AHLA

FDA Recommends Medical Device Manufacturers Implement a Comprehensive Cybersecurity Risk Management Program in Accordance with NIST Standards

Executive Summary, March 2016

Sponsored by the Life Sciences Practice Group. Co-sponsored by the Health Information and Technology Practice Group.

AUTHORS

Shilpa Prem

Epstein Becker & Green PC

New York, NY

Kim Tyrrell-Knott

Epstein Becker & Green PC

San Diego, CA

The U.S. Food and Drug Administration (FDA) is taking cybersecurity risks seriously. Today, medical devices, more often than not, include software or are connected to networks. Cybersecurity risks are different than other risks medical manufacturers typically address in their risk management systems. Manufacturers need to develop risk management programs that are specific to cybersecurity risks and incorporate cybersecurity best practices and National Institute of Standards and Technology (NIST) standards. Such risk management programs will need to go beyond International Organization for Standardization 19471 to address vulnerabilities of cyber-attacks. FDA has recognized the potential risks that these cybersecurity vulnerabilities may have on patient safety. In a series of guidances, FDA is emphasizing the need for medical device manufacturers to proactively manage such risks throughout the product life cycle.

On January 15, 2016, FDA released new draft guidance, "Postmarket Management of Cybersecurity in Medical Devices" (Postmarket Cybersecurity Guidance),[1] which recommended a series of cybersecurity postmarket controls. Previously, in October 2014, FDA published a guidance entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (Premarket Cybersecurity Guidance).[2] Taken together, these FDA guidance documents provide a framework for medical device manufacturers to create a comprehensive risk management program specifically focused on cybersecurity vulnerabilities of their medical devices that include some type of software or connectivity to networks.

Premarket Cybersecurity Risk Analysis

In its Premarket Cybersecurity Guidance, FDA recommends that medical device manufacturers develop a set of cybersecurity controls to reduce the likelihood that

[1] U.S. Food & Drug Admin., Postmarket Management of Cybersecurity in Medical Devices (Jan. 22, 2016), *available at* www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

[2] U.S. Food & Drug Admin., Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct. 2, 2014), *available at* www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

device functionality would be compromised by inadequate security and to maintain the integrity of medical device functionality and safety. As part of a premarket submission, FDA also expects a medical device manufacturer to provide documentation demonstrating how the manufacturer has considered cybersecurity risks and effectively implemented security controls in its device design.

That requirement includes, but is not limited to, establishing design inputs relating to cybersecurity. It also includes a cybersecurity management approach to software validation and a risk analysis as part of the manufacturer's quality system. FDA encourages manufacturers to address the following key elements:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies; and
- Assessment of residual risk and risk acceptance criteria.

While these key elements are similar to risk management processes implemented by medical device manufacturers today, FDA recommends that manufacturers follow five functions with respect to cypersecurity risks set out in NIST's "Framework for Improving Critical Infrastructure Cybersecurity" (NIST Framework):[3] Identify, Protect, Detect, Respond, and Recover.

Under the NIST Framework:

- "Identify and Protect" consists of: (1) identifying the cybersecurity risks of the medical device when used in connection with the wireless network, the Internet, or other portable media; and (2) appropriately implementing safeguards to

[3] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at:* www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

protect against such risks. Such protection could include allowing limited access to trusted users through password protection or biometric protections and restricting access to the software to trusted parties. FDA appreciates the impact that these security controls may have on usability and urges manufacturers to appropriately balance the need for security with efficient use and access given the devices' intended use and environment.

- "Detect, Respond, and Recover" involves implementing features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use. Manufacturers should consider safeguards that enable critical features of the device to continue to function even if a cybersecurity attack were to compromise the device.

Postmarket Cybersecurity Risk Analysis

Given the evolving nature of potential cybersecurity threats, FDA's Postmarket Cybersecurity Guidance emphasizes the need to continue to monitor, identify, and address potential cybersecurity risks after a device has been released to the market. To effectively monitor cybersecurity threats, it is important to recognize that information regarding cybersecurity vulnerabilities or attacks may come from non-traditional sources. While patient safety risks are traditionally identified through customer complaints, manufacturer investigations, or postmarket surveillance, intelligence about cybersecurity threats may originate from other industry sectors (e.g., finance or defense) or cybersecurity resources outside the medical device arena. These differences need to be taken into account when the manufacturer develops the postmarket elements of its cybersecurity risk management program.

FDA recommends that manufacturers incorporate cybersecurity considerations into the risk management program and apply the NIST Framework to their postmarket cybersecurity risk management program. Although at a high level the risk management recommendations are consistent with standard practices in the medical device industry, manufacturers should note a number of key differences and additions.

FDA recommends that manufacturers evaluate the risk to the device's "essential clinical performance" and remediate those risks down to an acceptable level. Specifically, under the draft Postmarket Cybersecurity Guidance, manufacturers should examine: (1) the exploitability of a cybersecurity vulnerability; and (2) the severity of harm to the patient if it were exploited.

This process is similar, in concept, to assessing probability of occurrence and severity of harm in a traditional risk assessment. However, FDA recommends that manufacturers use a cybersecurity vulnerability tool that evaluates a range of new factors. These factors include, for example:

- Attack Vector (physical, local, adjacent, network);
- Attack Complexity (high, low);
- Privileges Required (none, low, high);
- User Interaction (none, required);
- Scope (changed, unchanged);
- Confidentiality Impact (high, low, none);
- Integrity Impact (none, low, high);
- Availability Impact (high, low, none);
- Exploit Code Maturity (high, functional, proof-of-concept, unproven);
- Remediation Level (unavailable, work-around, temporary fix, official fix, not defined); and
- Report Confidence (confirmed, reasonable, unknown, not defined).

FDA also suggests that manufacturers perform threat modeling and an analysis of threat sources. Threat modeling optimizes network, application, or Internet security by identifying potential and actual vulnerabilities and defining countermeasures. Threat

modeling is different from traditional medical device risk management in that it provides a framework to assess threats from active adversaries or malicious users, which are common among cybersecurity threats.

Another key addition to the manufacturers' traditional risk management practices is the recommendation to proactively monitor cybersecurity-specific sources to identify potential cybersecurity threats or signals. These sources include Computer/Cyber Emergency Response/Readiness Teams, Information Sharing and Analysis Organizations, security researchers, or other critical infrastructure or industries. The early detection of emerging threats will assist manufacturers in timely addressing new exploits that could adversely impact patient safety. FDA also encourages manufacturers to incorporate detection mechanisms into their devices to enhance the identification of attacks and assist in exploit forensics.

Conclusion

Although the postmarket cybersecurity guidance is draft only, it does provide a glimpse into FDA's current thinking on the subject. Given the number of guidances released by FDA in the last two years, it can be assumed that this topic is very much on the frontier of FDA's regulatory efforts. Cybersecurity risks are a topic that FDA will continuously assess during pre-market review and post-market surveillance to ensure that the public health is being protected. It is critical for medical device manufacturers that are either planning to develop a medical device that could be subject to cyber-attacks, or have one on the market already, to assess their risk management programs to ensure the aforementioned issues are addressed. Manufacturers must submit any comments and suggestions regarding the guidance 90 days from January 15, 2016.