U.S. Department of Health & Human Services

Office of Inspector General

FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices

OEI-09-16-00220
September 2018

oig.hhs.gov

Suzanne Murrin
Deputy Inspector General for
Evaluation and Inspections

Report in Brief
September 2018
OEI-09-16-00220

U.S. Department of Health & Human Services
Office of Inspector General

FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices

Key Takeaway
FDA has taken steps to address emerging cybersecurity concerns in networked medical devices by issuing guidance, reviewing cybersecurity information in submissions, and—when needed—obtaining additional information from manufacturers. FDA could take additional steps to more fully integrate cybersecurity into its premarket review process.

What OIG Found

To assure the public that networked medical devices are safe and effective and that manufacturers are safeguarding their devices from potential cybersecurity threats, the Food and Drug Administration (FDA) reviews the cybersecurity documentation in premarket submissions that manufacturers submit to FDA before the devices can be marketed. FDA uses its 2014 guidance on the content of premarket submissions and cybersecurity as general principles to assist its review. FDA reviewers explained to us that they consider known cybersecurity risks and threats when reviewing submissions and apply that knowledge to devices that display similar risk profiles. For example, if FDA identifies a cybersecurity threat to a certain cardiac device from a specific manufacturer, it considers that same threat in evaluating submissions for similar cardiac devices from other manufacturers.

FDA reviewers look for cybersecurity documentation in the submissions. Such documentation may include a hazard analysis or a matrix that describes the device's cybersecurity risks, controls to mitigate those risks, and threats that the manufacturer considered. FDA reviewers often request additional information from manufacturers when submissions lack sufficient cybersecurity documentation or when clarification is needed. At the time of our review, FDA had almost always cleared or approved the cybersecurity aspect of networked medical devices because manufacturers had been able to respond with supplemental cybersecurity information that FDA deemed sufficient. FDA staff told us that manufacturers could use presubmission meetings to better understand what cybersecurity information FDA needs and the steps they need to take as they design their devices.

FDA could further integrate cybersecurity into its overall review process. FDA's "Refuse-To-Accept" checklists, which the agency uses to screen submissions for completeness, do not include checks for cybersecurity information. Also, FDA's "Smart" template, which FDA uses to guide its reviews of submissions, does not prompt FDA reviewers with specific cybersecurity questions to consider and also lacked a dedicated section for recording the results of the cybersecurity review.

What OIG Recommends

We recommend that FDA promote the use of presubmission meetings to address cybersecurity-related questions, include cybersecurity documentation as a criterion in FDA's Refuse-To-Accept checklists, and include cybersecurity as an element in the Smart template. FDA concurred with all three recommendations.

Full report can be found at oig.hhs.gov/oei/reports/oei-09-16-00220.asp

Why OIG Did This Review

Cybersecurity is an area with increasing risk to patients and the health care industry as more medical devices use wireless, Internet, and network connectivity. Researchers have shown that networked medical devices cleared or approved by FDA can be susceptible to cybersecurity threats, such as ransomware and unauthorized remote access, if the devices lack adequate security controls. These networked medical devices include hospital-room infusion pumps, diagnostic imaging equipment, and pacemakers.

FDA has emphasized that cybersecurity for medical devices is a responsibility shared among device manufacturers, health care providers, consumers, and FDA itself. Manufacturers design networked medical devices that can include security controls to mitigate the cybersecurity risks. They then seek FDA clearance or approval of their devices. As the Federal agency responsible for regulating these devices, FDA may consider the cybersecurity risks and controls in its overall assessment of a device's safety and effectiveness. Ultimately, FDA determines whether a networked medical device may be legally marketed in the United States.

How OIG Did This Review

To examine FDA's review of cybersecurity in premarket submissions for networked medical devices, we interviewed FDA staff who carry out and manage the reviews and interviewed members of the FDA's Cybersecurity Workgroup. We examined a nonrepresentative sample of 22 submissions and FDA reviewer notes for networked medical devices that FDA cleared or approved in 2016. We reviewed FDA policies, procedures, and guidance documents related to its medical device review process and to cybersecurity.

TABLE OF CONTENTS

BACKGROUND

Objective

To examine the Food and Drug Administration's review of cybersecurity risks and controls to mitigate those risks before it clears or approves networked medical devices for use in the United States.

Advancements in medical technology have led to a new generation of innovative medical devices that include functionalities such as wireless, Internet, and network connectivity.[1] These networked medical devices are becoming increasingly common and are being used to deliver care, remotely monitor patients, and transfer patient data efficiently and accurately. However, these networked functionalities introduce a new area of risk: cybersecurity. The Food and Drug Administration (FDA) defines cybersecurity as the process of preventing the following: unauthorized access; unauthorized modification; misuse or denial of use; or unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.[2]

Networked medical devices that do not have adequate controls may pose cybersecurity risks that can adversely affect device functionality, disrupt the delivery of health services, and lead to patient harm. For example, in 2015, FDA alerted the public that a networked infusion pump[3] could be remotely accessed and controlled by an unauthorized user because of a cybersecurity vulnerability. Because of the risk that an attacker could maliciously change the medication dosage that the pump delivered and harm the patient, FDA encouraged health care facilities to discontinue using this pump and

[1] The term "device" includes an instrument, machine, implant, or similar article that is intended for use in the diagnosis of a disease or other condition, or in the cure, mitigation, treatment, or prevention of a disease, or that is intended to affect the structure or function of the body. "Device" does not include certain software functions. For a complete definition of "device," see sections 201(h) and 520(o) of the Federal Food, Drug, and Cosmetic Act (FD&C Act).

[2] FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, October 2, 2014. Accessed at https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf on May 21, 2018.

[3] In general, an infusion pump is a medical device used to deliver fluids (e.g., insulin, hormones, chemotherapy drugs, and pain relievers) into a patient's body in a controlled manner. FDA, *What Is an Infusion Pump?* December 2017. Accessed at https://www.fda.gov/medicaldevices/productsandmedicalprocedures/generalhospitaldevicesandsupplies/infusionpumps/ucm202495.htm on August 22, 2018.

transition to an alternative infusion pump system.[4] Exhibit 1 illustrates examples of networked medical devices and cybersecurity risks that have been identified in the devices.

Exhibit 1. Examples of Networked Medical Devices and Their Potential Cybersecurity Risks

An infusion pump that automatically connects to a network using a hard-coded or default password may allow a remote attacker to gain unauthorized control of the device and tamper with a patient's medication dosage.

An implantable pacemaker that improperly validates or authenticates users may allow a nearby attacker to issue unauthorized commands to the device and deliver inappropriate pacing to a patient.

Medical imaging systems (e.g., ultrasound and MRI machines) that use software that is no longer supported or that has not received proper security patches or updates may be vulnerable to attacks, such as ransomware, and delay the delivery of patient care.

Source: OIG analysis of reported cybersecurity threats to networked medical devices.

FDA's Regulation of Networked Medical Devices

FDA's Center for Devices and Radiological Health (CDRH) is responsible for regulating medical devices, including networked medical devices. The Medical Device Amendments of 1976 amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) and provided FDA with a framework for regulating medical devices. The FD&C Act requires FDA to classify medical devices, including those that are networked, into three regulatory classes: Class I, Class II, and Class III.[5] In general, Class I medical devices are those that pose a low risk of harm, such as elastic bandages. Class II medical devices, such as certain infusion pumps,[6] pose a moderate risk of harm. Class III medical devices, such as implantable pacemakers, pose a high risk and generally are life-sustaining or life-supporting devices. The regulatory classification is based on the level of control necessary to provide reasonable assurance of the device's safety and effectiveness.

[4] FDA, *Symbiq Infusion System by Hospira: FDA Safety Communication – Cybersecurity Vulnerabilities*, May 2015. Accessed at http://wayback.archive-it.org/7993/20170722144742/https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm on May 21, 2018.

[5] Section 513 of the FD&C Act.

[6] Some infusion pumps are classified as Class III devices. FDA, *Infusion Pumps Total Product Life Cycle*, December 2014. Accessed at https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM209337.pdf on May 21, 2018.

As it does with other medical devices, FDA regulates networked medical devices using a "total product lifecycle" approach, which consists of two phases: premarket and postmarket.[7] In the premarket phase, FDA assesses whether a networked medical device is safe and effective for its intended use. To receive FDA clearance or approval to market a networked medical device in the United States, a manufacturer must submit to FDA proper documentation showing that its device is safe and effective. In the postmarket phase—after FDA clears or approves a networked medical device—FDA conducts oversight activities, such as monitoring and investigating the networked medical device's safety and effectiveness, and alerting the public of problems when warranted.[8]

FDA's Premarket Clearance and Approval Process for Networked Medical Devices

In general, manufacturers that wish to market moderate-risk or high-risk networked medical devices in the United States must seek FDA clearance or approval. Typically, manufacturers do not need to obtain FDA clearance or approval if they are seeking to market low-risk networked medical devices.

Manufacturer Premarket Submissions. Typically, to initiate the FDA clearance or approval process, a manufacturer must submit to FDA one of the following two types of premarket submissions: a 510(k) submission (also known as a premarket notification submission) or a premarket approval (PMA) submission. FDA receives more 510(k) submissions than PMAs.[9]

In general, a manufacturer that wishes to market a moderate-risk networked medical device must submit to FDA a 510(k) submission.[10, 11] In general, a manufacturer that submits a 510(k) submission must provide reasonable assurance of its device's safety and effectiveness by showing that the device is substantially equivalent to a legally marketed device that is not subject to a PMA.[12]

[7] FDA, "FDA's Role in Medical Device Cybersecurity," *FDA Voice*, October 31, 2017. Accessed at https://blogs.fda.gov/fdavoice/index.php/2017/10/fdas-role-in-medical-device-cybersecurity/ on May 21, 2018.

[8] FDA, *The Device Development Process, Step 5: FDA Post-Market Device Safety Monitoring*, January 2018. Accessed at https://www.fda.gov/ForPatients/Approvals/Devices/ucm405428.htm on May 21, 2018.

[9] LCDR Kimberly Piermatteo, CDRH, FDA, *The 510(k) Program* (CDRH learning module), November 2014. Accessed at http://fda.yorkcast.com/webcast/Play/d91af554691c4260b5eca0b2a28e636b1d on May 21, 2018.

[10] Section 510(k) of the FD&C Act.

[11] For some low-risk to moderate-risk medical devices of a new type (i.e., a type for which a legally marketed device does not exist), manufacturers may submit to FDA a "De Novo" request. The granting of a De Novo request creates a new regulatory classification, which enables subsequent devices with the same intended use to go through FDA's 510(k) process.

[12] Section 510(k) of the FD&C Act and 21 CFR pt. 807. See also FDA, *The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications [510(k)]*, July 2014. Accessed at https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM284443.pdf on May 21, 2018.

Manufacturers who wish to market a high-risk networked medical device must submit to FDA a PMA submission. Unlike most 510(k) submissions, a PMA submission must include clinical and nonclinical data demonstrating a device's safety and effectiveness.[13]

FDA's Presubmission Program. FDA's presubmission program allows a manufacturer to voluntarily seek and obtain formal, targeted feedback from FDA on the design, development, or testing of its medical device or its premarket submission.[14] During the presubmission meeting, a manufacturer may ask FDA specific questions, such as whether a device's cybersecurity controls and testing of those controls satisfies FDA's standard for clearance or approval, and may receive written feedback.[15] The meetings are intended to provide manufacturers with an efficient path to developing and marketing their networked medical devices in the United States.[16]

FDA Review of Submissions. FDA assigns a team of FDA staff to review the submission. The team conducts its review in two stages: an initial review and a substantive review. During the initial review, the team determines whether the submission is complete and whether the manufacturer has submitted the appropriate and necessary documentation.[17] After the team determines that the submission is administratively complete, they begin their substantive review. This entails reviewing the submission for various elements—like information on cybersecurity, labeling, software, and performance data—to assess the device's safety and effectiveness. A 510(k) submission that meets all of the premarket requirements results in FDA's "clearing" the device. A PMA submission that meets all of the premarket requirements result in FDA's "approving" the device. On its website, FDA posts information about networked devices that are cleared or approved.

[13] Section 515 of the FD&C Act and 21 CFR pt. 814.

[14] FDA, *Requests for Feedback on Medical Device Submissions: The Pre-Submission Program and Meetings with Food and Drug Administration Staff*, September 2017. Accessed at https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM311176.pdf on May 21, 2018.

[15] Presubmission meeting discussions between a manufacturer and FDA are not binding.

[16] Ibid.

[17] FDA, *Acceptance and Filing Reviews for Premarket Approval Applications (PMAs)*, January 2018. Accessed at https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM313368.pdf on May 21, 2018. FDA, *Refuse to Accept Policy for 510(k)s*, January 2018. Accessed at https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm315014.pdf on May 21, 2018.

FDA Cybersecurity Requirements and Guidance

A manufacturer that seeks to market its networked medical device must discuss the device's cybersecurity risks and controls to mitigate those risks in its 510(k) or PMA submission. FDA's Quality System Regulation requires that the manufacturer establish and maintain procedures for software validation and a risk analysis. FDA also requires that the manufacturer include in its submission this risk analysis,[18] which should include an analysis of the cybersecurity risks associated with the device.[19] Over the years, FDA has issued several guidance documents relating to the management of cybersecurity for medical devices.[20] FDA has also begun exploring other ways to address this concern, such as through its digital health initiatives.[21]

Premarket Cybersecurity Guidance. In October 2014, FDA issued a guidance document—*Content of Premarket Submission for Management of Cybersecurity in Medical Devices*—to assist manufacturers in preparing their submissions for networked medical devices and to guide FDA during its review.[22] In this report, we refer to this document as the premarket cybersecurity guidance. This guidance recommends that when manufacturers design and develop networked medical devices, they consider certain factors, such as identifying potential cybersecurity threats (e.g., unauthorized users' exploiting a vulnerability), the likelihood of the threats, the impact of the threats, and strategies to address the threats. These recommendations are intended to assist manufacturers in effectively managing the cybersecurity risks of their networked medical devices.

The guidance also recommends that manufacturers include documentation in their submissions to demonstrate that—as part of the validation and risk analysis that the Quality System Regulation requires—they considered cybersecurity in their networked medical devices. See Exhibit 2 for the types of cybersecurity documentation that FDA recommends manufacturers include in their submission. FDA has conducted several outreach activities to promote the guidance and educate manufacturers about it.[23]

[18] 21 CFR § 820.30(g).

[19] FDA, *FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity*, no date. Accessed at https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf on May 21, 2018.

[20] FDA guidance documents for industry on cybersecurity for medical devices include *Postmarket Management of Cybersecurity in Medical Devices* (December 2016), *Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices* (May 2005), and *Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software* (January 2005).

[21] FDA, *Digital Health Innovation Action Plan*, 2017. Accessed at https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm568735.pdf on May 21, 2018.

[22] FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, October 2, 2014. Accessed at https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf on May 21, 2018.

[23] For a list of FDA's outreach activities, see FDA's Digital Health webpage on cybersecurity at https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.

Exhibit 2. Cybersecurity Information That FDA Recommends Manufacturers Include in Their Submissions for Networked Medical Devices

1. A hazard analysis listing the cybersecurity risks that were considered and the cybersecurity controls established in the device.
2. A traceability matrix that links the actual cybersecurity controls to the cybersecurity risks that were considered.
3. Manufacturer's plans for validating and updating the software.
4. A description of controls in the software supply chain to assure integrity.
5. Device instructions and recommended cybersecurity controls appropriate for the intended use environment (e.g., antivirus software).

Source: FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, October 2014.

FDA Cybersecurity Workgroup. In response to the emerging cybersecurity concerns related to networked medical devices, FDA established a cybersecurity working group in 2013. The Cybersecurity Workgroup is charged with defining and evolving FDA's thinking about its oversight of medical device cybersecurity. This task includes working with the medical device industry and other stakeholders and formulating policies and guidance on medical device cybersecurity. The workgroup is composed of staff from CDRH and FDA's Center for Biologics Evaluation and Research[24] who have experience in reviewing submissions for networked medical devices, in responding to reports of cybersecurity concerns, and in participating in advisory committees, and who have scientific and engineering backgrounds.

Related Work

In addition to this evaluation, OIG is conducting an audit of FDA's plans and processes for responding to cybersecurity vulnerabilities affecting medical device that are already in the market.[25] The results of the audit are forthcoming.

In 2012, the Government Accountability Office (GAO) released a report related to FDA and implantable wireless medical devices, such as insulin pumps and cardiac defibrillators.[26] GAO reported that FDA considered cybersecurity risks from *unintentional* threats (e.g., a metal detector's

[24] The Workgroup includes Center for Biologics Evaluation and Research staff who review networked medical devices that handle biological products, such as blood and plasma.
[25] OIG Office of Audit Services report on FDA's postmarket plans and processes for responding to cybersecurity vulnerabilities identified in medical devices that are already in the market (A-18-16-30530), forthcoming.
[26] GAO, *FDA Should Expand Its Consideration of Information Security for Certain Types of Devices* (GAO-12-816), August 2012. Accessed at https://www.gao.gov/products/GAO-12-816 on May 21, 2018.

interfering with a pacemaker) but did not consider risks from *intentional* threats, such as hacking. Among other things, GAO recommended that FDA expand its consideration of cybersecurity to include intentional threats to implantable wireless medical devices. According to GAO, FDA has implemented the recommendation.

Methodology

We examined FDA's policies, procedures, and guidance documents on its review of 510(k) and PMA submissions, networked medical devices, and cybersecurity .

We conducted structured interviews with three groups of FDA staff to understand how FDA reviewed submissions for networked medical devices and how it assessed cybersecurity information, such as a device's cybersecurity risks and controls. We interviewed FDA reviewers who conduct the cybersecurity reviews, their managers, and members of the FDA Cybersecurity Workgroup. We analyzed their responses to learn more about FDA's approach to reviewing cybersecurity information in submissions for networked medical devices.

To help inform our structured interviews with FDA staff, we also reviewed a nonrepresentative sample of 22 submissions for networked medical devices that FDA cleared or approved in 2016. We reviewed cybersecurity information in each submission's hazard analysis, traceability matrix, software update plan, software description, and/or device instructions. We also reviewed any FDA reviewer notes that were related to a device's cybersecurity risks and controls. We analyzed cybersecurity information and reviewer notes to use as illustrative examples of FDA's approach to reviewing a device's cybersecurity risks and controls. We did not evaluate the appropriateness of FDA's clearance or approval of the cybersecurity aspect of a networked medical device. See Appendix A for more details on our selection of submissions.

Limitations

We did not independently verify FDA staff's self-reported information from the group interviews. Our analysis of the 22 selected submissions provides information about FDA's review process for networked medical devices but is not projectable to the full population of premarket submissions for medical devices.

Standards

This study was conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

FINDINGS

FDA reviews medical-device submissions for cybersecurity information and uses the premarket cybersecurity-related guidance as general principles to assist its review

FDA reviews cybersecurity information in submissions for networked medical devices during the substantive review process. FDA's review is intended to assure the public that networked medical devices are safe and effective and that manufacturers give adequate attention to safeguarding their networked medical devices from cybersecurity threats. Although cybersecurity threats cannot be eliminated, FDA looks for the risks that manufacturers considered and assesses the controls that they implemented to address those risks. For example, an FDA reviewer explained that when she reviews an implantable glucose system or insulin pump with Bluetooth or Wi-Fi capabilities, she checks whether the device uses data encryption and authentication to reduce the risk that an unauthorized user could take control of the device and overdeliver insulin to harm a patient.

> When we do our reviews, we try to make sure that manufacturers have done their due diligence to enhance their device's cybersecurity.
>
> -FDA Manager

Who at FDA conducts the cybersecurity reviews of networked medical devices?

CDRH Division staff. The FDA reviewers who conduct the general review of a submission for a networked medical device also often conduct the cybersecurity-specific review. The FDA reviewers are from the different divisions within CDRH (e.g., the cardiovascular division, the radiological health division, or the chemistry and toxicology division) and they specialize in reviewing specific types of devices. For example, implantable pacemakers are reviewed by reviewers from CDRH's cardiovascular division, whereas ultrasound or MRI machines are reviewed by reviewers from CDRH's radiological health division. New FDA reviewers are matched with mentors who review similar types of devices. FDA reviewers also reported being trained on the premarket cybersecurity guidance and regularly meet with subject-matter experts at CDRH to discuss current trends in cybersecurity for medical devices.

Office of Science and Engineering Laboratories staff. CDRH Division staff have the option to request that staff from CDRH's Office of Science and Engineering Laboratories (OSEL) conduct certain cybersecurity reviews. For example, FDA reviewers reported that if a networked medical device is complex or beyond their expertise, they will turn over the cybersecurity review to subject-matter experts at OSEL. OSEL staff specialize in providing technical, scientific, and engineering expertise to FDA reviewers. Among the submissions that we reviewed, OSEL staff conducted cybersecurity reviews on two types of networked medical devices: implantable insulin pumps and infusion pumps. These two device types were known to have cybersecurity vulnerabilities that were identified by cybersecurity researchers.

Source: OIG analysis of FDA staff interviews and FDA policies and procedures, 2017.

FDA uses its premarket cybersecurity guidance when reviewing submissions

During the substantive review process, FDA reviewers use the premarket cybersecurity guidance as general principles for reviewing cybersecurity information in the submissions. FDA reviewers explained that they review the submissions for the types of cybersecurity documentation that the premarket cybersecurity guidance recommends, which include a hazard analysis or traceability matrix that outlines the device's cybersecurity risks and associated controls for those risks. For example, when examining a hazard analysis or traceability matrix, FDA reviewers assess information provided by the manufacturer, such as the device's cybersecurity vulnerabilities; the likelihood of the cybersecurity threats; the potential impact or harm of those threats; and the controls used to address the cybersecurity vulnerabilities.

In addition, FDA reviewers examine any software update plans and cybersecurity-related instructions or specifications for end users. For example, in FDA's review of a submission for a glucose monitoring system, an FDA reviewer noted that she examined cybersecurity information in the device's user manuals but did not find any information on how the manufacturer included cybersecurity in the device's design. The FDA reviewer explained that the device relied heavily on users to protect against cybersecurity threats by using antivirus software and enabling firewalls. The FDA reviewer requested that the manufacturer update its hazard analysis to address the missing information. The manufacturer did so, and FDA found the update to be acceptable.

FDA staff explained that when reviewing cybersecurity documentation, they look for evidence of the things that manufacturers have considered, such as core cybersecurity functions identified in the premarket cybersecurity guidance. These core functions are described in Exhibit 3 on the next page. FDA's assessment of the core functions varies from device to device, in part because the cybersecurity threats depend on the device's functionality and features. FDA reviewers also consider other factors, such as the environment in which the device will be used. An FDA reviewer explained that when reviewers review a submission, they are always looking at the risks that are specific to the device.

Exhibit 3. Cybersecurity Core Functions and Activities that Manufacturers Should Consider in the Design and Development of Networked Medical Devices

Identify. Identify the networked medical device's intended use, use environment, type of connectivity, cybersecurity vulnerabilities, likelihood of threat, and probable risk of harm.

Protect. Protect the networked medical device using appropriate security controls.

Detect. Implement features that allow for cybersecurity threats to be detected, recognized, and logged.

Respond. Develop a response plan that end users can use and implement features that will protect a device's critical function in the case of a cybersecurity attack.

Recover. Provide methods for retaining and recovering control of a device.

Source: FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, October 2014.

FDA considers known cybersecurity risks in its review of submissions for networked medical devices

When conducting their cybersecurity reviews, FDA staff use information about previously identified cybersecurity risks. For example, in its review of a submission for an insulin pump that used certain software, the FDA reviewer took into account a widely known password vulnerability that was identified in a similar device that was marketed by the same manufacturer.

> We are continually learning about the extent of cyber threats. We see something happen to one manufacturer and consider that it might happen to another.
>
> -FDA Cybersecurity Workgroup member

FDA staff also shared an example of using their knowledge of a cybersecurity vulnerability in a cardiac device to ensure that other manufacturers give adequate attention to safeguarding their devices from cybersecurity threats. In a recent high-profile incident, FDA became aware of the risk that unauthorized users could be able to access and control an implantable cardiac device. Although no actual harm occurred, "white hat" hackers demonstrated that they could modify the device's settings, deplete the device's battery life, and administer inappropriate pacing or shock to a patient. FDA staff told us that the cybersecurity incident spurred FDA to hold presubmission meetings with multiple device manufacturers who were preparing submissions for similar implantable cardiac devices, like pacemakers and cardiac defibrillators.

During these presubmission meetings, FDA discussed with each manufacturer the newly discovered vulnerability and inquired what cybersecurity controls their devices had to address this type of threat. The presubmission meetings provided an opportunity for FDA to ask

manufacturers pointed questions about the cybersecurity risks and controls of their devices and to discuss information that manufacturers might not have known FDA was interested in reviewing as part of a submission.

FDA often needs to request supplemental cybersecurity information, which manufacturers are typically able to supply

FDA reviewers often request additional cybersecurity documentation from manufacturers during the premarket review process. Despite FDA's October 2014 release of the premarket cybersecurity guidance and its outreach to the medical device industry, FDA staff reported that they still receive initial submissions that insufficiently cover cybersecurity. When this happens, FDA reviewers issue to the manufacturer a deficiency letter that lists the reviewers' cybersecurity concerns about the networked medical device.

> Four years ago we were not looking for cybersecurity documentation all of the time. Now, if it is missing, we'll be asking questions.
>
> -FDA Cybersecurity Workgroup member

FDA staff reported that during the substantive review phase, they work extensively with manufacturers—through interactive meetings or emails—to address deficiencies in cybersecurity information. In the submissions that we reviewed, FDA reviewers often requested additional cybersecurity information and referred manufacturers to the premarket cybersecurity guidance to explain FDA's thinking. See Exhibit 4 for an example of a submission that had insufficient cybersecurity information and how the manufacturer addressed it. Because manufacturers have typically been able to provide FDA with the requested cybersecurity information to address deficiencies, FDA reported that at the time of our review, it had almost always cleared or approved the cybersecurity aspects of networked medical devices.

> We work extensively with a manufacturer if documentation is not sufficient.
>
> -FDA Reviewer

Exhibit 4. Example of a Submission That Lacked Sufficient Cybersecurity Information

FDA concluded that the manufacturer of a cardiovascular software diagnostic device did not provide enough information in its hazard analysis to assess the adequacy of the device's cybersecurity risks and controls to mitigate those risks. The manufacturer's initial submission provided a brief discussion of the device's data security risks and controls, but did not identify hazards related to its use of software or network connectivity. FDA noted this deficiency and requested that the manufacturer submit a full cybersecurity plan and a detailed description of its risk assessment, controls, and testing data. In response, the manufacturer provided FDA with a cybersecurity plan and, among other things, updated its traceability matrix linking the device's risks and controls. FDA then determined that the additional information was acceptable.

Source: OIG Analysis of Premarket Submissions, 2017.

FDA staff told us that more manufacturer use of FDA's presubmission program could help avoid the problem of submissions with insufficient cybersecurity information. FDA staff reported that during the presubmission meetings, manufacturers rarely ask questions related to cybersecurity and their devices. If manufacturers used these meetings to receive early, targeted feedback on cybersecurity, it could reduce their back-and-forth engagement with FDA and potentially decrease the amount of time that FDA takes to review a submission. FDA staff also said that presubmission meetings could help manufacturers, particularly those of high-risk devices, better understand the information that they need to prepare and include in their submissions, and the steps they need to take to mitigate cybersecurity threats to their devices.

Tools that FDA uses to review submissions for networked medical devices do not incorporate checks for cybersecurity information

FDA has not fully integrated cybersecurity into two types of written tools that FDA reviewers use to facilitate their reviews of networked medical devices. One tool is used to screen submissions during FDA's initial review. The other is a key template that FDA reviewers use during their substantive review to guide and organize the results of their review. FDA developed these tools before the increase in submissions of networked medical devices and in cybersecurity threats.

FDA's Refuse-To-Accept checklists, which it uses to screen 510(k) and PMA submissions for completeness, do not include a check for cybersecurity information

Because FDA's initial reviews of submissions do not include a check for cybersecurity information, FDA may accept 510(k) and PMA submissions that lack cybersecurity documentation, which may cause delays in FDA's review. While FDA's Refuse-To-Accept checklists identify specific criteria needed for acceptance—such as documentation on software, labeling, sterilization, engineering, and testing—they do not ask for documentation on cybersecurity. The Refuse-To-Accept checklists, which are publicly available, outline for manufacturers the minimum criteria that FDA uses to determine whether it may accept a 510(k) or PMA submission for substantive review.[27] If any of the required information is missing, FDA may refuse to accept the submission until the manufacturer provides it.

FDA's Smart template, which it uses to guide its review of 510(k) submissions, does not include a dedicated section on cybersecurity

At the time of our review, FDA's Smart template, which FDA reviewers use to guide their review of 510(k) submissions, prompted them to conduct

[27] The Refuse-To-Accept checklists for PMA and 510(k) submissions are included in the guidance documents *Acceptance and Filing Reviews for Premarket Approval Applications (PMAs)* and *Refuse to Accept Policy for 510(k)s*, respectively.

a cybersecurity review as part of their broader software review. The Smart template's software section referred FDA reviewers to the October 2014 premarket cybersecurity guidance. However, unlike the software section, which included specific software questions, the Smart template does not prompt FDA reviewers with specific cybersecurity questions that they should consider when reviewing submissions. Although a software review may cover some aspects of a cybersecurity review (e.g., review of the device's software update plan), FDA reviewers may not consider non-software aspects of a networked medical device, such as physically securing the device or limiting functionalities to authorized users.

The absence of a dedicated cybersecurity section in the Smart template may result in less consistent cybersecurity reviews of submissions for networked medical devices. In addition to FDA reviewers' using the Smart template as a guide, they also use it to organize and record the results of their review. Because the Smart template lacks a specific, dedicated section for recording such information, FDA reviewers noted the results of their cybersecurity reviews inconsistently under different elements. In some of the submissions that we reviewed, FDA reviewers had a stand-alone section or separate memo discussing cybersecurity while others discussed the results of their cybersecurity review as part of a software review. In a few submissions, however, it was unclear whether FDA reviewers noted the results of their cybersecurity review.

CONCLUSION AND RECOMMENDATIONS

Cybersecurity threats to networked medical devices are on the rise. Researchers and hackers have demonstrated that the lack of security controls in these devices makes them vulnerable to cybersecurity attacks, such as ransomware and unauthorized remote access. Such attacks can affect not only a single patient but can also impact a hospital system and disrupt the delivery of health care.

FDA has emphasized that addressing cybersecurity for networked medical devices is a responsibility shared among stakeholders, including the Agency, device manufacturers, and health care providers. As the Federal agency responsible for assuring the safety and effectiveness of networked medical devices, FDA has taken steps to address emerging cybersecurity concerns. It has established an internal cybersecurity workgroup, issued guidance documents on medical device cybersecurity, conducted outreach activities to educate stakeholders, and has begun to request and review cybersecurity information in premarket submissions for networked medical devices. However, FDA could do more to integrate its assessment of cybersecurity for networked medical devices into its premarket review process. From our observations, FDA is making limited use of key tools that could support consistency, efficiency, and effectiveness in its premarket review of cybersecurity.

Building upon the steps that it has already taken, FDA should further integrate the review of cybersecurity into its premarket review process in the following ways:

Promote the use of presubmission meetings to address cybersecurity-related questions

Greater use of the presubmission meetings could allow manufacturers of networked medical devices to ask FDA-specific cybersecurity-related questions that they need to address as they develop their device and prepare their submission for FDA review. FDA could promote the use of presubmission meetings when conducting outreach and awareness activities, such as presentations or workshops related to cybersecurity. In addition, the presubmission meeting could help improve the quality of cybersecurity information that manufacturers submit to FDA and decrease the amount of time it takes FDA to review a submission.

Include cybersecurity documentation as a criterion in FDA's Refuse-To-Accept checklists

FDA should include cybersecurity as one of the items in its Refuse-To-Accept checklists to ensure that manufacturers submit cybersecurity documentation before accepting a submission for review.

As a prerequisite of substantive review, if applicable, FDA could refuse to accept a submission until the manufacturer provides cybersecurity information needed to assess the networked medical device's cybersecurity risks and controls to mitigate those risks.

Include cybersecurity as an element in the Smart template

FDA should include cybersecurity as a stand-alone element in the Smart template to ensure consistent cybersecurity reviews. Inclusion of this element would assist FDA reviewers to thoroughly consider cybersecurity in their review and provide a specific, dedicated section where they can explain the results of their review.

AGENCY COMMENTS AND OIG RESPONSE

FDA concurred with all three of our recommendations and noted that it has begun taking steps to implement them.

See Appendix B for the full text of FDA's response.

APPENDIX A: Selection of Premarket Submissions

Sample Selection

We used FDA's public 510(k) and PMA databases to select a nonrepresentative sample of submissions. We limited the population to medical devices cleared through the 510(k) and De Novo[28] pathways between September 1, 2016, and October 30, 2016, and devices approved through the PMA pathway between January 1, 2016, and October 30, 2016. In fiscal year 2016, FDA received from manufacturers a total of 3,633 510(k) submissions, 54 De Novo requests, and 72 PMA submissions for review.[29] Because FDA does not separately track medical devices that have networked functionalities, we identified those that were capable of connecting wirelessly or wired to the Internet, a network, or other devices.

We selected 12 networked medical devices that FDA cleared via the 510(k) pathway; 1 device for which FDA granted a request for the device to be reviewed as "De Novo"; and 9 devices approved via the PMA pathway. We requested from FDA the submissions for each of these networked medical devices. We also collected documentation related to FDA's cybersecurity review for each networked medical device, such as reviewer notes, deficiency letters, meeting minutes, and email correspondence.

[28] For an explanation of "De Novo" requests, see footnote 11, page 3.

[29] FDA, *Quarterly Update on Medical Device Performance Goals, MDUFA III CDRH Performance Data, November 3, 2017*. Accessed at https://www.fda.gov/downloads/ForIndustry/UserFees/MedicalDeviceUserFee/UCM583882.pdf on June 20, 2018.

APPENDIX B: Full Text of FDA's Comments

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration
Silver Spring MD 20993

DATE: August 15, 2018

TO: Inspector General

FROM: Deputy Associate Commissioner for Public Health Strategy and Analysis

SUBJECT: FDA's General Comments to OIG Draft Report, "FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Medical Device Review Process" (OEI-09-16-00220)

FDA is providing the attached general comments to the OIG Draft Report, "FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Medical Device Review Process" (OEI-09-16-00220)

We appreciate the opportunity to review and comment on this draft report before it is published.

Lisa Rovin
Deputy Associate Commissioner for Public Health
Strategy and Analysis

Attachment

The Food and Drug Administration's General Comment to the OIG Draft Report, "FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Medical Device Review Process"

The Food and Drug Administration appreciates the opportunity to review and comment on the Office of the Inspector General's (OIG) draft report entitled, FDA Should Further Integrate Its Review of Cybersecurity into the Premarket Medical Device Review Process.

FDA welcomes the OIG report as a means for strengthening the agency's already robust premarket review of networked medical devices. FDA has already taken steps to implement these recommendations, and plans to update OIG as these items are completed.

OIG Recommendation: Promote the use of presubmission meetings to address cybersecurity-related questions

FDA response: FDA concurs that the pre-submission program can be used to address cybersecurity related questions. As noted in the report, pre-submission meetings were used extensively with implantable cardiac devices, and we continue to use these meetings to address device specific cybersecurity issues. While FDA believes that discussions on cybersecurity are already encompassed broadly in the presubmission program, and are already being used for this purpose in current practice, we intend to specifically mention cybersecurity in the next planned update of our presubmission guidance to further promote the use of presubmissions for cybersecurity questions.

OIG Recommendation: Include cybersecurity documentation as a criterion in FDA's Refuse-to-Accept checklists

FDA response: FDA concurs with the recommendation to include cybersecurity documentation as a criterion in the Refuse-To-Accept (RTA) checklist. The RTA checklist is an administrative tool and we believe that including cybersecurity as an item on the list could improve review efficiency by ensuring that the file contains all the necessary elements before the review is initiated rather than asking for such information, if not already in the premarket submission, during review. It is important to note that even while cybersecurity is absent from the current RTA checklist, FDA carefully reviews the material in the submission to support device cybersecurity and, where appropriate, requests additional information and/or clarifications during the review process. Therefore, incorporating cybersecurity on the RTA checklist (in and of itself) does not alter the scientific analysis of the submission which is grounded in a thorough assessment of all the material provided by the sponsor during premarket review to make a regulatory decision that is in the best interest of public health, nor will it impact marketing authorization decisions we make. As discussed in the OIG's report, cybersecurity information has been and will continue to be required in premarket submissions and FDA reviews such information as part of the review. FDA intends to update the RTA checklist and the accompanying guidance to specifically identify cybersecurity as an item in the checklist during the next update of these items.

The Food and Drug Administration's General Comment to the OIG Draft Report, "FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Medical Device Review Process"

OIG Recommendation: Include cybersecurity as an element in the Smart template

FDA response: FDA concurs with this recommendation. In fact, FDA independently initiated this step in the fall of 2016 by updating the Smart template to include a specific section on cybersecurity. This version of the smart template was implemented in September 2016. As the medical device ecosystem continues to mature around device cybersecurity, we anticipate that the Smart Template will be iteratively updated to keep pace with this evolution.

ACKNOWLEDGMENTS

Abby Amoroso served as the team leader for this study, and Ivy Ngo served as the lead analyst. Office of Evaluation and Inspections staff who provided support include Clarence Arnold, Christine Moritz, Michael Novello, and Melicia Seay.

This report was prepared under the direction of Blaine Collins, Regional Inspector General for Evaluation and Inspections in the San Francisco regional office, and Michael Henry, Deputy Regional Inspector General.

To obtain additional information concerning this report or to obtain copies, contact the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

ABOUT THE OFFICE OF INSPECTOR GENERAL

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.