AMA Journal of Ethics®
September 2021, Volume 23, Number 9: E705-711

STATE OF THE ART AND SCIENCE: PEER-REVIEWED ARTICLE

# What Should Cardiac Patients Know About Device Cybersecurity Prior to Implantation?

Emily P. Zeitler, MD, MHS and Daniel B. Kramer, MD, MPH

**Abstract**

Cardiac implantable electronic device (CIED) procedures require informed consent and, ideally, shared decision making to guide patients through their experiences as CIED recipients. The information that different patients need or want about cybersecurity risk varies. This article considers device cybersecurity risks in light of federal guidelines and suggests strategies for communicating these risks clearly during informed consent conversations and follow-up.

## Introduction

Cardiac implantable electronic devices (CIEDs) reduce morbidity and mortality across a wide spectrum of cardiovascular conditions.[1] Devices such as permanent pacemakers, implantable cardioverter-defibrillators, and pulmonary artery pressure monitors for patients with heart failure store patient data and transmit it wirelessly to clinicians. Clinicians who implant these devices have legal and ethical obligations to obtain informed consent after outlining risks and benefits of surgical implantation to patients,[2] and they face policy mandates to engage in formal shared decision making with patients to align device-based therapy with patients' goals.[3] Regulators charged with premarket evaluation of these devices and their postmarket surveillance, particularly the US Food and Drug Administration (FDA), communicate established risks through approved labeling when marketing authority is granted. Emerging safety concerns are addressed through tailored communications, advisories, or recalls.

While computing and data transmission functions of CIEDs necessarily entail selected cybersecurity risks,[4,5] it remains unclear whether and in what way regulators ought to include this risk in initial and ongoing communications with clinicians and patients. Broad disclosure of all potential risks may needlessly worry patients and crowd out other information during time-pressured clinician encounters. Accordingly, there is genuine debate about whether patients need this information at all and, if so, at what level of detail.[6,7] This approach would seem to align with the recognition that manufacturers communicate postmarket risks directly to clinicians but generally only indirectly to patients.[8] Yet leaving disclosure decisions to clinicians alone likely stretches most physicians' expertise on technical cybersecurity details. Overly narrow communication about risks might be too paternalistic and fail to appropriately inform patients about essential aspects of their own treatment.

This article briefly characterizes current cybersecurity risks associated with CIED use and reviews recent FDA guidance on communicating cybersecurity vulnerabilities to patients. We then provide an ethical analysis of this FDA communication framework and suggest potential revisions that might help balance competing values and interests.

## Potential Cybersecurity Risks of CIEDs

Unlike risks associated with implantation or longitudinal performance of CIEDs, cybersecurity concerns might seem abstract and difficult to quantify. The risks most familiar to both patients and clinicians are those related to privacy.[2] Data stored and transmitted by CIEDs monitor device function (eg, battery life, wire integrity) and patient status, such as detection of arrhythmias or changes in underlying disease in the case of heart failure. Data transmissions typically occur wirelessly through signals sent (either through radiofrequency telemetry or Bluetooth) from an implanted device to either a home monitor or a patient's smartphone, which then relays data to device manufacturers for storage on large servers. Data are then shared with clinical sites for monitoring of clinical and device status. Remote monitoring has been demonstrated to improve patient outcomes and health care utilization.[9,10,11]

Much like other forms of patient data, patient information stored in these devices and transmitted wirelessly is encrypted and subject to privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA).[2] Currently, data that are stored and transmitted by CIEDs are shared only with treating physicians and other health care professionals, patients, regulatory bodies, payers, and researchers in accordance with HIPAA regulations. Preimplantation counseling rarely, if ever, includes a discussion of risks related to privacy,[12] and limited data suggest that patients who consider these risks at all view them as acceptable in light of the clinical benefits of receiving a device for their specific condition.[13]

In addition to privacy concerns, which are not unique to CIEDs, implanted devices are at risk for direct interference with device function through malicious intrusion. Although, to the best of our knowledge, cases of actual patient harm have never been reported, it is theoretically possible to disrupt device function (eg, pacing therapy) through introduction of malware or direct interference that leverages the wireless communication through which devices are programmed clinically.[14] This possibility was brought to wide public attention when former Vice President Dick Cheney, who had an implantable cardioverter-defibrillator during his time in office, noted in a *60 Minutes* interview in 2013 that the wireless telemetry on his device was deactivated, at his request, to reduce the possibility of malicious interference.[15] The same idea of hacking a CIED was dramatized in the TV show *Homeland* in 2012,[16] although the methods employed were not realistic.

Creative license notwithstanding, these types of cybersecurity concerns have potential for clinical impact and present clinicians with the dilemma of informing patients without creating panic or confusion. For example, in 2016, there were early reports of a possible cybersecurity threat related to remote monitoring of a particular manufacturer's pacemakers, but FDA communication on this issue was withheld until a software patch was available from the manufacturer, which downloaded automatically without patient engagement.[5] Improving regulatory and clinical management of these circumstances is the primary motivation for recent, admirable engagement among the FDA, professional societies, and patient groups.

## FDA Guidance

The FDA's public health mandate to provide reasonable assurance of safety and effectiveness for medical devices now includes evaluation of the cybersecurity features of implanted devices and strategies for communicating potential concerns. Accordingly, FDA guidance clarifies key definitions related to cybersecurity risks. *Vulnerabilities* refer to potential weaknesses within medical devices or systems that could potentially cause patient harm or impact safety or performance of connected devices or systems. *Threats* are events or circumstances with the potential to leverage vulnerabilities. *Exploits* are instances in which vulnerabilities are actually utilized, whether intentionally or accidentally, thereby compromising safety or performance. For example, in recent years there have been multiple advisories pertaining to identified cybersecurity vulnerabilities affecting various device manufacturer platforms, although actual exploits have not been reported.[17]

The FDA plays a central role in evaluating CIEDs for potential cybersecurity concerns not only through premarket evaluation but also through postmarket assessments and regulatory action.[18] The real-life and theoretical risks of cybersecurity have led the FDA to issue guidance for CIED manufacturers on how to address cybersecurity issues when developing new devices[19] and on postmarket cybersecurity activities, including controls or safeguards and monitoring vulnerabilities and controls' effectiveness.[20] FDA guidance provides transparency in regulatory decision making while setting standards for risk mitigation. Guidance documents are not legally binding but provide clarity to manufacturers and the public regarding current FDA thinking on specific regulatory topics.[21] The FDA joins a chorus of other stakeholders who recognize the importance of cybersecurity vigilance for patient protection.[22] Indeed, the FDA partners with other cybersecurity experts, including other federal agencies, academic groups, and nongovernment "white hat hackers" who proactively help to identify medical device vulnerabilities.[23]

As part of this effort, the FDA has also sought to understand how best to communicate cybersecurity concerns to patients. Early results of these efforts indicate that patients prefer to be given control over how much information they receive related to cybersecurity vulnerabilities and that they wish to be informed as soon as the threat is identified, regardless of whether risk reduction measures are available.[8,24] In October 2020, the FDA sought comments on a discussion paper written by the Patient Engagement Advisory Committee titled "Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework," which provided preliminary recommendations for best practices for presenting these unique risks to clinicians and patients.[25]

## Clear Disclosure Avoids Panic

The FDA's working framework on communicating cybersecurity risks to clinicians and patients implicitly draws on key ethical principles in coordinating responses to cybersecurity concerns. First, the framework admirably attempts to balance beneficence and nonmaleficence. A running theme is the need for the FDA and industry to inform clinicians and patients and to provide clear, accessible guidance on necessary steps for avoiding harm (for example, by communicating as clearly as possible whether patients have a specific action item, such as downloading a security patch).[25] Making the magnitude and likelihood of potential harm transparent is also emphasized, as the risk of vulnerabilities being exploited—at least for insulin pumps—is considered to be extremely small and outweighed by the benefits of the devices themselves.[26] Accurately

conveying the rarity of potential harms weighed against the much larger and more concrete clinical benefits might help patients avoid choosing to forgo devices that, on balance, substantially promote their well-being. Second, the FDA framework admirably addresses information transfer or access inequity by noting the need for translations, printed materials targeting modest levels of education, and multiple formats.[25]

Despite these strengths, several specific aspects of communicating cybersecurity risks merit further consideration by the FDA and others. First, our practical experience with previous advisories suggests that most patients will only hear "pacemaker" or "implantable defibrillator" and tend not to absorb the details even of the brand of device affected, let alone a model name and number. Just as patients might not know their own device details, so health care proxies might not have that information readily accessible to them.

Second, even if the FDA's own communications clearly identify the affected systems—and whether the cybersecurity risk applies to more than one class of device or vendor—clinics can still expect a large volume of inquiries from patients about whether their device is affected. The FDA can support clinics in answering patient queries through at least 2 different mechanisms. One would be to accelerate requirements for documenting the unique device identifier (UDI)—details about a specific device embedded in the device itself, such as type, model, and manufacturing lot—in patient records. This regulatory requirement for implantable devices has experienced delays in implementation, but the need to rapidly identify specific patient exposures to cybersecurity threats provides a motive for fully documenting UDIs. Another way for the FDA to support ambulatory clinics' response to patient inquiries would be to use its platform and partnerships with professional societies to emphasize the importance of such clinics maintaining a structured database of all of their implanted CIEDs and following patients longitudinally. There are several third-party vendors who supply these systems,[27] which allow for rapid searches and identification of patients according to device type, serial number, and other parameters. Such systems are expensive, however, and might not be universally employed.

Third, the FDA's framework points to an opportunity for clinicians, at the time of implantation, to be much more proactive in providing patients with their own device-specific information and emphasizing why it is critical to keep these data accessible. Doing so is within the scope of physicians' traditional role in obtaining consent and advising patients of ongoing risks.

Finally, the FDA and professional societies can partner in engaging patients in remote monitoring and regular clinic follow-up by stressing that these activities promote cybersecurity protection. Presenting recommended follow-up and the use of remote monitoring as a strategy for forestalling cybersecurity concerns might motivate patients to undertake clinical care that might otherwise seem to be of low value.[28]

## Conclusion

With the overarching charge of protecting public health, medical device cybersecurity is part of the broader regulatory effort to balance making innovative devices available and ensuring their safe use. These pressures can be in conflict when limited data exist on a new device or device feature with significant promise of improving public health. Although patients have not traditionally been directly involved in regulatory decisions, they presume that medical device regulation prioritizes assurance of safety over other

factors.[13] Continuing to engage patients in tailoring the FDA's approach to cybersecurity might help balance competing values underlying risk disclosure.

## References


1. Epstein AE, DiMarco JP, Ellenbogen KA, et al; Heart Rhythm Society. 2012 ACCF/AHA/HRS focused update incorporated into the ACCF/AHA/HRS 2008 guidelines for device-based therapy of cardiac rhythm abnormalities: a report of the American College of Cardiology Foundation/American Heart Association Task Force on Practice Guidelines and the Heart Rhythm Society. *J Am Coll Cardiol*. 2013;61(3):e6-e75.
2. Cohen IG, Gerke S, Kramer DB. Ethical and legal implications of remote monitoring of medical devices. *Milbank Q*. 2020;98(4):1257-1289.
3. Merchant FM, Dickert NW Jr, Howard DH. Mandatory shared decision making by the Centers for Medicare & Medicaid Services for cardiovascular procedures and other tests. *JAMA*. 2018;320(7):641-642.
4. Ransford B, Kramer DB, Foo Kune D, et al. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. *Pacing Clin Electrophysiol*. 2017;40(8):913-917.
5. Kramer DB, Fu K. Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. *JAMA*. 2017;318(21):2077-2078.
6. Baranchuk A, Refaat MM, Patton KK, et al; American College of Cardiology's Electrophysiology Section Leadership. Cybersecurity for cardiac implantable electronic devices: what should you know? *J Am Coll Cardiol*. 2018;71(11):1284-1288.
7. Slotwiner DJ, Deering TF, Fu K, Russo AM, Walsh MN, Van Hare GF. Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians—proceedings of the Heart Rhythm Society's Leadership Summit. *Heart Rhythm*. 2018;15(7):e61-e67.
8. Maisel WH, Paulsen JE, Hazelett MB, Selzman KA. Striking the right balance when addressing cybersecurity vulnerabilities. *Heart Rhythm*. 2018;15(7):e69-e70.
9. Slotwiner D, Varma N, Akar JG, et al. HRS expert consensus statement on remote interrogation and monitoring for cardiovascular implantable electronic devices. *Heart Rhythm*. 2015;12(7):e69-e100.
10. Varma N, Epstein AE, Irimpen A, Schweikert R, Love C; TRUST Investigators. Efficacy and safety of automatic remote monitoring for implantable cardioverter-defibrillator follow-up: the Lumos-T Safely Reduces Routine Office Device Follow-up (TRUST) trial. *Circulation*. 2010;122(4):325-332.
11. Cronin EM, Ching EA, Varma N, Martin DO, Wilkoff BL, Lindsay BD. Remote monitoring of cardiovascular devices: a time and activity analysis. *Heart Rhythm*. 2012;9(12):1947-1951.
12. Nielsen JC, Kautzner J, Casado-Arroyo R, et al. Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles—ESC Regulatory Affairs Committee/EHRA Joint Task Force report. *Europace*. 2020;22(11):1742-1758.
13. Zeitler EP, Al-Khatib SM, Yapejian R, Tripp CC, Sears SF. Regulation without representation: cardiac device patient knowledge and attitudes about the FDA regulatory process. *Circ Arrhythm Electrophysiol*. 2020;13(8):e008561.
14. National Audit Office. Investigation: WannaCry cyber attack and the NHS. October 24, 2017. Accessed July 22, 2021. https://www.nao.org.uk/wp-

content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
15. Ford D. Cheney's defibrillator was modified to prevent hacking. *CNN*. October 24, 2013. Accessed November 10, 2020. https://www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html.
16. Newmarker C. Hacking pacemakers is good TV, but is it for real? *Medical Design & Outsourcing*. February 27, 2018. Accessed April 26, 2021. https://www.medicaldesignandoutsourcing.com/hacking-pacemakers-good-tv-real/#:~:text=The%20idea%20that%20hackers%20might,president's%20pacemaker%20and%20killed%20him
17. Cybersecurity. US Food and Drug Administration. June 7, 2021. Accessed October 15, 2020. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#guidance
18. Paulsen JE, Hazelett MB, Schwartz SB. CIED cybersecurity risks in an increasingly connected world. *Circulation*. 2018;138(12):1181-1183.
19. US Food and Drug Administration. Content of premarket submissions for management of cybersecurity in medical devices: draft guidance for industry and Food and Drug Administration staff. October 18, 2018. Accessed July 22, 2021. https://www.fda.gov/media/119933/download
20. US Food and Drug Administration. Postmarket management of cybersecurity in medical devices: guidance for industry and Food and Drug Administration staff. December 28, 2016. https://www.fda.gov/media/95862/download
21. Weitzman RE, Stern AD, Kramer DB. Food and Drug Administration guidance documents and new medical devices: the case of breast prostheses. *Am J Ther*. 2021;28(1):e127-e130.
22. Das S, Siroky GP, Lee S, Mehta D, Suri R. Cybersecurity: the need for data and patient safety with cardiac implantable electronic devices. *Heart Rhythm*. 2021;18(3):473-481.
23. Marks J. *The Cybersecurity 202*: hackers are going after medical devices—and manufacturers are helping them. *Washington Post*. August 8, 2019. Accessed July 22, 2021. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/08/08/the-cybersecurity-202-hackers-are-going-after-medical-devices-and-manufacturers-are-helping-them/5d4b556088e0fa4cc4c23465/
24. US Food and Drug Administration. Summary of the Patient Engagement Advisory Committee. September 10, 2019. Accessed November 10, 2020. https://www.fda.gov/media/130778/download
25. Patient Engagement Advisory Committee. Communicating cybersecurity vulnerabilities to patients: considerations for a framework. Discussion paper and request for feedback. US Food and Drug Administration. October 2020. Accessed November 10, 2020. https://www.fda.gov/media/143000/download
26. Patient Engagement Advisory Committee, Center for Devices and Radiological Health. Cybersecurity and medical devices: communication that empowers patients. Transcript. US Food and Drug Administration; September 10, 2019. Accessed April 26, 2021. https://www.fda.gov/media/131688/download
27. Diamond J, Varma N, Kramer DB. Making the most of cardiac device remote management: towards an actionable care model. *Circ Arrhythm Electrophysiol*. 2021;14(3):e009497.
28. Saxon LA, Varma N, Epstein LM, Ganz LI, Epstein AE. Rates of adoption and outcomes after firmware updates for Food and Drug Administration

cybersecurity safety advisories. *Circ Arrhythm Electrophysiol*. 2020;13(8):e008364.

**Emily P. Zeitler, MD, MHS** is a cardiac electrophysiologist at the Dartmouth-Hitchcock Medical Center in Lebanon, New Hampshire, where she is also an assistant professor of medicine at the Geisel School of Medicine and the Dartmouth Institute. Dr Zeitler's research focuses on regulatory science and clinical outcomes associated with cardiovascular therapeutics.

**Daniel B. Kramer, MD, MPH** is a cardiac electrophysiologist and the director of the Pacemaker and ICD Clinic at Beth Israel Deaconess Medical Center in Boston, Massachusetts, where he is section head of electrophysiology and digital health at the Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology. He has faculty affiliations at the Harvard Medical School Center for Bioethics; the Program on Regulation, Therapeutics, and Law at Brigham and Women's Hospital; and the Hinda and Arthur Marcus Institute for Aging Research. His research focuses on outcomes, policy, and ethics questions arising from the use of medical devices.

Citation
*AMA J Ethics*. 2021;23(9):E705-711.

DOI
10.1001/amajethics.2021.705.

Conflict of Interest Disclosure
Dr Kramer reports receiving support from the Greenwall Foundation and payment for consultation from the Circulatory Systems Advisory Panel of the Food and Drug Administration (FDA) and Firefly Health. Dr Zeitler reports receiving payment for consultation from the FDA's Circulatory Systems Advisory Panel, Sanofi-Aventis, and Medtronic, Inc.

*The viewpoints expressed in this article are those of the author(s) and do not necessarily reflect the views and policies of the AMA.*


ISSN 2376-6980