VIEWPOINT

Cybersecurity Concerns and Medical Devices
Lessons From a Pacemaker Advisory

Daniel B. Kramer, MD, MPH
Harvard Medical School, Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology, Beth Israel Deaconess Medical Center, Boston, Massachusetts.

Kevin Fu, PhD
College of Engineering, University of Michigan, Ann Arbor.

Medical devices increasingly include capabilities for wireless communication and remote monitoring systems that relay clinical information from patients to clinicians. For example, many cardiac implantable electrical devices can transmit data regarding arrhythmia burden and heart failure metrics with minimal patient effort. This technology can improve patient care, but also introduces possible risks to data security and patient safety.

In August 2017, the US Food and Drug Administration (FDA) issued a safety communication regarding potential cybersecurity concerns involving malicious interference with battery life or essential programming functions in several pacemaker models made by St Jude Medical (which was acquired by Abbott in January 2017).[1] (Cybersecurity refers to the prevention of unauthorized access, modification, or use of information stored or transmitted by medical devices or networks.) An estimated 450 000 or more patients with these permanently implanted, life-sustaining devices may be affected. As software and remote monitoring become embedded in more medical devices, such as diabetes management systems and sleep apnea devices, cybersecurity concerns will inevitably increase the risk of advisories affecting a wider scope of patients. Therefore, it is important to consider the ways in which patients and clinicians might prepare for such events, and the optimal ways for manufacturers and the FDA to engage the public around this emerging area of postmarketing surveillance.

Cybersecurity Concerns in Pacemakers

In 2016, reports arose suggesting that Abbott pacemakers and implantable cardioverter-defibrillators may have particular vulnerabilities related to their use of radiofrequency telemetry for wireless communication.[2] These devices wirelessly transmit patient data to "base stations" in patients' homes and are connected by telephone or the internet to web-based portals managed by the manufacturers, which in turn provide information to clinicians. Potential risks identified included the possibility that adversarial parties could intentionally drain the battery of affected devices, or use the home base station in such a way as to issue malicious programming commands to patients' implanted systems.

Although no reports of actual patient harm have been identified, the FDA described these vulnerabilities in a safety communication in January 2017 at the same time it announced that a downloadable software patch would be applied automatically to patients' home monitors.[3] Thus, the correction occurred largely without patient engagement, as long as the base station was plugged in and connected. To further enhance the security of implanted devices, a firmware upgrade was developed by Abbott and approved by the FDA in August 2017, and included in all new device implants from that date forward. (Unlike a general purpose operating system like Windows, firmware is a special kind of software that provides a highly specific capability on devices distinct from typical home computing systems.) This upgrade included added layers of security for protecting against radiofrequency telemetry attacks, and defenses against the use of the base station to send commands to the implanted devices.

In general, the FDA issues safety alerts to inform the public of a risk of substantial harm from a medical device in commercial use. By contrast, recalls are issued when the corrective action taken by the manufacturer targets a problem with a reasonable likelihood of causing harm. This correction was described as a recall in the safety communication issued by the FDA[1] and in popular media reports,[4] but not in the "Dear Doctor" letter from Abbott,[5] and the corrective action is not currently listed in the FDA recalls database.

Clinicians are responsible for identifying patients with affected devices and contacting them. Patients who currently have affected devices need to have the firmware upgrade in person. The upgrade process is noninvasive, similar to a routine device interrogation that might be performed in a clinic, but with several key distinctions. During the several minutes of reprogramming, all devices revert to ventricular demand pacing, which may cause temporary symptoms in some patients. In addition, there is an estimated small rate of unpredictable device reset or failure during such an upgrade, which could lead to serious consequences, including death. As such, both the FDA and Abbott recommend that patients who are dependent on their pacemakers have this upgrade performed in a "facility where temporary pacing and pacemaker generator [replacement] can be readily provided."[1] Although such events are estimated to be rare (0.003%),[5] the prevalence of such pacemakers in US populations means that hundreds of patients could potentially encounter this risk.

The FDA's safety communication acknowledged the general theoretical risks associated with wireless technology and provided links to resources, including its own adverse event reporting system and a guidance document for postmarketing management of cybersecurity.[6] But it did not specify whether devices from other manufacturers were likely affected by this same set of vulnerabilities. In addition, the upgrade request appears to clinicians using Abbott clinical programmers (essentially modified laptop computers that are used for in-person communication, interrogation, and programming of pacemakers) as an "alert," indicating that the "device cybersecurity upgrade is available," with the upgrade initiated by selecting 1 button. Because interrogations are commonly performed in ambulatory clinics or other sites without access to emergency

Corresponding Author: Daniel B. Kramer, MD, MPH, Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology, 375 Longwood Ave, Ste 440, Boston, MA 02215 (dkramer@bidmc.harvard.edu).

pacing, it is possible that many clinicians may initiate the upgrade in such settings without recognizing the potential risks.

Practical Considerations

This first widespread cybersecurity advisory involving a permanent medical device implant provides some insight into the ways in which the public experience with these types of medical device malfunctions might be improved. Communications regarding widely used products for which multiple vendors exist in the marketplace should serve as opportunities to highlight current FDA and industry standards, and the degree to which similar products made by other manufacturers may be subject to similar concerns. For devices such as pacemakers, it could have been anticipated that popular media reports of a "pacemaker recall" would capture the attention of many patients living with unaffected devices (including pacemakers made by other companies), who would wonder if their own device would be vulnerable to the same problem. Although it is not widely known if the vulnerabilities described for Abbott devices currently affect models from other manufacturers, prior research suggests that theoretically this may be the case, unless similar cybersecurity defenses have been incorporated into these implanted devices and base stations.[7] Thus, given the novelty of this event, the FDA might have leveraged the safety communication to specifically identify whether there is an industry-wide concern, and to clarify current security standards established by regulators for new device approval. This guidance might also proactively reassure the millions of patients who have pacemakers that are not subject to the advisory, a model for communication that may serve the public well going forward.

Another opportunity for improvement might include a partnership between the FDA and industry to formally pilot the corrective action to acquire clinical data and user feedback, and to allow for ongoing quantification of the actual adverse event rate from implementing the solution in particular. Importantly, the adverse event rate highlighted by Abbott is extrapolated from other circumstances, and the true rate of malfunction may not be known until tens of thousands of devices are already upgraded. Alternatively, a focused, publicly disclosed pilot initiative might have provided critical feedback regarding the process that could have been collected in a structured way as part of a required postmarketing surveillance study mandated by the FDA. In this specific case, even preliminary feedback from clinical sites might rapidly identify an important set of concerns regarding the logistics of providing the firmware upgrade in settings capable of providing emergency backup pacing, perhaps leading to revision (for example) of the user interface to avoid inadvertent initiation of the upgrade in an unsafe setting. With the current approach, in which all clinical sites received the firmware upgrade on clinic programmers essentially simultaneously, adverse events related to the firmware upgrade will be subject to the known unreliability and underreporting of passive adverse event collection.[8]

The Abbott cybersecurity vulnerability should make clear to patients and clinicians that technological progress in implantable medical devices will necessarily involve important challenges, including risks that may not be easily quantified in the manner of more typical clinical concerns. Heightened sophistication in devices, including embedded sensors and flexible transmission of patient data through remote monitoring, has always been balanced against considerations such as cost and battery life. However, remote connectivity, even as it is endorsed as the standard of care for many conditions, invokes a different set of risks that may be difficult to characterize. Risks to patients involving compromise of their protected health information and the possibility of malicious interference with device function are by their nature obscure.

To its credit, the FDA has collaborated with cybersecurity experts across government agencies, academia, and industry over the past several years to help identify and characterize cybersecurity threats and provide guidance for premarketing and postmarketing actions. However, the experience with this pacemaker advisory should serve as a reminder to the broader clinical community that an entirely new class of potential medical device malfunction is likely to become increasingly common. Patients and clinicians need to appreciate these risks alongside the convenience and diagnostic and therapeutic potential of remotely connected devices.

ARTICLE INFORMATION

Published Online: October 18, 2017. doi:10.1001/jama.2017.15692

Conflict of Interest Disclosures: Both authors have completed and submitted the ICMJE Form for Disclosure of Potential Conflicts of Interest. Dr Kramer reported being supported by the Greenwall Faculty Scholars Program in Bioethics; and serving as a consultant to the Circulatory Systems Advisory Panel of the Food and Drug Administration and the Baim Institute for Clinical Research for clinical trials of medical devices (unrelated to current topic). Dr Fu reported being the director of the Archimedes Center for Medical Device Security at the University of Michigan, which is supported by industry; being co-founder of Virta Laboratories Inc; and being supported by National Science Foundation grant CNS-1330142.

Disclaimer: The views and conclusions contained in this article are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the National Science Foundation.

Additional Contributions: We thank Aaron S. Kesselheim, MD, JD, MPH (Department of Medicine, Brigham and Women's Hospital, and Harvard Medical School, Boston, Massachusetts), for comments on an earlier draft.

REFERENCES

1. US Food and Drug Administration. Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St Jude Medical's) implantable cardiac pacemakers. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm. Accessed September 5, 2017.

2. Ransford B, Kramer DB, Foo Kune D, et al. Cybersecurity and medical devices. *Pacing Clin Electrophysiol*. 2017;40(8):913-917.

3. US Food and Drug Administration. Cybersecurity vulnerabilities identified in St Jude Medical's implantable cardiac devices and Merlin@home transmitter. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. Accessed September 5, 2017.

4. Morris C. 465 000 pacemakers recalled on hacking fears. http://fortune.com/2017/08/31/pacemaker-recall-fda/. Accessed September 14, 2017.

5. Abbott. Important cybersecurity advisory information about cybersecurity firmware update for Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI devices. https://www.sjm.com/en/professionals/resources-and-reimbursement/technical-resources/product-advisories-archive. Accessed September 5, 2017.

6. US Food and Drug Administration. Postmarket management of cybersecurity in medical devices. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. Accessed September 12, 2017.

7. Halperin D, Heydt-Benjamin TS, Ransford B, et al. Pacemakers and implantable cardioverter-defibrillators. https://www.secure-medicine.org/icd-study/icd-study.pdf. Accessed September 14, 2017.

8. Kramer DB, Yeh RW. Practical improvements for medical device evaluation. *JAMA*. 2017;318(4):332-334.