the documentation should include a description of all relevant testing, and a CBOM that cross-references with a national database of known vulnerabilities in each constituent component.

Conclusion

In light of the publication of the guidance and the playbook, it is clear that the FDA sees the vulnerability of medical devices as a serious issue. This is a rapidly developing field, and it is likely that guidance from the FDA will continue to evolve as new risks and threats are understood, and new methods for cybersecurity are developed.

Michael F. Buchanan is a partner and Joshua Furman is an associate at Patterson Belknap Webb & Tyler LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and.

[2] https://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm623568.htm.

[3] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf.

[4] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

[5] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[6] https://www.fda.gov/medicaldevices/productsandmedicalprocedures/ucm373213.htm.