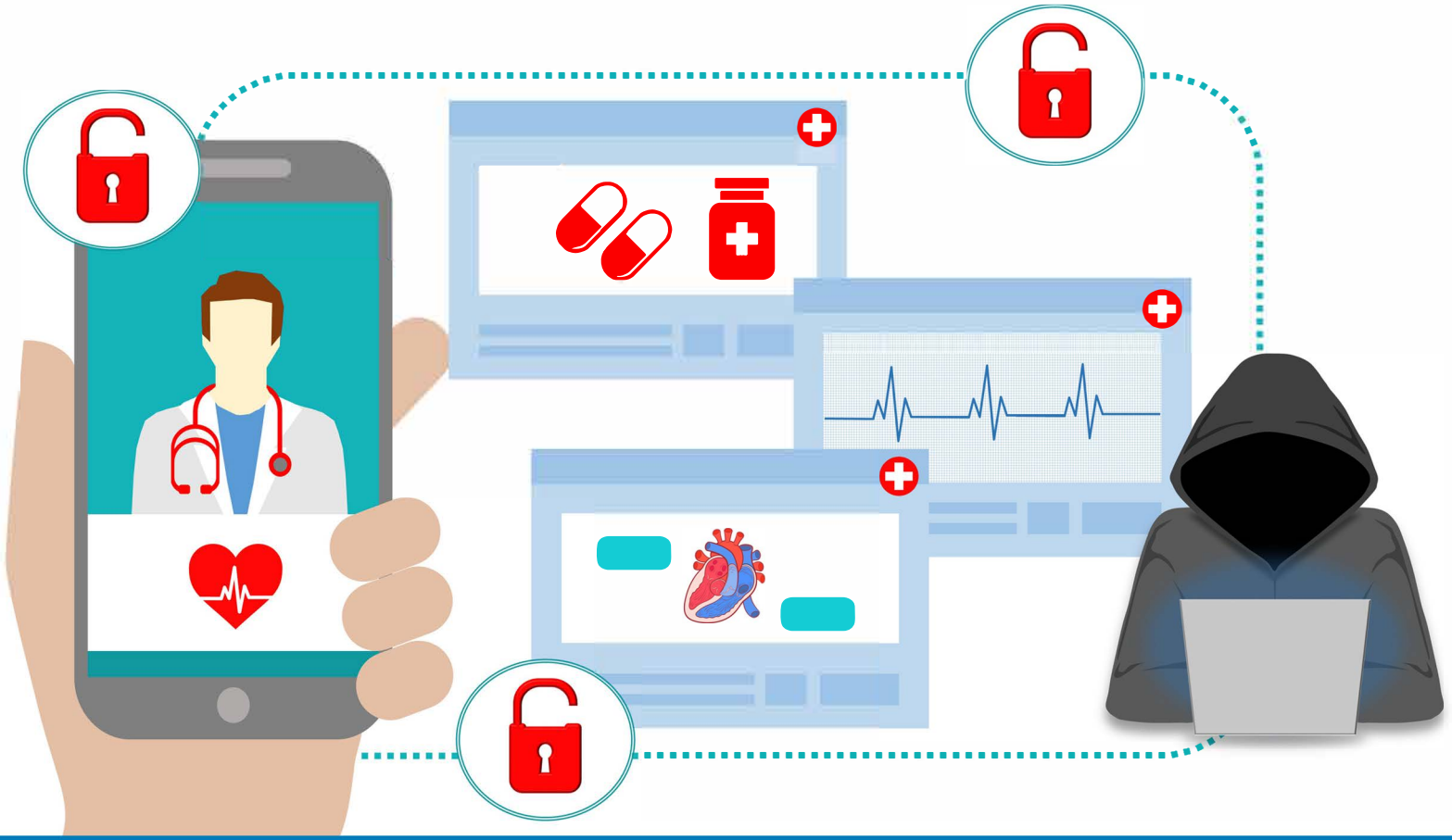
U.S. FOOD & DRUG ADMINISTRATION

Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities

June 2021



FDA.GOV

Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities

This discussion paper is for discussion purposes only and is not draft or final guidance. This document is not intended to communicate FDA's proposed (or final) regulatory expectations regarding the cybersecurity of serviced devices but is instead meant to seek early input from groups and individuals outside the Agency to inform future efforts related to this topic.

1 Introduction and Background

In FDA's Report on Device Servicing in May 2018,[1] FDA committed to strengthening cybersecurity practices associated with the servicing of medical devices. In the Report, FDA defines service to be the repair and/or preventive or routine maintenance of one or more parts in a finished device, after distribution, for purposes of returning it to the safety and performance specifications established by the original equipment manufacturer (OEM) and to meet its original intended use. Servicing excludes activities that significantly change the finished device's safety or performance specifications, or intended use.[2] This discussion paper furthers FDA's commitment by outlining specific cybersecurity challenges and opportunities associated with medical device servicing and seeking stakeholder feedback.

Cybersecurity is a widespread issue affecting medical devices connected to the Internet, networks, and other devices. Cybersecurity is the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.[3] FDA has taken numerous steps to strengthen medical device cybersecurity, including issuance of final guidances on FDA's premarket[4] and postmarket[5] medical device cybersecurity recommendations, which incorporate a "total product lifecycle (TPLC)" approach. These guidances communicated that effective cybersecurity is a shared stakeholder responsibility and that device manufacturers should incorporate the concept of threats, vulnerabilities, and exploits into their risk management, design controls, maintenance, surveillance, and response processes. A manufacturer's effective integration of cybersecurity controls into devices, such as through the inclusion of security controls for privileged access and improved data protection using encryption, may have important implications for the ability to perform effective servicing of a device.

Failure to maintain cybersecurity throughout the medical device's product life cycle can result in compromised functionality, loss of medical or personal data, inadequate data integrity, or the spreading of security threats to other connected devices or networks. These cybersecurity concerns have the

[1] "FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices," available at https://www.fda.gov/media/113431/download.

[2] For more information, see "Remanufacturing of Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff," available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/remanufacturing-medical-devices. When final, this guidance will represent FDA's current thinking on whether activities performed on devices are likely "remanufacturing."

[3] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0.

[4] Ibid.

[5] "Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

potential to result in patient harm such as illness, injury, or death as a result of delayed treatment or other impacts to medical device availability and functionality. Although it is not possible to completely eliminate all cybersecurity vulnerabilities from medical devices, manufacturers should implement a cybersecurity program that quickly identifies, assesses, and where appropriate, mitigates identified cybersecurity vulnerabilities and exploits. Entities that service medical devices are well positioned to help identify cyber exploits and vulnerabilities, and to participate in the continued deployment and maintenance of devices.

Cybersecurity is a shared responsibility among stakeholders, including OEMs, healthcare establishments,[6] healthcare providers, and independent service organizations (ISOs). FDA previously discussed cybersecurity and servicing of medical devices at public workshops[7, 8] and in published reports and white papers.[9, 10] The ability to service medical devices raises specific cybersecurity challenges related to the non-OEM entity's need, in many cases, for privileged access to perform diagnostic, maintenance, and repair functions. FDA expects[11] manufacturers to appropriately secure their devices in order to continue to assure the devices' safety and effectiveness, for example, by implementing adequate access controls to ensure only authorized privileged access to the device regardless of the entity performing servicing activities.[12] Importantly, FDA is not suggesting that devices be secured to prevent non-OEM servicing when such servicing is technically feasible and appropriate. Some manufacturers design their devices with the anticipation of non-OEM servicing and permit secure servicing by such entities, as needed and appropriate. Similar to these manufacturers, we recognize that non-OEM servicing entities play an important role in maintaining the quality, safety, and efficacy of medical devices without compromising cybersecurity.

FDA is releasing this discussion paper to discuss cybersecurity issues that are unique to the servicing of medical devices. The concepts presented in this discussion paper are intended to guide discussions among stakeholders about potential challenges and opportunities in cybersecurity and servicing. FDA is also seeking input on each of these topics and on the specific questions posed at the end of this discussion paper.

---

[6] Healthcare establishments are also referred to as healthcare delivery organizations (HDOs) in this discussion paper.

[7] 81 FR 11477. Details and information on the public workshop entitled "Refurbishing, Reconditioning, Rebuilding, Remarketing, Remanufacturing, and Servicing of Medical Devices Performed by Third-Party Entities and Original Equipment Manufacturers" are available at http://wayback.archive-it.org/7993/20171114130552/https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm511411.htm.

[8] Details and information on the public workshop entitled "Medical Device Servicing and Remanufacturing Activities" are available at https://www.fda.gov/medical-devices/workshops-conferences-medical-devices/public-workshop-medical-device-servicing-and-remanufacturing-activities-december-10-11-2018-12102018.

[9] "Evaluating Whether Activities are Servicing or Remanufacturing," available at https://www.fda.gov/media/117238/download.

[10] "FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices," available at https://www.fda.gov/media/113431/download.

[11] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0.

[12] See for more information "FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity; Dispelling Myths and Understanding Facts," available at https://www.fda.gov/media/123052/download in which FDA addresses common misconceptions that persist even with the availability of pre- and post-market guidances about medical device cybersecurity.

2 Scope

This discussion paper discusses the cybersecurity of medical devices serviced by non-OEMs. The scope of this discussion paper does not include activities that are remanufacturing.[13] This discussion paper applies to software enabled medical devices (including firmware) or programmable logic, software that is a medical device, and devices that are considered part of an interoperable system.

3 Cybersecurity Challenges and Opportunities for Medical Device Servicing - Changes involving software

Servicing of medical devices remains an important part of the medical device ecosystem. Ensuring high quality, safe, and effective cybersecurity practices when servicing medical devices is a critical aspect of strengthening the nation's cybersecurity infrastructure in the health care sector. The intersection of cybersecurity and medical device servicing presents unique challenges and opportunities. While device users and servicing entities can provide valuable feedback, help monitor and detect vulnerabilities, and timely implement authorized updates and patches throughout a medical device's life cycle, challenges exist when updating a device's software or patching a vulnerability. For example, there is a difficult and important balance between safety and practical use of the device so that safety measures are effective but do not inhibit or burden device operators from using the device efficiently or effectively. FDA has outlined a few additional challenges and opportunities below to help inform the discussion questions.

3.1 Privileged Access

Designing devices to limit access only to privileged device users ("privileged access") is a key component of ensuring a secure medical device. The servicing of medical devices by entities other than the OEM raises specific cybersecurity challenges related to the entity's need for privileged access to perform diagnostic, maintenance, and repair functions. Specifically, entities would need privileged access to the device to effectively perform servicing activities. The ability to grant certain entities privileged access can be designed into the device by the OEM.[14, 15]

To ensure adequate cybersecurity, FDA generally recommends that access to operating systems and applications be limited, and that user authentication and appropriate controls be in place.[16] Without privileged access, servicing activities may not be possible. However, devices that lack basic security may present significant safety concerns; therefore, it is important that stakeholders develop solutions to

[13] A remanufacturer means any person who processes, conditions, renovates, repackages, restores, or does any other act to a finished device that significantly changes the finished device's performance or safety specifications, or intended use. See 21 CFR 820.3(w). For additional information, see "Remanufacturing of Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff," available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/remanufacturing-medical-devices. When final, this guidance will represent FDA's current thinking on whether activities performed on devices are likely "remanufacturing."

[14] Privileged access is the right or a permission that is granted to access a device resource. Adapted from "NISTIR 7298: Glossary of Key Information Security Terms," available at https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. Authorization is the access privileges granted to a user, program, or process or the act of granting those privileges.

[15] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0 (explaining that a "Privileged User" is "a user who is authorized (and, therefore, trusted) to perform security relevant functions that ordinary users are not authorized to perform.").

[16] Ibid.

ensure medical devices are secure and mitigate unauthorized use without compromising the safe and effective servicing and use of medical devices.[17, 18]

3.2 Identification of Cybersecurity Vulnerabilities and Incidents

Detecting and responding to cybersecurity incidents remains a challenge for all critical infrastructure and not just the healthcare and public health sector. Servicing entities are well positioned to help identify cybersecurity vulnerabilities and exploits early, sometimes even before the OEM becomes aware. This postmarket data, if shared with stakeholders, including the OEM, FDA, Information Sharing and Analysis Organizations (ISAOs), and/or Department of Homeland Security (DHS), may be used to detect cyber vulnerabilities and exploits earlier, and develop responses and mitigations, where appropriate, to reduce cyber risk. The information can also be used to concentrate resources where they are needed most such that risks to public health are addressed in a continual and timely fashion.

3.3 Prevention and Mitigation of Cybersecurity Vulnerabilities

The response to identified cybersecurity vulnerabilities or exploits is often a software update or upgrade to address a virus, malware, or other cybersecurity vulnerability. Entities that service medical devices are well-positioned to ensure that devices have received the latest and most appropriate software updates to ensure adequate cybersecurity. In FDA's white paper "Evaluating Whether Activities are Servicing or Remanufacturing," the Agency sought comment on certain activities that FDA was considering proposing in draft guidance as servicing, including: implementing OEM provided or authorized cybersecurity updates and upgrades; and assessing for viruses, malware, and other cybersecurity related issues. Implementing validated software in a timely manner is critical to mitigating cybersecurity risk. Currently, servicing entities play a significant role in effectively and efficiently deploying this software; therefore, OEMs may help facilitate more robust cybersecurity by enabling servicing entities to assist in maintaining device security.

The Quality System Regulation (QSR) requires device manufacturers to establish and maintain procedures for verification and validation of design changes where appropriate, including software changes to address cybersecurity vulnerabilities, such as cybersecurity updates and patches.[19] However, high risk situations may necessitate timely action, which can be a challenge to develop and implement in an appropriate time frame to reduce cybersecurity risks to an acceptable level.[20] We encourage all interested stakeholders to collaborate on methods or pathways that could be used to efficiently develop, validate, and implement software changes for medical devices.[21] All stakeholders can contribute, ensure the software is correctly implemented, and that the device works as intended.

3.4 Product Life Cycle Challenges and Opportunities

FDA understands that the continued availability of "legacy devices" plays an important role, particularly

---

[17] Ibid.

[18] "Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

[19] See, e.g., 21 CFR 820.30(i).

[20] "FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity; Dispelling Myths and Understanding Facts," available at https://www.fda.gov/media/123052/download.

[21] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff," available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0.

in rural and underserved communities.[22] While OEMs have regulatory obligations regarding safety issues beyond security supportability, the individual components, such as operating systems and other third-party software components, may no longer be supported in advance of the healthcare establishment procurement cycles – or there may be financial reasons why a healthcare establishment elects to continue the use of a device past its end of life. In some cases, OEMs may be unable to provide updates to reduce an identified security risk after a component manufacturer ends their support. At some point, OEMs may decide that they no longer can support the device and inform customers of the device's end of support or end of life. Simultaneously, the device may remain clinically useful, meet its original performance and safety specifications, and intended use. However, unpatched devices will become increasingly vulnerable to cyber-attack. Accordingly, the international cybersecurity community has encouraged OEMs to declare, communicate, and work with users to notify of impending end of support or end of device-life decisions.[23] Even so, decisions for OEMs to end device support are multi-factorial and timing is difficult to predict, limiting the lead time for adequate transition planning. One possible mitigation OEMs and healthcare establishments could implement is responsibility agreements.[24] Servicing entities may be able to keep a product within acceptable performance specifications, but unable to address the increasing cyber risks associated with unsupported devices. It remains critical for healthcare entities to understand the cybersecurity risks they are taking and for the device health care system to develop strategies to assess and address security risks of devices located within these communities.

4 Discussion Questions

Effective cybersecurity practices are essential for the continued safety and effectiveness of medical devices, particularly with the increasing use of wireless, internet-, and network-connected devices. High quality servicing, whether performed by OEMs or non-OEM entities, ensures robust cybersecurity throughout the device's total product life cycle. Addressing the challenges and taking advantage of the opportunities associated with cybersecurity and the servicing of medical devices can help maximize the benefits and minimize the risks for patients, and help address many obstacles in the device's life cycle.

FDA would like to receive comments on the issues raised in this document. In addition, stakeholders are invited to address the following questions:

1. What are the cybersecurity challenges and opportunities associated with the servicing of medical devices?
2. Are the four areas identified in this discussion paper (privileged access, identification of cybersecurity vulnerabilities and incidents, prevention and mitigation of cybersecurity vulnerabilities, and product lifecycle challenges and opportunities) the correct cybersecurity priority issues to address in the servicing of medical devices? If not, which areas should be the focus?
3. How can entities that service medical devices contribute to strengthening the cybersecurity of medical devices?

[22] For the purposes of this document, legacy devices are those that cannot be reasonably protected against currently cybersecurity threats. For more information, see "Principles and Practices for Medical Device Cybersecurity" by the International Medical Device Regulators Forum (IMDRF), available at http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf.

[23] Ibid.

[24] ANSI/AAMI/IEC 80001-1:2010, "Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities," available at https://www.iso.org/standard/44863.html.