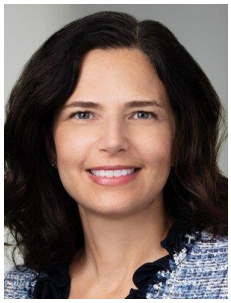
LAW360

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

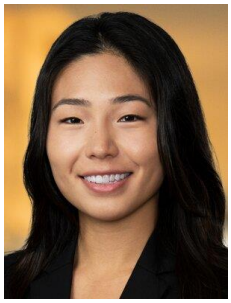
Cybersecurity Expectations Intensify For Medical Device Cos.

By **Stacy Cline Amin, Kristen Mathews and Rachel Park**
(October 25, 2022, 6:06 PM EDT)

Stacy Cline Amin



Kristen Mathews



Rachel Park

A recent FBI private industry notification[1] provided an important reminder to medical device companies that cybersecurity has to be front of mind.

The FBI alert warned that unpatched vulnerabilities can create serious issues that may affect health care facilities' operational functions, patient safety, data confidentiality and data integrity.

This action from the FBI follows U.S. Food and Drug Administration draft guidance[2] from April 8, regarding cybersecurity responsibilities for medical device manufacturers. Given the significant spotlight both agencies have put on medical device cybersecurity, the industry faces an urgent need to ensure it is complying with the recommendations of its regulators.

The FBI notification and FDA guidance are consistent in raising alarm regarding the growing cybersecurity risk to the health care sector. Both agencies have focused specifically on the medical device industry, raising concerns about vulnerabilities stemming from device hardware design and device software management.

The FBI specifically highlighted the vulnerability of underlying software life cycles, which are often specified by the manufacturer and aid in providing cyber threat actors time to discover and exploit weaknesses. The FBI warned that outdated software which is not compatible with security patches and updates are prone to cyberattacks.

Similarly, devices using the manufacturer's default configuration, those with customized software requiring special upgrading and patching procedures, and those not initially designed with security in mind are often easily exploitable by cyber threat actors.

The FBI recommends strategies for mitigating risk as follows:

- Endpoint protection, whereby in medical database management tools and devices, manufactures should consider integrity verification for logins and ensure the encryption of data

in transit and at rest. In addition, the manufactures can ensure that the algorithms used in the encryption process have not been compromised in the past;

- Identification and access management to ensure default passwords are not used, and to require complex passwords for specified medical devices and restriction of multiple login attempts;
- Asset management to include electronic inventory system for devices and associated operating and vendor developed software; and
- Vulnerability management to monitor and review various avenues susceptible to compromise and, more importantly, training of users to help recognize threat and aid in the mitigating process promptly.

The April FDA draft guidance expands on prior FDA recommendations in its 2014 final guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."[3]

The April draft guidance provides more details on integration of cybersecurity considerations into quality systems and what cybersecurity information should be included in premarket submissions to the FDA to demonstrate reasonable assurance of safety and effectiveness.

On Oct. 17, the FDA's Center for Devices and Radiological Health included finalizing this guidance as one of its A-list[4] priorities for 2023, meaning the cybersecurity of medical devices is one of the FDA's top policy concerns.

In line with the FBI recommendations, the FDA's draft guidance develops the concept of a secure product development framework as a way to satisfy quality system regulation requirements in Title 21 of the Code of Federal Regulations, Part 820.

The draft guidance defines a secure product development framework as a set of processes designed to reduce the number and severity of vulnerabilities throughout all aspects in device product lifecycle, including development, release, support and decommission.

The FDA also recommends manufacturers prepare of a software bill of materials describing the software components used by the medical device.

The software bill of materials may be used by the FDA and device users to understand the device's cybersecurity controls. While providing more detailed recommendations in this draft guidance, the FDA acknowledges that manufacturers may also satisfy the quality system regulation requirements through other approaches and frameworks that already exist, such as the Medical Device and Health IT Joint Security Plan.

The FDA's draft guidance emphasizes the shared responsibility of stakeholders in the medical device system, including health care facilities, providers and patients, and the need for manufacturers to provide information about cybersecurity risks and mitigation to effectively manage security risks associated with the devices.

The FDA recommends that manufacturers include cybersecurity information in device labeling and provides a list of information that such labeling should contain, including (1) instructions and product specifications related to cybersecurity controls, (2) detailed diagrams to assist in implementation of

controls, (3) lists of network ports and interfaces that send or receive data, (4) guidance on supporting infrastructure requirements, and (5) the software bill of materials.

The FDA also recommends that manufacturers establish vulnerability management plans, which should define the steps for identifying vulnerabilities and communicating with users, and details elements that vulnerability communication plans should include, such as responsible personnel, periodic testing and communication for patches and customer updates.

The FDA's guidance also focuses on the content of premarket submissions, noting that cybersecurity considerations must be built into the system architecture. The FDA plans to assess the adequacy of the device's security as part of its premarket review and emphasizes that premarket submissions should include information that describes how security objectives are addressed and integrated into the device design.

The FDA recommends that the following be included in a premarket submission:

- Threat modeling process for identifying security objectives, risks and vulnerabilities and defining countermeasures to prevent, or mitigate the effects of, threats to the system throughout its life cycle.
- List of software anomalies existing at the time of submission noting the anomaly's impact on safety and effectiveness. The standards and rationales for addressing the anomalies should be provided as part of the security risk assessment documentation in the premarket submission.
- Documentation related to each third-party software component, including the software bill of materials and supporting information.
- Outputs of security risk management processes, including the management plans and reports and plans for continuous management throughout the total product life cycle.
- Cybersecurity testing documentation and associated reports, including threat mitigation testing, vulnerability testing and penetration testing.
- Vulnerability communication plans.

Federal regulators have generally treated the health care sector, including the medical device industry, as victims when it comes to cybersecurity breaches and exploitation.

However, these recent actions by the FBI and FDA may reflect a shift in that viewpoint. The FDA has established it will withhold premarket clearance or approval if cybersecurity is not adequately addressed.

Furthermore, the draft guidance states that failure to have adequate cybersecurity controls may cause a device to be misbranded, either under Section 502(f) of the Federal Food, Drug and Cosmetic Act if the device labeling does not contain adequate directions for use, or under Section 502(j) if the device lacks adequate cybersecurity controls that cause it to be dangerous to health when used as suggested by the labeling.

These agencies' explicit identification of cybersecurity threats and vulnerabilities for medical devices and

establishment of clear expectations for how industry should address them signals increased scrutiny on, and liability for, manufacturers that do not take the necessary steps to mitigate these risks.

Stacy Cline Amin is a partner and chair of the FDA regulatory and compliance practice group at Morrison Foerster LLP. She previously served as chief counsel of the U.S. Food and Drug Administration.

Kristen Mathews is a partner at the firm.

Rachel Park is an associate at the firm.

[1] https://www.aha.org/cybersecurity-government-intelligence-reports/2022-09-12-fbi-pin-tlp-white-unpatched-and-outdated.

[2] https://www.fda.gov/media/119933/download.

[3] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices.

[4] https://www.fda.gov/medical-devices/guidance-documents-medical-devices-and-radiation-emitting-products/cdrh-proposed-guidances-fiscal-year-2023-fy2023?utm_medium=email&utm_source=govdelivery#a.