Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit

David J. Slotwiner, MD, FHRS,[*,†] Thomas F. Deering, MD, FHRS, CCDS,[‡] Kevin Fu, PhD,[§] Andrea M. Russo, MD, FHRS,[¶] Mary N. Walsh, MD, FACC,[‖] George F. Van Hare, MD, FHRS, CCDS, CEPS-PC[**]

*From the *New York-Presbyterian Queens, New York, New York, †Cardiology Division, Weill Cornell Medical College, New York, New York, ‡Arrhythmia Center, Piedmont Heart Institute, Atlanta, Georgia, §College of Engineering, University of Michigan, Ann Arbor, Michigan, ¶Cooper Medical School of Rowan University, Camden, New Jersey, ‖St. Vincent Heart Center, Indianapolis, Indiana, and **Division of Pediatric Cardiology, Washington University in St. Louis School of Medicine, St. Louis, Missouri.*

TABLE OF CONTENTS

Introduction e61
Landscape e61
When to notify stakeholders e63
Who should be notified e64
Preferred communication methods e65
Key elements of a discussion about cyber threats e65
Conclusion e65
References e66

Introduction

Computers, networking, and software have become essential tools for health care. Our daily lives increasingly depend on digital technology, and we are persistently bombarded by the need to secure the systems and data they generate and store from attack, damage, and unauthorized access. Cybersecurity vulnerabilities of cardiac implantable electronic devices (CIEDs) are no longer hypothetical. While no incident of a cybersecurity breach of a CIED implanted in a patient has been reported, and no patient is known to have been harmed to date by the exploitation of a vulnerability, the potential for such a scenario does exist. The public awareness of cybersecurity vulnerabilities in medical devices, particularly devices such as CIEDs on which a patient's life may depend and where the potential for reprogramming or rendering the device nonfunctional exists, is raising questions and fueling fears among patients and the clinical provider community. The Heart Rhythm Society (HRS) has identified a gap in clinician-patient communication about the appropriate balance of the risks of such a potential attack against the benefits of lifesaving medical devices. To address these communication gaps, HRS convened a 1-day summit in November 2017, in partnership with the U.S. Food and Drug Administration (FDA). The goal of the meeting was to develop patient-centered communication strategies for health care professionals, industry, and governmental agencies. Participants included patient representatives, subject matter experts, HRS and the American College of Cardiology leadership, representatives from the FDA, and the Federal Bureau of Investigation (FB1) and leadership of 5 CIED manufacturers. This proceedings statement is based on the 4 communication themes that emerged from the discussion: when to notify patients, whom to notify, how to communicate with patients, and key elements to discuss with patients.

KEYWORDS Cardiac resynchronization therapy; Cardiac implantable electronic device; Computer hacking; Cybersecurity; Implantable defibrillator; Remote monitoring; Shared decision making (Heart Rhythm 2018;15:e61–e67)

Endorsed by the Heart Rhythm Society Board of Trustees. **Address reprint requests and correspondence:** Dr David J. Slotwiner, New York Presbyterian Queens, 56-45 Main Street, Flushing, NY 11355. E-mail address: djs2001@med.cornell.edu.

Landscape

The rapidly changing health care environment and global interconnectivity exposes information technology to increasing vulnerabilities. Individuals with nefarious intentions can leverage these vulnerabilities for monetary gain or for

 https://doi.org/10.1016/j.hrthm.2018.05.001

Table 1 Common cybersecurity terminology

Terminology	Definition
Computer hacking	In the context of computer security, this term refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is outside the creator's original objectives.
Denial of service (DoS) attack	A cyberattack in which a threat actor seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. DoS is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[5]
Exploit	Software or a sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or electronic (usually computerized).[3]
Firmware	A specific class of computer software that provides the low-level control for the device's specific hardware. Firmware can either provide a standardized operating environment for the device's more complex software (allowing more hardware independence) or, for less complex devices, act as the device's complete operating system, performing all control, monitoring, and data manipulation functions.[6]
Ransomware attack	An attack utilizing a form of malware in which malicious software code effectively holds a user's computer hostage until a ransom fee is paid. Ransomware often infiltrates a personal computer as a computer worm or Trojan horse that takes advantage of open security vulnerabilities. Most ransomware attacks are the result of accessing an infected e-mail attachment or visiting hacked or malicious Web sites.[4]
Threat actor	An entity typically with malicious intent that is partially or wholly responsible for an incident that affects—or has the potential to affect—an organization's security or a device's security.[2]
Vulnerability	A weakness in computer software code that could be exploited by a threat actor (defined below) to perform unauthorized actions within a computer system.[1]

causing disruption. The public, regulatory agencies, the health care community, and manufacturers increasingly recognize the urgency of the challenge. By gaining unauthorized access to diagnostic or therapeutic medical equipment, hackers may cause a variety of problems (Table 1). These range from ransomware attacks to denial of service attacks, sensor malfunction, or degradation of device function. CIEDs could potentially be reprogrammed, or their normal function could be degraded or disabled. Remote monitoring of CIEDs that requires frequent communication between a home transceiver and the device using radiofrequency telemetry adds an additional stage that could be vulnerable to a cybersecurity breach.

In some cases, such as the WannaCry ransomware attack, medical equipment can be affected without being the primary target of an attack. WannaCry targeted computers running an outdated version of the Microsoft Windows operating systems of which users failed to install updates to patch known vulnerabilities. The WannaCry actors encrypted user data and demanded ransom payment to release it, affecting, among others, multiple hospitals and health care professionals around the globe. As a result, network-connected medical devices across the United States running on this operating system were affected and taken off-line for remediation. Even equipment not connected to the Internet or internal health system servers is vulnerable to hacking. For example, ventilators and external defibrillators can become infected by malware on thumb drives that are plugged into systems when updating software or transferring data.[7]

Inconsistent cybersecurity prioritization in health care delivery organizations and the broad range of manufacturers supplying equipment to the health care industry (diagnostic and therapeutic medical equipment, electronic health records, billing software, purchasing software, etc) has resulted in significant cybersecurity vulnerabilities. Most modern medical equipment contains hardware and software components. The life cycle of software is often shorter than the product life of the hardware components. Institutions frequently use software beyond the period supported by the developer, and device manufacturers may not provide timely updates to identified cybersecurity vulnerabilities, leaving the software vulnerable to attack and providing an entry point for hackers to gain access across the interconnected information technology environment of a health care organization.

In 2013, President Barack Obama issued an executive order calling on the U.S. federal agencies to work collaboratively with critical infrastructure owners and operators to protect the nation's most sensitive infrastructures, including the health care sector, from cybersecurity threats.[8] The U.S. Department of Homeland Security's (DHS's) National Cybersecurity and Communications Integration Center (NCCIC) is tasked with analyzing and reducing cybersecurity threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities (Figure 1). When an incident occurs or is reported, NCCIC triages and collaborates a response to the incident. FDA becomes involved in the evaluation of a threat if it is deemed possible to result in patient harm. In such an event, the agency's role and responsibilities fall largely in line with non–cybersecurity responsibilities. For example, in the event of a CIED cybersecurity vulnerability, the FDA's Center for Devices and Radiological Health (CDHR) interacts with the manufacturer to assess the vulnerability and develop mitigating and/or corrective action (Table 2). In the event of a cybersecurity breach in which

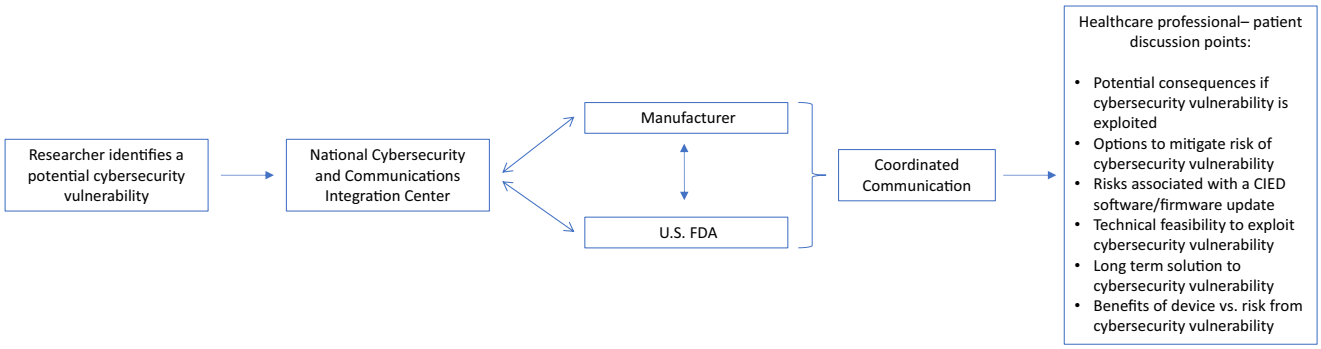

Figure 1 Evaluation and notification sequence of a new cybersecurity vulnerability threat: Assessment of a potential cybersecurity vulnerability requires expertise from the Department of Homeland Security's National Cybersecurity and Communications Integration Center and the manufacturer. The Federal Bureau of Investigation becomes involved if there is potential criminal activity. If the vulnerability is validated, the discussion between health care professionals and patients should consider these 6 topics. If the claim of a new vulnerability is released directly to the public, there will be a period of uncertainty and anxiety while the claim is being evaluated. FDA = Food and Drug Administration.

protected health information is exposed, the Department of Health and Human Services (HHS) Office for Civil Rights may coordinate with affected health plans, health care clearinghouses, and health care providers. The operating divisions of HHS such as FDA, Office for Civil Rights, and Office of the National Coordinator for Health Information Technology (electronic health records), and Office of the Assistant Secretary for Preparedness and Response coordinate regularly within the HHS Cybersecurity Working Group and on an as-needed basis, through established mechanisms, and during cyber events, such as WannaCry. Interactions between HHS and other agencies such as DHS and the FBI also occur on a routine and event basis.

As cybersecurity vulnerabilities are increasingly appreciated as a high priority, there needs to be a joint effort by industry, regulatory agencies, and providers to implement solutions. While the problems are potentially vast, they are not insurmountable. The Association for the Advancement of Medical Instrumentation (AAMI) in 2016 published TIR57: Principles of Medical Device Security—Risk Management.[10] This provides technical recommendations for medical device manufacturers on developing cybersecurity risk management processes into their products. A second publication in development, TIR97, will focus on the postmarket approval security management of medical devices with recommendations on threats, vulnerabilities, and exploits as well as recommendations if a vulnerability is exploited. FDA has issued guidance to industry for both 510(k) premarket notifications and premarket approval applications identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as a separate guidance document with recommendations emphasizing how manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices.[11,12] Since the Leadership Summit, FDA has outlined their vision for how FDA can continue to enhance their cybersecurity programs and processes to ensure the safety of medical devices throughout the total product life cycle in the Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health.[13] In the long term, systems should be developed to minimize vulnerabilities and, if compromised, designed to fail in a way that minimizes risk to patients (ie, fail gracefully).

A cultural shift within the health care community is imperative to mitigate vulnerabilities. Health care institutions must make a commitment to timely implementation of software updates and to retiring or updating software that is no longer supported. Clinicians should be proactive and seek guidance from information technology experts to ensure that new and existing systems and equipment meet the recommended specifications to minimize cybersecurity risks. Health care professionals must be educated about cybersecurity risks, their role in minimizing vulnerabilities, and how to incorporate cybersecurity into discussions with patients. In the realm of CIEDs where patients are often dependent on their devices, clinicians must also appreciate that cybersecurity vulnerabilities are often solved only by updating the devices firmware, a specific type of software embedded in the hardware of a CIED that is involved with very basic low-level operations without which a device would be nonfunctional. When considering updating a CIED's firmware, clinicians will need to weigh the risks to patients in terms of both the cybersecurity vulnerability and the risk of the firmware update that carries a small but real risk of reducing device longevity or causing the device to malfunction. The best practice model is for patients to receive intermittent software updates as part of the ongoing management of their CIED at the time of face-to-face visits, mitigating concerns that accompany each recognition of a new vulnerability.

When to notify stakeholders

Patients and health care professionals have varying preferences about when and by whom they would like to be notified of cybersecurity vulnerability, depending on the threat level and urgency.

If an individual or organization chooses to bring a cybersecurity concern to the manufacturer or the proper authorities/organizations, the vulnerability can be evaluated efficiently by proper experts. If the threat is validated, the manufacturer and FDA, in concert with medical experts and cardiovascular societies, may then work together to develop a strategy to

Table 2 U.S. federal agencies and international organizations involved in cybersecurity oversight

Agency or organization	Role
Association for the Advancement of Medical Instrumentation (AAMI)	A nonprofit international organization founded with the single mission of promoting the development, management, and safe use of effective health technology. AAMI is the primary source of consensus standards, both national and international, for the medical device industry.[9]
Health Care Industry Cybersecurity Task Force	A U.S. Department of Health and Human Services convened task force mandated through congressional legislation (CISA 2015) to conduct a landscape analysis of the current state of cybersecurity within the health care sector and to provide recommendations for its improvement.
National Cybersecurity and Communications Integration Center (NCCIC)	The branch of the U.S. Department of Homeland Security responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.
Office of the Assistant Secretary for Preparedness and Response (ASPR)	The office within the U.S. Department of Health and Human Services created to lead the United States in preventing, preparing for, and responding to the adverse health effects of public health emergencies and disasters.
Office of the National Coordinator for Health Information Technology (ONC)	The branch of the U.S. Department of Health and Human Services charged with coordinating nationwide efforts to implement and use health information technology and the electronic exchange of health information. This agency regulated electronic health records to ensure they meet the specifications of the "meaningful use" legislation.
U.S. Department of Health and Human Services, Office for Civil Rights	Enforces federal civil rights laws and the Health Insurance Portability and Accountability Act.
U.S. Federal Bureau of Investigation(FBI)	The branch of the U.S. Department of Justice and member of the U.S. Intelligence Community and principal federal law enforcement agency with oversight of criminal investigations pertaining to cybersecurity.
U.S. Food and Drug Administration, Center for Devices and Radiological Health	The center of FDA tasked with regulating medical devices and radiation-emitting products.

manage and communicate it to stakeholders (Figure 1). This is the ideal scenario. This approach avoids unnecessary alarm over threats that prove to be unfounded; and when it is a real threat, it provides stakeholders with guidance from experts on how to best respond. Most vulnerabilities are identified by the security research community for the purpose of notifying manufacturers in a responsible manner in order to prevent the vulnerability from being exploited. Unfortunately, there are individuals or groups with nefarious intent and they may choose to release a claim directly to the public. When this occurs, it leaves the manufacturer, government agencies, and the public in a difficult position as they attempt to evaluate and respond to the claim. In these circumstances, the decision of when to notify stakeholders has been determined by the actor. The authorities and manufacturer must attempt to rapidly assess both the validity of the claim and the potential risks to patients to prevent improper action or exploitation of the situation. Health care professionals and patients are placed in a precarious and uncertain situation when the validity of an external claim remains unresolved. Since information about potential risks often evolves as more information becomes available, communication to health care professionals and patients about the process and how it might evolve is important. If an actor chooses to release details of a potential cybersecurity vulnerability to the public directly, then that individual or organization has made the decision of whom to notify. Sometimes this occurs when a security researcher has been unable to gain a satisfactory response after notifying a manufacturer of a vulnerability. Occasionally this is done to cause fear and confusion and to gain a benefit, or profit.

Clinicians, patients, and the public understandably seek a single source of timely, comprehensive, and accurate information as well as guidance in the event of an urgent advisory or cybersecurity threat. Currently, no such single resource exists. The manufacturers, FDA, and medical societies each have mechanisms in place to address this need. HRS has created a Therapy Advisory Response Working Group to engage subject matter experts, as needed, to quickly assess the available data and to communicate the information and its recommendations to members and other relevant stakeholders.

Who should be notified

The most effective notification process is one that allows proper review and evaluation by experts before a cyber threat becomes publicly known. The decision of whom to notify

can be made by the device manufacturer working with government agencies, medical experts, and the medical societies on the basis of an informed evaluation of the vulnerability's validity when a potential cybersecurity threat is reported to authorities in a responsible manner. Patients at potential risk and their health care professionals should be informed of the vulnerability, the potential for harm, and the ease at which it could be exploited. This scenario allows patients to work with their health care professionals and device manufacturer to take preventive action and to install available security updates.

The goal is to reach a point in time at which patients receive intermittent software updates, including patches for cybersecurity vulnerabilities as part of their regular follow-up, like the updates received by computers and smartphones. A critical point is to set expectations of good cybersecurity hygiene prior to the implantation of the CIED. When this goal is achieved, conversation about threats can become a part of routine patient care.

Preferred communication methods

Given the diverse learning styles, the broad range of health literacy, age, educational background, personal preferences, and values of patients, it is necessary to communicate the information about cybersecurity vulnerabilities via different communication platforms. Communication tools from health care professionals and device manufacturers to improve understanding, reduce anxiety, and accommodate diverse learning preferences should include print materials, mail, electronic communication modalities (eg, e-mail and web-based approaches), as well as preferably clinician- patient discussions. Patient representatives at the Leadership Summit expressed an unequivocal desire to receive information on potential cybersecurity vulnerabilities directly from the manufacturers of their CIED. As CIED manufacturers currently communicate to health care professionals via "Dear Doctor" letters when there is a device recall or safety advisory, this preference would require a change in communication strategies. Patients recognize that understanding and evaluating cybersecurity vulnerabilities requires expertise outside the medical field. However, patients want and expect their health care professionals to help interpret a cybersecurity threat and identify and implement an effective management strategy in the context of their individual medical needs and the details of the potential threat.

Key elements of a discussion about cybersecurity threats

A conversation about cybersecurity threats is integral to a discussion about the risks and benefits of a CIED prior to implantation and should be a part of routine follow-up care of patients with CIEDs. Unlike the familiar discussion of risks and benefits, which draws on the underlying pathophysiology of a patient's disease and the known characteristics of a specific therapy, the discussion of cybersecurity threats must be different and is unique to health care. For example, a routine discussion of risks and benefits would include an estimate of a chance of bleeding, stroke, or other serious complications, as well as eliciting patient's values and preferences as utilized during shared decision making. In contrast, it can be difficult to estimate the risk associated with cybersecurity vulnerabilities. In addition, software and firmware updates to devices have the potential for causing unintended or unforeseen consequences, including device malfunction. While this risk is variable and often minimal, it must be considered. As such, the mitigation of a cybersecurity vulnerability depends not only on its reparability but more importantly on the risk benefit assessment related to the repair vs the security risk.

Despite the fundamental distinction between the well-established discussion of risks and benefits of device therapy vs the risk of cybersecurity threats and implications for patient choices of therapy, research on patient preferences and communication strategies is absent and should be addressed. This conversation is an opportunity to share information about managing and mitigating potential threats through intermittent software updates that are installed at the time of in-office face-to-face visits. Initiating the discussion of potential cybersecurity vulnerabilities prior to device implantation and explaining the need for routine software updates over the CIED's lifetime sets patient expectations and informs the shared decision making encounter. If a specific vulnerability is identified, the discussion can be individualized to patients and should consider the following 6 topics (Figure 1):

1. Potential consequences for the CIED if the cybersecurity vulnerability is exploited,
2. Options to mitigate the risks,
3. Risks associated with a CIED software/firmware update,
4. Relative ease of exploiting the vulnerability,
5. Long-term solutions to eliminate the vulnerability, and
6. Benefits provided by the CIED vs the risk if the cybersecurity vulnerability is exploited.

The dialogue should also address the patient's preference to pursue their treatment in a shared decision manner.

Conclusion

Given sufficient time and resources, actors or groups can potentially identify software vulnerabilities in nearly any product. The interconnectedness of the health care environment combined with the common persistence of outdated and unsupported software in these facilities makes them particularly vulnerable to exploitation. Industry and regulatory agencies now emphasize security from the beginning stages of product design, with the goals of reducing vulnerabilities and minimizing patient risk if a CIED security is compromised by ensuring that life-sustaining functions remain functional. Patients with CIEDs may feel particularly vulnerable and fearful as their survival may depend on the proper function of their device. Patients will turn to their health care professionals seeking guidance. It is imperative that HRS, the American College of Cardiology, and their partners educate health care professionals to minimize cybersecurity risks and understand the current mechanisms in

place to evaluate individual threats. It is also critical to set expectations at the time of implantation that medical devices, such as CIEDs, will require software updates until the battery is depleted. When specific vulnerabilities become known, the risk assessment must balance the ease of exploitability and weigh the consequences and benefits of continuing therapy (eg, remote monitoring of CIEDs). Threat actors with malicious intent may exploit patient fears by directly releasing claims of vulnerabilities to the public rather than through the well-established channels to properly evaluate claims and develop risk management strategies. By educating patients prior to CIED implantation and in advance of an announcement of a specific vulnerability or threat, patients will better understand the systems in place to quickly assess and respond to potential vulnerabilities.

In summary:

- Several agencies and organizations are responsible for assessing cybersecurity threats including DHS's NCCIC and FDA.
- The American Association for Medical Instrumentation continues to lead efforts to refine technical guidelines and standards designed to minimize CIED cybersecurity vulnerabilities and to prevent catastrophic device failure if a cybersecurity threat is exploited.
- Federal agencies, device manufacturers, and organizations have specific responsibilities when evaluating potential cybersecurity vulnerabilities and communicating to stakeholders:
  - Federal agencies are responsible for working together to evaluate the validity of the claim, work with the manufacturer to mitigate risk to patients, and pursue criminal investigations when necessary.
  - Manufacturers are responsible for notifying authorities, evaluating the claim and, if validated, developing a strategy to mitigate the risk to patients and ultimately to developing a solution.
  - Medical societies can serve as a resource to manufacturers, federal agencies, and health care professionals by taking a consensus recommendation from experts and communicating consistent, accurate, and clear information to health care professionals.
  - Health care professionals serve a critical role in assisting patients to interpret the significance of a cybersecurity vulnerability, the relative risks and benefits of continuing to receive therapy from the potentially affected device and deciding if they will pursue a mitigation strategy.
- Health care professionals and patients recognize that software upgrades are as important as medication lists, follow-up regimens, a new diagnosis, and other elements of routine care.
- When a potential vulnerability is identified, health care professionals should consider discussing the following:
  - Potential consequences if the vulnerability is exploited,
  - Strategies to mitigate their vulnerability,
  - Risks associated with a CIED software/firmware update,
  - Technical feasibility of exploiting the vulnerability,
  - Long-term solutions to eliminate the vulnerability,
  - Benefits of continued device therapy vs risk of vulnerability.
- Ultimately, the health care field must reach a point where intermittent software updates are considered the standard of care. This practice will minimize the risk and reduce fear when new vulnerabilities are identified.

The challenge of cybersecurity vulnerabilities in CIEDs and the health care delivery system is significant but not insurmountable. The primary goal is to educate health care providers about the risks and new initiatives by stakeholders to incorporate cybersecurity considerations into early stages of product design as well as about the infrastructure in place to evaluate and mitigate specific vulnerabilities when they arise. This will reduce fear and decrease the opportunity for threat actors to successfully achieve their malicious aims.

Appendix

Supplementary data

Supplementary data associated with this article can be found in the online version at https://doi.org/10.1016/j.hrthm.2018.05.001.

References

1. Vulnerability (computing). Wikipedia Web site, https://en.wikipedia.org/wiki/Vulnerability_(computing). Accessed April 18, 2018.
2. Threat actor. TechTarget Web site, https://whatis.techtarget.com/definition/threat-actor. Accessed April 18, 2018.
3. Exploit (computer security). Wikipedia Web site, https://en.wikipedia.org/wiki/Exploit_(computer_security). Accessed March 25, 2018.
4. Ransomware. Webopedia Web site, https://www.webopedia.com/TERM/R/ransomware.html. Accessed February 25, 2018.
5. Security Tip (ST04-015). Understanding Denial-of-Service Attacks. United States Computer Emergency Readiness Team (US-CERT) Web site, https://www.us-cert.gov/ncas/tips/ST04-015. Accessed February 25, 2018.
6. Firmware. Wikipedia Web site, https://en.wikipedia.org/wiki/Firmware. Accessed April 18, 2018.
7. Software Update Site For Hospital Respirators Found Riddled With Malware. Threatpost Web site, https://threatpost.com/software-update-site-hospital-respirators-found-riddled-malware-061412/76695/. Accessed February 10, 2018.
8. Executive Order – Improving Critical Infrastructure Cybersecurity. The White House President Barack Obama Web site, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Accessed February 10, 2018.
9. Membership Community. Association for the Advancement of Medical Instrumentation Web site, http://www.aami.org/membershipcommunity/content.aspx?ItemNumber=1292&navItemNumber=2906. Accessed April 18, 2018.
10. AAMI TIR57: Principles for Medical Device Security—Risk Management. Association for the Advancement of Medical Instrumentation Web site, http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729. Accessed February 10, 2018.
11. Postmarket Management of Cybersecurity in Medical Devices. U.S. Food and Drug Administration Web site, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. Accessed January 20, 2018.
12. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. U.S. Food and Drug Administration Web site, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf. Accessed January 20, 2018.
13. Medical Device Safety Action Plan: Protecting Patients, Promoting Public Heath. U.S. Food and Drug Administration Web site, https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf. Accessed January 20, 2018.

Appendix Table A1 Writing group author disclosure table

Writing group	Employment	Consultant/ advisory board/ honoraria	Speakers' Bureau	Research grant	Fellowship support	Equity interests/ stock options	Others
David J. Slotwiner, MD, FHRS	New York-Presbyterian/Queens, New York, New York; Weill Cornell Medical College, Cardiology Division, New York, NY	None	None	None	None	None	None
Thomas F. Deering, MD, FHRS, CCDS	Arrhythmia Center, Piedmont Heart Institute, Atlanta, GA	None	None	None	None	None	None
Kevin Fu, PhD	College of Engineering, University of Michigan, Ann Arbor, MI	None	1; Medtronic, Inc.	None	None	None	None
Andrea M. Russo, MD, FHRS	Cooper Medical School of Rowan University, Camden, NJ	None	1; Medtronic, Inc., Biotronik, Boston Scientific Corp., St. Jude Medical	2; Medtronic, Inc., Boehringer Ingelheim, Boston Scientific Corp.	2; Medtronic, Inc.	None	0; Apple
Mary N. Walsh, MD, FACC	St. Vincent Heart Center, Indianapolis, IN;	None	None	None	None	None	None
George F. Van Hare, MD, FHRS, CCDS, CEPS-PC	Division of Pediatric Cardiology, Washington University in St. Louis School of Medicine, Saint Louis, MO	None	None	None	None	None	None

Number Value: 0 = $0; 1 = < $10,000; 2 = > $10,000 to < $25,000; 3 = > $25,000 to < $50,000; 4 = > $50,001 to < $100,000; 5 = > $100,000.