The FDA Steps Up Efforts to Address Medical Device Cybersecurity

PG Bulletin

December 6, 2018

Elizabeth F. Hodge (Akerman LLP, West Palm Beach, FL)

*This Bulletin is brought to you by AHLA's Health Information and Technology Practice Group.**

The Food and Drug Administration (FDA) has been in the news over the past few months regarding its efforts to improve the cybersecurity of medical devices, especially connected medical devices. As more medical devices use wireless, Internet, and network connectivity, the opportunities to provide cost-effective care to more people increases, but so do the risks to patient safety. The recent WannaCry ransomware and Petya/NotPetya attacks, along with demonstrations by "white hat hackers" of how connected devices may be compromised, highlight how cybersecurity threats to the health care sector are increasing in frequency and severity and having a greater clinical impact on health care facility operations and patient safety. Over the last couple of months, the FDA has announced a number of initiatives to address the growing threats to medical device functionality and patient safety, some of which are described below.

To better understand these initiatives, it is helpful to first consider two recent reports from the U.S. Department of Health and Human Services Office of Inspector General (OIG) addressing the FDA's previous premarket and postmarket efforts regarding medical device cybersecurity.

OIG Report on FDA Premarket Review Process for Medical Devices

In September 2018, the U.S. Department of Health and Human Services Office of Inspector General (OIG) issued a report, *FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices*.[1] The report is the result of OIG's examination of the FDA's review of cybersecurity risks and controls to mitigate those risks before clearing or approving networked medical devices for use in the United States. To receive FDA clearance or approval for a networked device, the manufacturer must submit documentation that the device is safe and effective.

The OIG found that while the FDA reviews the cybersecurity documentation provided by device manufacturers as part of the premarket submission process, the agency could further integrate cybersecurity in the review process by:

- Promoting the use of pre-submission meetings to address cybersecurity-related questions;
- Including cybersecurity documentation in the FDA's "Refuse-To-Accept" checklists used to review 510(k) and premarket approval (PMA) submissions so such documentation must be submitted before the agency accepts a submission for review; and
- Including cybersecurity as an element in the Smart template used to review 510(k) submissions to ensure consistent cybersecurity reviews and to provide FDA reviewers the opportunity to explain the results of their review.

The FDA concurred with the OIG's recommendations, noting that it integrated cybersecurity into the Smart template beginning in September 2016. It also plans to specifically identify cybersecurity as a checklist item when it next updates the "Refuse-To-Accept" checklist. Finally, the FDA said that it would specifically mention cybersecurity in its next planned update of its pre-submission guidance. As described in more detail below, in October 2018, the FDA released a draft update to its *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*guidance document.

OIG Report on FDA Policies Addressing Postmarket Cybersecurity Risk to Medical Devices

The OIG followed its report on the FDA's premarket review process for networked medical devices with a report released November 1, 2018 addressing the agency's policies for assessing postmarket cybersecurity risk to devices, *The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices.*[2] The report on the FDA's postmarket policies and procedures was prompted in part by concern from the public and Congress regarding the risks to patient safety posed by connected medical devices. The OIG reviewed the FDA's plans and processes for timely communicating and addressing cybersecurity medical device compromises in the postmarket phase of the devices' lifecycle.

The OIG found that while the FDA had plans and processes for addressing certain medical device problems after the device was on the market, those plans and processes were deficient in addressing medical device cybersecurity compromises and the FDA had not tested its ability to respond to emergencies resulting from cybersecurity incidents involving medical devices. As a result, the OIG recommended that the FDA:

- Continually assess the cybersecurity risks to medical devices and update the agency's plans and strategies to address those risks;
- Establish written procedures and practices for securely sharing sensitive information about cybersecurity events with key stakeholders who have a "need to know";
- Enter formal agreements with federal agency partners that establish roles and responsibilities and the support those agencies will provide to assist the FDA in its mission with respect to medical device cybersecurity; and
- Establish and maintain procedures for handling recalls of medical devices vulnerable to cybersecurity vulnerabilities and threats.

The FDA said that it already implemented some of the OIG's suggestions before the report’s release. For example, as described more fully below, the FDA entered into a Memorandum Agreement with the Department of Homeland Security (DHS) in October 2018 that documents the roles of the respective agencies for addressing threats and challenges involving medical device cybersecurity.

Updated Guidance on FDA Premarket Submissions

On October 18, 2018, the FDA issued *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices—Draft Guidance*,[3] which updates the final guidance on premarket submissions that FDA previously issued in 2014. The draft guidance responds to the rapidly evolving cybersecurity landscape and issues identified by the OIG in its report on the FDA's premarket review cybersecurity review process. When finalized, the new draft guidance will supersede the October 2014 guidance document.

The recommendations in the draft guidance are intended to help device manufacturers to:

- use a risk-based approach in designing and developing medical devices with appropriate cybersecurity protections;
- take a holistic approach to device cybersecurity by assessing risks and mitigations throughout the lifecycle of the device;
- ensure maintenance and continuity of critical device safety and essential performance; and
- promote the development of trustworthy devices.[4]

One of the more noteworthy recommendations regarding adoption of a risk-based approach to the design of devices is for device manufacturers to provide a Cybersecurity Bill of Materials (CBOM). The draft guidance describes the CBOM as a list of commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities. Such a list could enable device customers and users to more effectively manage cybersecurity vulnerabilities and respond more quickly to potential threats.

To assist device manufacturers in designing secure devices and providing supporting documentation to the FDA, the draft guidance creates (for purposes of the Premarket Guidance only) two tiers of medical devices:

- Tier 1 ("Higher Cybersecurity Risk") for those devices:
    - Capable of connecting to another medical or non-medical product, a network, or the Internet; and
    - Where a cybersecurity incident affecting the device could result in patient harm to multiple patients.
- Tier 2 ("Standard Cybersecurity Risk") for those medical devices that do not meet the criteria for a Tier 1 device.

The FDA will host a public workshop for various stakeholders on January 29–30, 2019 to discuss the draft guidance. The FDA is particularly interested in receiving comments about the proposed CBOM, including the type of information and level of detail that should be included in a CBOM, the format the CBOM should take, and whether a CBOM should include software and hardware components. The deadline to submit comments to the FDA regarding the draft guidance is March 18, 2019.

Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook

In October 2018, the MITRE Corporation, with support from the FDA, released a *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook*[5] to assist health care delivery organizations (HDOs) to better prepare for and respond to cybersecurity issues that could affect the functionality of medical devices and continuity of patient care. The Playbook addresses challenges identified by HDOs in the aftermath of the WannaCry ransomware and the Petya/NonPetya attacks, including not knowing with whom to communicate, what actions should be considered to respond to such an attack, and what resources are available to assist HDOs in responding to cyber attacks.

The Playbook offers HDOs an open source and customizable framework that they can use as part of their emergency response plan to limit disruptions to the functioning of connected medical devices and, among other topics, addresses:

- Preparedness, including preparing a device asset inventory, performing a hazard vulnerability analysis, and training workforce members;
- Detection and analysis, including incident detection and validation and reporting;
- Containment, eradication and recovery; and
- Post-incident activity, including identifying lessons learned and updating the HDO's response plan.

Echoing FDA's position that cybersecurity is a shared responsibility, the Playbook promotes regional outreach and collaboration as part of HDOs' readiness and response activities. Engaging with regional partners can stretch limited resources and maintain continuity of patient care if an incident occurs. The Playbook framework is designed to enable a unified response to a cybersecurity event within HDOs and across regions.

FDA—DHS Memorandum Agreement

As mentioned above, in October 2018, the FDA and DHS announced a Memorandum Agreement[6]to implement a new framework for "greater coordination and cooperation" between the two agencies to address cybersecurity in medical devices. The agreement is intended to further improve information sharing between the agencies about potential or confirmed medical device cybersecurity threats and vulnerabilities resulting in better responses to potential and actual threats to patient safety.

Under the agreement DHS will continue its role as the central medical device vulnerability coordination center and the FDA will advise DHS regarding the risk to patient safety posed by cybersecurity threats and vulnerabilities. DHS also will consult with the FDA for technical and clinical expertise regarding medical devices.

Conclusion

As the FDA has repeatedly said, medical device cybersecurity is a shared responsibility among device manufacturers, health care facilities, health care providers, and patients. The agency's recent initiatives to address cybersecurity risks involving networked medical devices should be reviewed by all stakeholders so that the benefits to patient health these devices offer are not outweighed by the risks to patient safety.

**AHLA thanks the Health Information and Technology Practice Group for sharing this Bulletin with the Academic Medical Centers and Teaching Hospitals, Business Law and Governance, Life Sciences, and Physician Organizations Practice Groups.*

[1] *Available at* https://oig.hhs.gov/oei/reports/oei-09-16-00220.asp.
[2] *Available at* https://oig.hhs.gov/oas/reports/region18/181630530.asp.
[3] *Available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf.
[4] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices—Draft Guidance, October 18, 2018, at p. 9.
[5] *Available at* https://www.mitre.org/publications/technical-papers/mitre-creates-playbook-on-medical-device-cybersecurity.
[6] *Available at*https://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm623568.htm.