Mitigating Security Risks Associated with Wireless Infusion Pumps

Save to myBoK

By William R. Shenton, JD

Wireless infusion pumps must provide a steady inflow of life-saving or life-sustaining medications, but these critical devices come with significant risks that every healthcare organization must address. To operate effectively and efficiently, infusion pumps often must be linked to a network and to the internet, which brings the risk of malicious manipulation that can result in patient harm, data breaches, and can even expose an entire organization's computer system to ransomware. Federal regulatory agencies have put attention on these key security issues, leading to conclusions on practical takeaways for healthcare organizations.

The risks of wireless medical devices have received dramatic attention, including an episode of the TV series *Homeland*, where a hacked cardiac pacemaker was manipulated to assassinate the vice president. While the portrayal in the *Homeland* episode may have been dramatized for effect, it reflects very real security concerns.

Government Issues Warnings, Guidance

Networked medical devices have been on the cybersecurity radar screen for some time and received attention in the 2017 report from the Health Care Industry Cybersecurity Task Force.[1] The report identified a number of patient risks that can result from inadequate security on medical devices, including unauthorized alteration of data or operating parameters and denial of service attacks which can render a device inoperable and lead to exfiltration of patient data.

In September 2017, the Food and Drug Administration (FDA) issued a recall for almost a half million pacemakers.[2] In that same month came news about infusion pumps' vulnerability.[3]

The FDA has been issuing guidance about the risks associated with infusion pumps for some time and has a webpage dedicated to this issue.[4] Mitigating risks to wireless infusion pumps has received more attention recently. In October 2018, the FDA issued a draft update of its 2014 guidance concerning Premarket Submissions for Management of Cybersecurity in Medical Devices.[5] In November 2018, the FDA issued a "FDA In Brief" document highlighting its oversight efforts for infusion pumps and other medical devices.[6]

The FDA guidance is directed at manufacturers of all types of medical devices and provides information to manufacturers about cybersecurity issues that the FDA will examine in future pre-market reviews of devices. However, the guidance has helpful information about issues that healthcare organizations currently face in deploying and maintaining wireless devices, discussed later in this article.

In August 2018, the National Cybersecurity Center of Excellence (NCCoE) finalized the draft guidance it first issued last year on securing wireless infusion pumps.[7] The NCCoE guidance is targeted for clinical and administrative leaders, as well as the IT staff who run their networks. The 375-page report has detailed information about technical measures to secure infusion pumps. For a good visual representation of the suggested system architecture consult the second page of NCCoE's Summary, which is linked on the webpage where NCCoE's guidance is available.[8] The guidance stresses that the architecture for these solutions uses commercially available hardware and software and was developed with input from the vendors.

A fundamental takeaway from NCCoE is the need to come to grips with common vulnerabilities of these devices, listed in Appendix B of NCCoE's guidance, including:

- Infusion pumps may stay in service beyond the point at which they can be easily updated or patched.
- Infusion pumps will store sensitive patient information, but may lack the ability to encrypt it either at rest or in transit.
- Infusion pumps with external or removable media heighten the risk of inappropriate disclosure of information, as well as the introduction of malicious software.

Appendix C in the NCCoE Report contains a concise list of recommendations and best practices, but emphasizes that the threat landscape is constantly evolving. NCCoE is inviting comments on its guidance. To comment or to learn more, including how to arrange a demonstration of its example implementation, contact NCCoE at hit_nccoe@nist.gov.

In the meantime, there are a number of basic practical steps that organizations can implement which are suggested by the NCCoE and the FDA. They revolve around the three overarching domains of security in the HIPAA Security Rule: the physical, the technical, and the administrative.

Physical Security

The first step in the NIST Cybersecurity Framework is identify, which entails a concerted effort to identify every wireless infusion pump in the organization (along with other wireless devices).[9] Each organization will want to create and continuously update this inventory with detailed information, including the manufacturer of each device and contact information; the departments or locations within the organization where each type of pump is typically used and their typical use cycles; and whether the manufacturer has issued software updates or patches and documentation that patches were installed.

Another obvious but still important issue highlighted by NCCoE is establishing a secure area where devices not in use may be stored, which remains reasonably accessible to the clinical staff who must employ them.

Technical Safeguards

The FDA draft guidance in October recommends that device manufacturers begin providing customers with a list of the hardware and software components of a device, so that customers can understand when a publicized vulnerability might affect their deployed devices. While this is not yet a FDA requirement, it is not too early to collect and maintain that information as part of the device inventory.

The NCCoE guidance spotlights the repository of vulnerability management data maintained at the National Vulnerability Database as a source of this information.[10]

Since infusion pumps often are deployed for years, there must be a program to assess, update, and patch them on an ongoing basis. But patching should follow a systematic approach. Guidance on software vulnerabilities and patching software issued in June 2018 by the US Department of Health and Human Services' Office for Civil Rights emphasized the importance of confirming that a patch has not compromised the functionality of a device and of making sure that the clinical staff is oriented appropriately.[11]

The FDA draft guidance in October 2018 also mentions the concept of segregating some devices on the organization's network to limit the negative impact of an exploit of an older device that can no longer be patched or updated effectively. NCCoE recommends implementing media access address filtering to limit access to medical devices by unauthorized actors attempting to infiltrate the organization's network through an exposed ethernet port on the device.

Administrative Policies

The human element is critical to cybersecurity and this arena is no different. Securing wireless infusion pumps and other wireless devices will involve clinical and IT staff working collaboratively to develop procedures that will ensure reasonable, workable physical and technical safeguards are implemented and can be followed without disrupting patient care. On its Medical Device webpage, the FDA recommends establishing teams of clinical, management, and IT personnel who work collaboratively to develop and refine policies and respond to incidents, and the FDA website has several webpages targeted at the various clinical, IT, and management disciplines that have responsibilities for the acquisition, deployment, or use of infusion pumps.[12]

The NCCoE guidance highlights the importance of role-based access to the devices, limiting access to particular functions on an infusion pump solely to persons whose job functions require them to use those functions. NCCoE also emphasizes the fundamental principle that devices should not be deployed with default passwords or other manufacturer-installed settings that would expose them to malicious attacks.

The ability to carry out these protective measures must be factored into the process of acquiring new devices, and the FDA has highlighted a number of important features for manufacturers to implement in a checklist on page 13 of its draft guidance. The checklist identifies important features that should be considered by healthcare organizations in purchasing wireless devices.

The FDA's draft guidance in October 2018 also emphasizes the value of information sharing about risks and vulnerabilities among the user community. Among the Information Sharing Analysis Organizations (ISAOs) established to facilitate timely sharing of information about cybersecurity threats is the Health Information Sharing and Analysis Center.[13]

Stay Tuned as Threats Evolve

While the guidance from the FDA and NCCoE contains important cybersecurity tools that are ready to be implemented now, it is important to stay tuned as cybersecurity threats evolve.

Notes

1. Department of Health and Human Services (HHS). "Health Care Industry Cybersecurity Task Force Report on Improving Cybersecurity in the Health Care Industry." June 2017. www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

2. Food and Drug Administration (FDA). "Class 2 Device Recall Accent family of pacemakers." November 2018. www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRes/res.cfm?ID=158779.
3. Paganini, Pierluigi. "Hackers can remotely access Smiths Medical Syringe Infusion Pumps to kill patients." Security Affairs. September 11, 2017. https://securityaffairs.co/wordpress/62918/hacking/syringe-infusion-pumps.html.
4. FDA. "Infusion Pump Risk Reduction Strategies." August 22, 2018. www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202498.htm.
5. FDA. "FDA In Brief: FDA proposes updated cybersecurity recommendations to help ensure device manufacturers are adequately addressing evolving cybersecurity threats." October 17, 2018. www.fda.gov/NewsEvents/Newsroom/FDAInBrief/ucm623624.htm.
6. FDA. "FDA In Brief: FDA's increased inspections of medical device manufacturers and targeted risk-based approach leads to improved compliance." November 21, 2018. www.fda.gov/NewsEvents/Newsroom/FDAInBrief/ucm626428.htm.
7. National Institute of Standards and Technology and National Cybersecurity Center of Excellence. "Securing Wireless Infusion Pumps in Healthcare Delivery Organizations." August 2018. www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf.
8. O'Brien, Gavin et al. "Securing Wireless Infusion Pumps." National Institute of Standards and Technology and National Cybersecurity Center of Excellence. August 17, 2018. www.nccoe.nist.gov/projects/use-cases/medical-devices.
9. National Institute of Standards and Technology. "Cybersecurity Framework." www.nist.gov/cyberframework.
10. National Institute of Standards and Technology. "National Vulnerability Database." https://nvd.nist.gov/.
11. HHS' Office for Civil Rights. "June 2018 OCR Cybersecurity Newsletter." www.hhs.gov/sites/default/files/june-2018-newsletter-software-patches.pdf.
12. FDA. "Infusion Pump Risk Reduction Strategies." August 22, 2018. www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202498.htm.
13. Health Information Sharing and Analysis Center (H-ISAC). Home page. https://nhisac.org/.

William R. Shenton (wshenton@poynerspruill.com) is a partner at Poyner Spruill LLP in Raleigh, NC. His areas of expertise include health and hospital law, civil litigation, and administrative law, and his practice includes advising and representing healthcare facilities and individual providers in federal and state regulatory compliance issues, certificate of need issues, administrative appeals, compliance issues, HIPAA, and state and federal civil litigation.

Article citation:
Shenton, William R. "Mitigating Security Risks Associated with Wireless Infusion Pumps." *Journal of AHIMA* 90, no. 1 (January 2019): 24-27.