EDITORIAL COMMENTARY

Striking the right balance when addressing cybersecurity vulnerabilities

William H. Maisel, MD, MPH, Jessica E. Paulsen, BE, Matthew B. Hazelett, BS, Kimberly A. Selzman, MD, MPH, FHRS

From the U.S. Food and Drug Administration, Silver Spring, Maryland.

Medical devices, including cardiac implantable electronic devices (CIEDs), have become increasingly interconnected, leading to an increased risk of exploitation of cybersecurity vulnerabilities that can affect device functionality. Device interconnectivity and interoperability can provide great benefits to patients, as evidenced by the growing body of literature demonstrating the positive effect of remote monitoring of CIEDs.[1] Unfortunately, these benefits are accompanied by the potential for cybersecurity risks—and these are not just theoretical risks. Medical devices have been infected and disabled by malware, and recent cyberattacks, such as the WannaCry ransomware attack last year that affected hospital networks around the world, demonstrate the disruptive potential of unmitigated cybersecurity vulnerabilities. The world has changed, and we need to proactively work together to strengthen medical device cybersecurity and protect patient safety.

The Cybersecurity Leadership Summit convened by the Heart Rhythm Society in November 2017 was a critical step forward. We would like to underscore the importance of this effort to engage with stakeholders across the CIED ecosystem to identify patient-focused communication strategies for device cybersecurity. In the Proceedings of the Heart Rhythm Society's Leadership Summit, Slotwiner et al[2] provide important recommendations to facilitate thoughtful benefit-risk discussions on cybersecurity between patients and health care providers. Given the longevity of CIEDs and the evolving threat of exploitation of cybersecurity vulnerabilities, device software and firmware updates will periodically be needed to promote good cybersecurity hygiene.

The Food and Drug Administration's (FDA's) Center for Devices and Radiological Health is responsible for assuring that patients have timely and continued access to safe and effective medical devices. Over the past several years, we have taken important steps to assist industry in identifying cybersecurity considerations throughout the life cycle of a device. Before granting market authorization, we carefully assess the cybersecurity controls of a given device. Medical device manufacturers are expected to address security during the design and development phase and to continually maintain it once marketed to effectively mitigate patient safety risks. Manufacturers and FDA must remain vigilant as cybersecurity risks in networked devices are constantly evolving. The ability of a marketed device to be updated quickly and easily to mitigate these emerging risks is imperative and should be part of a manufacturer's cybersecurity preparedness and response planning efforts. A risk-based approach to the ongoing management of medical device cybersecurity is imperative.

We recognize the importance of striking the right balance between advancing device cybersecurity and avoiding unnecessary anxiety and inconvenience for patients and their health care providers. We do not take the decision to implement or communicate about software updates lightly. However, we are also committed to preventing a widespread cybersecurity incident that could have important public health consequences. Recent experience with software deployments for CIEDs has demonstrated that there is variability among the clinical community in the implementation of cybersecurity updates for these devices. The novelty of these issues and the misconception that cybersecurity risks are theoretical may have contributed to the variable and inconsistent approach to handling these updates. Unlike traditional benefit-risk discussions that clinicians are accustomed to having with their patients, cybersecurity risks cannot be quantified in the same way. It is our hope that increased and timely adoption of cybersecurity updates will become a part of routine CIED care.

While significant progress has been made, FDA recently announced its intention to explore the development of a CyberMed Safety (Expert) Analysis Board, a public-private partnership that would complement existing device vulnerability coordination and response mechanisms.[3] The CyberMed Safety (Expert) Analysis Board's functions would include assessing vulnerabilities, proposed mitigations, and patient safety risks and serving as a "go-team" that could

Address reprint requests and correspondence: Ms Jessica E. Paulsen, Chief, Implantable Electrophysiology Devices Branch, Center for Devices and Radiological Health, U.S. Food and Drug Administration, 10903 New Hampshire Avenue, WO66-RM1316, Silver Spring, MD 20993. E-mail address: jessica.paulsen@fda.hhs.gov.

1547-5271/$-see front matter Published by Elsevier Inc. on behalf of Heart Rhythm Society.

https://doi.org/10.1016/j.hrthm.2018.05.002

be deployed to the field to investigate a suspected or confirmed device compromise.

As a community, we need to continue to promote education, awareness, and engagement to address the challenges with strengthening medical device cybersecurity. FDA encourages continued collaboration among the manufacturers, government agencies, researchers, professional societies, health care providers, and patients to employ a risk-based approach to assessing vulnerabilities and implementing routine software updates that promote good cybersecurity hygiene to protect patients.

References

1. 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:e69–e100.
2. 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:e61–e67.
3. Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health. Food and Drug Administration Web site, https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf. Accessed April 26, 2018.