The Evolving State of Medical Device Cybersecurity

Suzanne Schwartz, Aftin Ross, Seth Carmody, Penny Chase, Steve Christey Coley, Julie Connolly, Cathy Petrozzino, and Margie Zuk

To advance patient care, medical devices are becoming increasingly connected and interoperable. Although interconnectivity and interoperability may provide great benefits, connected devices also present considerable cybersecurity risks. Device cybersecurity vulnerabilities, whether exploited maliciously or triggered unintentionally, may not only affect device performance but also the availability and integrity of the device and its data. These effects also may result in patient and/or user harms, such as illness, injury, or death, and negatively affect hospital operations. Thus, it is imperative that medical device stakeholders (e.g., government, private industry, healthcare organizations) embrace their shared responsibility for medical device cybersecurity.

The Food and Drug Administration's (FDA's) Center for Devices and Radiological Health (CDRH) is responsible for ensuring that patients and healthcare providers have access to safe and effective medical devices. This is accomplished by FDA's review of medical device submissions prior to market release and its surveillance of medical devices in the postmarket setting. CDRH is committed to enhancing patient safety by mitigating medical device cybersecurity risk throughout the product life cycle, from device conception to obsolescence. This is reflected in the 2014[1] and 2016[2] FDA guidance documents on cybersecurity.

In addition to issuing guidance, the FDA has held three public workshops on medical device cybersecurity that convened diverse stakeholders to discuss relevant regulatory science, technology, and policy gaps; address challenges; and share best practices.[3–5] Although the FDA has catalyzed medical device cybersecurity activities, enhancing medical device cybersecurity is a shared responsibility among stakeholders. FDA has encouraged collaboration among government, medical device manufacturers, hospitals and other health delivery organizations (HDOs), cybersecurity researchers, and patients in order to address medical device cybersecurity challenges.

In support of the FDA, the MITRE team worked with diverse stakeholder groups to understand the challenges and opportunities in medical device cybersecurity. Specifically, MITRE conducted an independent stakeholder engagement study to capture challenges, concerns, insights, and potential solutions for managing medical device cybersecurity, from stakeholders across the medical device cybersecurity ecosystem. This article summarizes the information gathered in stakeholder interviews and synthesizes initial observations and analysis.

In particular, the study focused on three key stakeholder groups: 1) HDOs, 2) manufacturers, and 3) the cybersecurity community. The team began the study by identifying representative organizations from each of the three key stakeholder groups, striving to capture the

About the Authors

Suzanne Schwartz, MD, MBA, is associate director for science and strategic partnerships at the Center for Devices and Radiological Health of the Food and Drug Administration in Silver Spring, MD.

Aftin Ross, PhD, is senior project manager at the Center for Devices and Radiological Health of the Food and Drug Administration in Silver Spring, MD.

Seth Carmody, PhD, is a cybersecurity program manager at the Center for Devices and Radiological Health of the Food and Drug Administration in Silver Spring, MD. Email: seth.carmody@fda.hhs.gov

Corresponding author

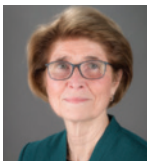
About the Authors

Penny Chase is information technology and cybersecurity integrator at the MITRE Corporation in Bedford, MA.

Steve Christey Coley is a principal cybersecurity engineer at the MITRE Corporation in Bedford, MA.

Julie Connolly is a principal cybersecurity engineer at the MITRE Corporation in Bedford, MA.

Cathy Petrozzino is a principal cybersecurity engineer at the MITRE Corporation in Bedford, MA.



Margie Zuk is a senior principal cybersecurity engineer at the MITRE Corporation in Bedford, MA.

diversity of each group. Altogether, the MITRE team spoke to more than 75 organizations and 125 individuals. The MITRE team also interviewed other members of the ecosystem who represented associations, trade groups, and other organizations.

This article provides a current snapshot of the evolving state of medical device cybersecurity across the product life cycle, including the challenges impeding safe and secure medical devices and current initiatives to advance medical device cybersecurity.

The results of this stakeholder study indicate that the diverse medical device community is actively working to strengthen medical device cybersecurity and has made great strides. However, viewing medical device cybersecurity through the lens of patient safety and product quality represents a major cultural shift, and this ongoing change in perspective requires education and time to accomplish.

Current State across the Product Life Cycle

In the United States, medical devices follow a process that integrates FDA guidance, regulatory decision making, postmarket surveillance, and oversight with a typical product development life cycle (Figures 1 and 2). This life cycle is used as a framework for contextualizing the challenges and opportunities described in this article, with a particular focus on the development, deployment, and operations and maintenance phases, as a lot of activity occurs in these areas.

As the phase alignment in Figure 1 conveys, manufacturers typically own the bulk of the device development phase, whereas HDOs lead the procurement phase. Manufacturers and HDOs often share responsibility for the remaining phases. Cross–life cycle medical device cybersecurity challenges are explored in the following sections.

Life Cycle–Wide Challenges

In the past, the healthcare industry focused on consideration of medical device quality and safety risks primarily as standalone devices rather than as connected systems. Consequently, cybersecurity risk was not given much attention. Today, potential device impacts on patient care compel manufacturer and HDO management to confront medical device cybersecurity. Nevertheless, widespread C-suite awareness and understanding of business risk to the organization are slow to gain traction in the healthcare sector.

Recent global cyberattacks, such as WannaCry and Petya/NotPetya, have served as wake-up calls to the healthcare community at large. Yet, waiting for negative consequences to mobilize a "call to action" is antithetical to FDA's approach, as the agency encourages proactive behavior across stakeholders in the medical device ecosystem. Proactive behavior requires sufficient economic incentives to drive awareness and education across all stakeholders and across all parts of their organizations. Articulating device cybersecurity incentives and business cases will help. For manufacturers, taking a total product life cycle approach to medical device cybersecurity—with cybersecurity built into devices during product development and sustained via postmarket continuous monitoring[2]—also will help

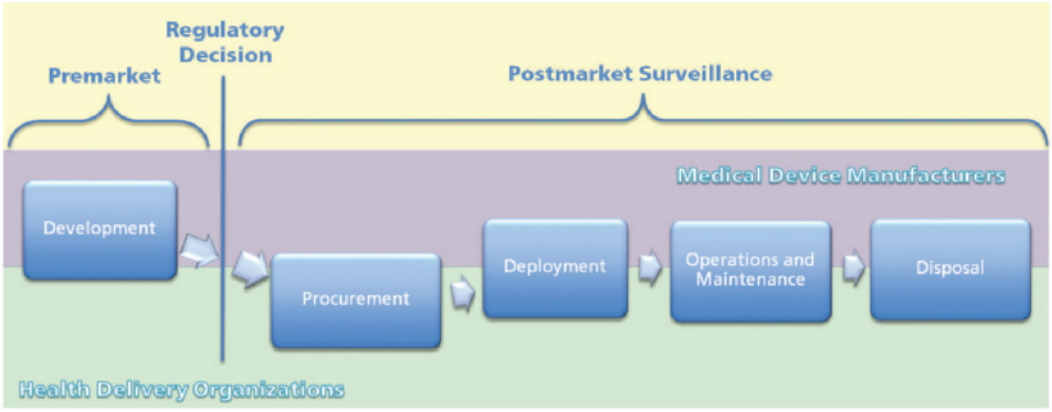


Figure 1. Medical device product life cycle

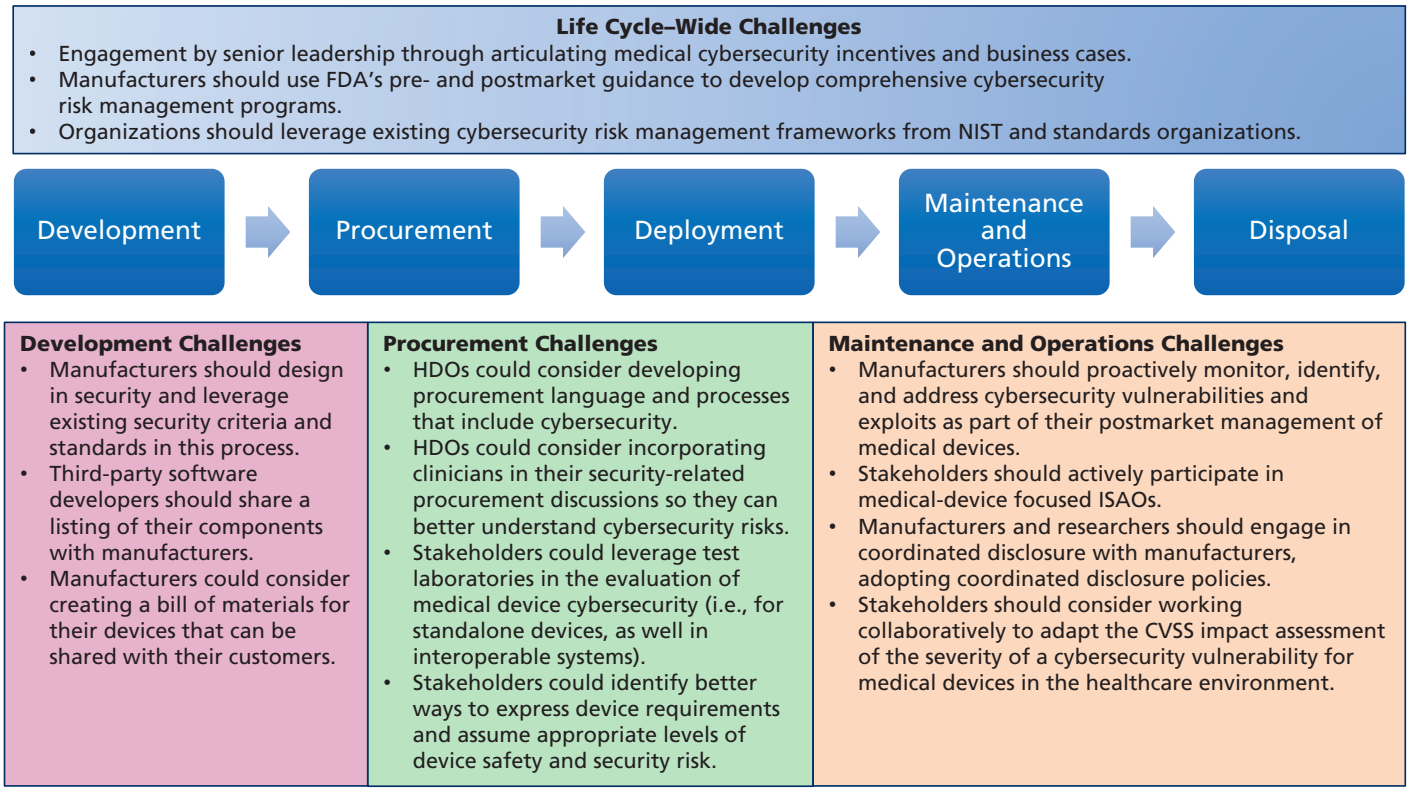


Figure 2. Summary of medical device cybersecurity life cycle challenges. Abbreviations used: CVSS, Common Vulnerability Scoring System; FDA, Food and Drug Administration; HDO, healthcare delivery organization; ISAO, Information Sharing and Analysis Organization; NIST, National Institute of Standards and Technology.

manage cybersecurity risk and protect patients from potential harm.

HDOs may wish to consider adoption of a systems engineering approach to better ensure secure medical device use and integration with electronic health records (EHRs), other medical devices, and broader hospital networks. Further, manufacturers and HDOs are encouraged to work together to ensure data are removed prior to medical device disposal.

Manufacturers and HDOs will benefit from a common high-level risk framework for security and safety. Cybersecurity is complicated, and many organizations (irrespective of size) have difficulty knowing where to start now that medical device cybersecurity is viewed through the lens of patient safety rather than solely being an information technology (IT) issue. Organizations cannot begin to address cybersecurity risks without understanding these concerns in context. Thus, a need exists for a common framework and lexicon to enable a coordinated approach to addressing cybersecurity challenges among manufacturers and HDOs. For medical devices, this includes considering misuse as well as intended use. Such a framework also would help make cybersecurity more accessible to less resourced manufacturers and HDOs.

Development

Several challenges occur during the device development phase. First, regulatory requirements and business needs often drive device design and development decisions, and these decisions have not always addressed cybersecurity.[1] Because devices historically have been standalone entities, little manufacturer emphasis was placed on cybersecurity. Meaningful use requirements in the United States, however, are driving device deployments into integrated network environments.[6] To design secure solutions, manufacturers need to raise their awareness of targeted customers' clinical environments and consider the ramifications of networked devices.

As is necessary in other domains,[7] collaboration between manufacturers and HDOs in the early stages of defining device requirements and design will help to ensure that manufacturers understand HDOs' needs and the healthcare environment in which the devices

will be deployed. As stated in FDA's final guidance (October 2014), manufacturers should also build medical devices by using a secure development life cycle that accounts for cybersecurity during the design and development stage.[1]

Many medical devices that are currently in use were designed, developed, and distributed years ago; they were not built from the ground up with cybersecurity as an essential design principle. These older medical devices implicitly trust inputs that contribute to cybersecurity challenges later in the life cycle.

The absence of cybersecurity testing also affects medical device readiness to operate within today's cybersecurity environment. For instance, manufacturers often have a well-defined approach for evaluating medical device safety and test medical devices using the FDA-guided concepts of "intended use" and "unintended misuse." However, this paradigm generally does not account for an environment with active cyber adversaries. Optimally, the development process would also scrutinize the supply chain of third-party components, including complete details regarding the origin, contents, and/or security of these embedded components. Manufacturers and HDOs are currently discussing methods to improve transparent and secure device management, including sharing of software bills of materials.

Procurement

Clinical needs drive medical device purchases. Ideally, the clinical engineering and/or IT departments (i.e., those responsible for device maintenance and network security) are engaged in HDO device procurement, especially for networked devices. However, limited clinician cybersecurity awareness or the absence of a centralized procurement process could enable insecure medical devices to jeopardize HDO networks, EHR data, and even patient safety.

Another challenge is the need for HDOs' clear expression of device cybersecurity requirements. The lack of a common framework to assess and assume appropriate levels of security and safety risk, to include the use of medical devices on HDO networks, exacerbates this challenge. Although manufacturers can offer the Manufacturer Disclosure Statement for Medical Device Security (MDS^2),[8] which describes medical device security and privacy properties, the form can be insufficient for fully conveying medical device security features. Articulating a set of minimum medical device cybersecurity requirements across the device life cycle, including testing focused on cybersecurity weaknesses, will give manufacturers and HDOs a common baseline to build, buy, and operate against. Device validation testing may be out of reach for some HDOs; thus, sharing testing insights is desired. However, nondisclosure restrictions may constrain sharing findings.

Operations and Maintenance

Secure medical device operation and maintenance differ from secure IT operation and maintenance. IT cybersecurity is more mature, and the relative homogeneity of IT systems permits patch management, vulnerability scanning, antivirus software, asset management, and more. This is not the case with medical devices, for which obtaining an accurate device inventory in a clinical facility setting may be nearly impossible. Older, deployed "legacy" devices are a particular challenge; these devices are black boxes offering minimal transparency.

Traditional cybersecurity maintenance, such as vulnerability scanning and patch management, often is not possible. Security solutions may be absent or custom-crafted by local manufacturer field service engineers, clinical facility IT, and/or clinical engineering staff. The ability to share these and other cybersecurity best practices, as well as device and third-party component vulnerability and threat information, among device users would greatly enhance communitywide cybersecurity maturity. However, historically, liability and intellectual property concerns have limited sharing within the healthcare community. The continuity of operations, as well as disaster recovery plans, in order to sustain device operation amid cybersecurity interruption or failure also need to be defined.

Cybersecurity researcher engagement with manufacturers is another operational challenge. Researchers often encounter pushback when trying to acquire a medical device or alert a manufacturer about a discovered medical device vulnerability. In turn, based on frustration with manufacturers, genuine concern for

Learn More Ways to Meet Cybersecurity Challenges

- AAMI TIR57:2016, *Principles for medical device security—Risk management* **http://my.aami.org**
- ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT networks incorporating medical devices* **https://my.aami.org**
- *Horizons*, fall 2017. **www.aami.org/horizons_cybersecurity**
- AAMI Podcast, episode 22: Patch Management in Healthcare **www.aami.org/podcasts**
- Fearsome Four in Cybersecurity (video) **www.aami.org/FearsomeFour**

patient safety, and/or a desire for publicity, researchers may go public with their findings before a mutually agreed-upon resolution with the manufacturer can be reached. A well-defined approach for cybersecurity researchers to identify medical device vulnerabilities, and for manufacturers to respond, will enable successful vulnerability resolution. At the time this article was written, 10 manufacturers had public-facing coordinated vulnerability disclosure policies,[9] and it would be beneficial for this practice to be more widely adopted.

The clinical community also plays an important role in secure medical device operation. Healthcare professionals interact with devices daily and may be the first to notice a medical device issue potentially resulting from a cybersecurity concern. However, these professionals may lack sufficient cybersecurity awareness.

Opportunities and Initiatives

Many efforts across the product life cycle are actively evolving medical device cybersecurity (Figure 3). Of note, the organizations and examples described in the following sections are not intended to be promotional; they simply reflect efforts that emerged during stakeholder interviews.

Life Cycle–Wide Opportunities and Initiatives

The U.S. government is proactively taking steps to help motivate device cybersecurity investment and improve cybersecurity resource accessibility for all device-related organizations.

The U.S. Cybersecurity Information Sharing Act (CISA)[10] encourages cybersecurity information sharing across government and industry to help safeguard U.S. critical infrastructure, including healthcare. To facilitate sharing, CISA espouses the use of Information Sharing and Analysis Organizations (ISAOs).[11] CISA also mandated the Department of Health & Human Services (HHS), the sector-specific agency for the healthcare and public health sector of critical Infrastructure, to establish a Healthcare Cybersecurity Task Force.[12] The task force was charged with analyzing the current state of cybersecurity in healthcare and

A well-defined approach for cybersecurity researchers to identify medical device vulnerabilities, and for manufacturers to respond, will enable successful vulnerability resolution.

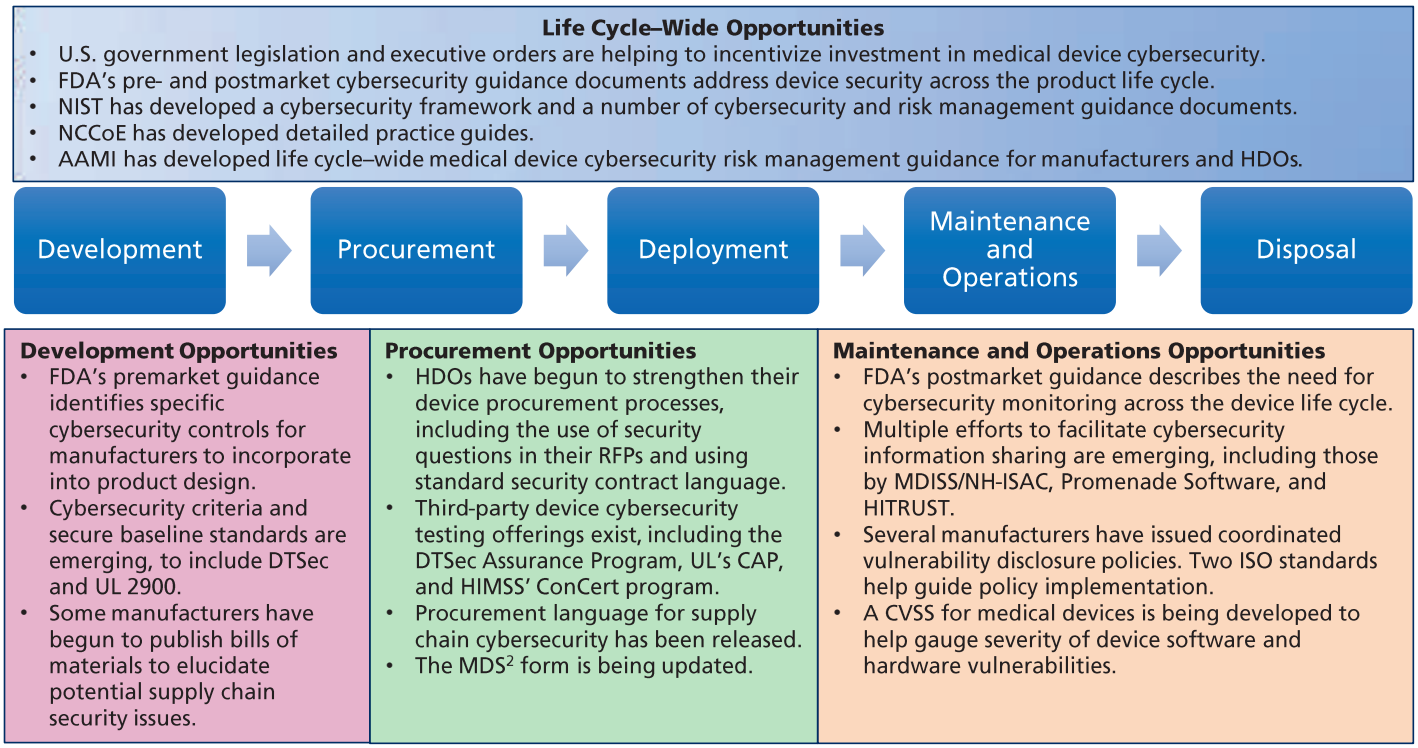


Figure 3. Summary of medical device cybersecurity life cycle opportunities. Abbreviations used: AAMI, Association for the Advancement of Medical Instrumentation; CAP, Cybersecurity Assurance Program; CVSS, Common Vulnerability Scoring System; DTSec, Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices; FDA, Food and Drug Administration; HDO, healthcare delivery organization; HIMSS, Healthcare Information and Management Systems Society; HITRUST, Health Information Trust Alliance; ISO, International Organization for Standardization; MDISS, Medical Device Innovation, Safety and Security Consortium; MDS², Manufacturer Disclosure Statement for Medical Device Security; NCCoE, National Cybersecurity Center of Excellence; NH-ISAC, National Health Information Sharing and Analysis Center; NIST, National Institute of Standards and Technology; RFP, request for proposal.

identifying recommendations for addressing gaps and challenges. Its report was released to Congress by HHS in June 2017.[13] The report incorporates analysis and recommendations for medical device cybersecurity.

The FDA, through its pre- and postmarket cybersecurity guidance, has underscored the importance and process of proactively addressing medical device cybersecurity threats and vulnerabilities. Regulatory reporting requirements are eased for manufacturers who meet certain criteria, such as participation in an ISAO.

Executive Order 13636[14] directed the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework[15] to help frame cybersecurity issues and provide a common lexicon for all critical infrastructure sectors. For more experienced users, NIST also offers broader risk and cybersecurity guidance documents.[16] In addition, NIST's National Cybersecurity Center of Excellence[17] has developed detailed practice guides for securing EHRs on mobile devices and for wireless medical infusion pumps.[18]

Beyond government, the Association for the Advancement of Medical Instrumentation (AAMI) has developed a life cycle–wide medical device security risk management technical information report (TIR)[19]; has adopted key standards published by the International Electrotechnical Commission (IEC), including IEC 80001-1:2010[20]; and has other work products in development.[21]

Development

Manufacturers need to build security into medical devices. FDA's premarket guidance identifies cybersecurity issues that manufacturers should consider in the design and development of medical devices. In particular, the guidance emphasizes that specific controls that address cybersecurity should be incorporated into the product design and that both intentional and unintentional cybersecurity risk should be evaluated. Efforts to define security baselines that manufacturers could incorporate into their design and development are also established or underway.[22] Although not endorsements, examples of these efforts include the following:

- AAMI is developing a new security standard applicable to the entire life cycle, SW96/Ed. 1, *Medical Devices—Application of security risk management to medical devices*.[23]
- The international cybersecurity standard Common Criteria (ISO/IEC 15408)[24] is the basis for the Diabetes Technology Society (DTS) Cybersecurity Standard for Connected Diabetes Devices (DTSec).[25] (Note: DTS is not an American National Standards Institute [ANSI] Accredited Standards Developer. The referenced document [DTSec] was not developed using a consensus process compliant with ANSI requirements [see *ANSI Essential Requirements: Due process requirements for American National Standards*[26]]. DTSec has not been recognized by the FDA.)
- UL's Cybersecurity Assurance Program (CAP)[27] contains UL 2900 standards that specify testable cybersecurity criteria for network-connectable systems.

The transparency of embedded third-party software also is essential for managing overall medical device cybersecurity risk. Although it has not been widely adopted, a manufacturer has publicly committed to publishing bills of materials for its devices to better inform HDOs of potential risks.[28]

Procurement

HDOs are starting to exert more influence over their device procurement process. The Mayo Clinic, for instance, incorporates security questions in its requests for proposals and uses standard security contract language.[29] Preacquisition device cybersecurity assessment also is growing. From a technical standpoint, no consensus exists that a point-in-time "certification" from a laboratory is effective in reducing cybersecurity risk, particularly for complex medical devices, and addressing emerging risk is difficult under these models. Besides in-house testing at some HDOs, testing bodies have begun to address this need. A few efforts that arose during the course of the stakeholder interviews included:

- DTSec's assurance program has two approved laboratories that independently evaluate devices against its cybersecurity standard.
- UL's CAP performs testing against its 2900 criteria and has a formalized agreement with the Department of Veterans Affairs to enhance the UL 2900 series for testing medical devices.[30] (Note: UL 2900-1 is

A Look at AAMI SW96/Ed. 1

The forthcoming AAMI standard, SW96/Ed. 1, *Medical Devices—Application of security risk management to medical devices*, will seek to provide the required steps and processes expanded upon in the guidance of AAMI TIR57:2016, *Principles for medical device security — Risk management*.

Together, these two companion documents aim to provide the impact and guidance found in ANSI/AAMI/ISO 14971, *Medical devices—Application of risk management to medical devices*, and ANSI/AAMI/ISO TIR 24971, *Medical devices—Guidance on the application of ISO 14971*, by leveraging the core principles of risk management and applying a device security lens to it.

SW96/Ed. 1 is scheduled to be published in 2020.

currently recognized by FDA. Recognition of this standard is not intended as an endorsement of the UL CAP program or to indicate that devices that complete UL 2900 testing are fit for FDA clearance or approval.)
- The Health Information and Management Systems Society's ConCert[31] tests and certifies healthcare component interoperability; a pilot effort added cybersecurity to its interoperability testing.

Although the above list may not be exhaustive, these efforts were commonly mentioned during the stakeholder study. These models have value, and we encourage those involved in other efforts to reach out to MITRE and FDA. Other efforts to improve the procurement process include procurement language for supply chain cybersecurity[32] and an effort to update the MDS[2] form.

Operations and Maintenance

Several device cybersecurity initiatives that are underway fall into the "operations and maintenance" phase, as described below.

Postmarket guidance. FDA's postmarket guidance focuses on deployed device cybersecurity and emphasizes that manufacturers should proactively monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices. AAMI SM/WG05 also is developing a new postmarket TIR (TIR97) to aid manufacturers.[33]

Medical device vulnerability information sharing. Several efforts to share medical device vulnerability information, enabling proactive community mitigation of operational device cybersecurity issues, are emerging. For example, the National Health Information Sharing and Analysis Center and the Medical Device Innovation, Safety & Security Consortium have signed a memorandum of understanding with FDA and established a Medical Device Security Information Sharing Council to serve as an umbrella for several initiatives, including standing up an ISAO and conducting medical device risk assessments.[34]

Promenade Software, a medical device software developer, recently established MedISAO.[35] In addition, the private Health Information Trust Alliance shares healthcare cyberthreat intelligence, including compromise indicators.[36]

Coordinated vulnerability disclosure policies. The FDA postmarket guidance also encourages manufacturers to adopt coordinated vulnerability disclosure policies to enable positive engagement with cybersecurity researchers. The guidance tries to balance competing needs: informing device users in a timely manner and giving manufacturers the necessary time to assess identified vulnerabilities and to respond effectively. Two FDA-recognized International Organization for Standardization standards are available to help guide implementation,[37,38] and several manufacturers have adopted coordinated vulnerability disclosure policies.[9]

Common vulnerability scoring system for medical devices. The Common Vulnerability Scoring System (CVSS) is an open standard for assessing the severity of software vulnerabilities, enabling threat-appropriate responses and resources.[39] Initially released in 2005 and managed by the computer incident response consortium FIRST,[40] CVSS (version 3) is in widespread use internationally. However, as CVSS was not calibrated for the healthcare environment, current application against medical device vulnerabilities may result in an inaccurate score. To remedy this, MITRE, in collaboration with stakeholders, is developing a rubric that will guide manufacturers, HDOs, and cybersecurity researchers in generating consistent CVSS vectors and scores. The goal is to have this rubric qualified as a Medical Device Development Tool by the FDA to help the community develop more useful risk metrics that also can be supplied as regulatory evidence to the FDA.

Summary

The imperative of cybersecurity in medical devices is no longer a topic of debate. Stakeholders across the healthcare sector must understand the importance of medical device cybersecurity for protecting patient safety, provider networks, and the sensitive data that they access. Rather than imposing onerous regulations, FDA has opted to convene and encourage various medical device stakeholders to work together to generate workable cyber solutions. This approach has borne, and continues to bear, fruit as diverse community members put aside their differences in the interest of patient safety and collaborate in

Rather than imposing onerous regulations, FDA has opted to convene and encourage various medical device stakeholders to work together to generate workable cyber solutions.

closing medical device cybersecurity gaps. Recognizing that medical device cybersecurity is a global public health concern, increased collaboration across borders also is needed. ■

References

1. **Department of Health & Human Services.** *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.* Available at: www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf. Accessed Dec. 6, 2017.
2. **Department of Health & Human Services.** *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.* Available at: www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. Accessed Dec. 6, 2017.
3. **Food and Drug Administration.** Public Workshop: Collaborative Approaches for Medical Device and Healthcare Cybersecurity, October 21-22, 2014. Available at: http://wayback.archive-it.org/7993/20170111083032/http:/www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm. Accessed Dec. 6, 2017.
4. **Food and Drug Administration.** Public Workshop: Moving Forward: Collaborative Approaches to Medical Device Cybersecurity, January 20-21, 2016. Available at: www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm474752.htm. Accessed Dec. 6, 2017.
5. **Food and Drug Administration.** Public Workshop: Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis, May 18-19, 2017. Available at: www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm549732.htm. Accessed Dec. 6, 2017.
6. **Department of Health & Human Services.** Standards & Certifications Criteria Final Rule. Available at: www.healthit.gov/policy-researchers-implementers/standards-certifications-criteria-final-rule. Accessed Dec. 6, 2017.
7. **Department of Health & Human Services.** *Applying Human Factors and Usability Engineering to Medical Devices: Guidance for Industry and Food and Drug Administration Staff.* Available at: www.fda.gov/downloads/MedicalDevices/.../UCM259760.pdf. Accessed Dec. 6, 2017.
8. **Healthcare Information and Management Systems Society.** Manufacturer Disclosure Statement for Medical Device Security (MDS²). Available at: www.himss.org/resourcelibrary/MDS2. Accessed Dec. 6, 2017.
9. **Iamthecavalry.org.** Known Disclosure Programs. Available at: www.iamthecavalry.org/resources/disclosure-programs. Accessed Dec. 6, 2017.
10. **Library of Congress.** S.754: Cybersecurity Information Sharing Act of 2015. Available at: www.congress.gov/114/bills/s754/BILLS-114s754es.pdf. Accessed Dec. 6, 2017.
11. **Department of Homeland Security.** Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs). Available at: www.dhs.gov/isao-faq. Accessed Dec. 6, 2017.
12. **Department of Health & Human Services.** Health Care Industry Cybersecurity Task Force. Available at: www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx. Accessed Dec. 6, 2017.
13. **Department of Health & Human Services.** *Report on Improving Cybersecurity in the Health Care Industry.* Available at: www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf. Accessed Dec. 6, 2017.
14. **The White House: President Barack Obama.** Executive Order: Improving Critical Infrastructure Cybersecurity. Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Accessed Dec. 6, 2017.
15. **National Institute of Standards and Technology.** Cybersecurity Framework: Latest Updates. Available at: www.nist.gov/cybersecurity-framework. Accessed Dec. 6, 2017.
16. **National Institute of Standards and Technology.** Search Publications: Topic Area: "Cybersecurity." Available at: www.nist.gov/publications/search?term_node_tid_depth%5B%5D=248731. Accessed Dec. 6, 2017.
17. **National Cybersecurity Center of Excellence.** Homepage. Available at: https://nccoe.nist.gov. Accessed Dec. 6, 2017.
18. **National Cybersecurity Center of Excellence.** Healthcare Sector. Available at: https://nccoe.nist.gov/projects/use-cases/health-it. Accessed Dec. 6, 2017.

19. **AAMI TIR57:2016.** *Principles for medical device security—Risk management*. Arlington, VA: Association for the Advancement of Medical Instrumentation.

20. **ANSI/AAMI/IEC 80001-1:2010.** *Application of risk management for IT Networks incorporating medical devices*. Arlington, VA: Association for the Advancement of Medical Instrumentation.

21. **Association for the Advancement of Medical Instrumentation.** Projects. Available at: https://standards.aami.org/higherlogic/ws/public/projects. Accessed Dec. 6, 2017.

22. **Food and Drug Administration.** Recognized Consensus Standards. Available at: www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm. Accessed Dec. 6, 2017.

23. **AAMI SW96/Ed. 1.** *Medical Devices—Application of security risk management to medical devices*. Arlington, VA: Association for the Advancement of Medical Instrumentation. In progress.

24. **Common Criteria Recognition Arrangement Members.** Common Criteria. Available at: www.commoncriteriaportal.org. Accessed Dec. 6, 2017.

25. **Diabetes Technology Society.** DTS Cybersecurity Standard for Connected Diabetes Devices. Available at: www.diabetestechnology.org/dtsec.shtml. Accessed Dec. 6, 2017.

26. **American National Standards Institute.** *ANSI Essential Requirements: Due process requirements for American National Standards*. Available at: https://standards.ieee.org/about/sasb/audcom/ansi_essreq.pdf. Accessed Feb. 2, 2018.

27. **UL.** *Cybersecurity Assurance Program (CAP) for network-connectable products & systems addresses security concerns*. Available at: https://industries.ul.com/wp-content/uploads/sites/2/2016/04/UL_CAP-Overview-Info.pdf?_ga=1.33727657.904562875.1491326790. Accessed Dec. 6, 2017.

28. **McNeil MC.** Medical Device Cybersecurity: Overcoming Challenges to Effective Information Sharing. Available at: www.himssconference.org/sites/himssconference/files/pdf/MD1.pdf. Accessed Dec. 6, 2017.

29. **Hudson FD.** Biomedical Device Security: New Challenges and Opportunities. Available at: https://nchica.org/wp-content/uploads/2015/06/Bruemmer-Hudson-Wirth.pdf. Accessed Dec. 6, 2017.

30. **FCW.** VA taps UL for medical device cybersecurity. Available at: https://fcw.com/articles/2016/06/17/va-ul-medical-cyber.aspx. Accessed Dec. 6, 2017.

31. **ICSA Labs.** ConCert by HIMSS: Overview. Available at: www.icsalabs.com/technology-program/concert-himss. Accessed Dec. 6, 2017.

32. **Synopsys.** *Procurement Language for Supply Chain Cyber Assurance*. Available at: http://globalforum.items-int.com/gf/gf-content/uploads/2016/10/Jarzombek-Procurement-Language-SCM.pdf. Accessed Dec. 6, 2017.

33. **AAMI TIR97/Ed. 1.** *Principles for medical device security—Post-market security management for device manufacturers*. Arlington, VA: Association for the Advancement of Medical Instrumentation. In progress.

34. **National Health Information Sharing and Analysis Center.** NH-ISAC and MDISS Partner to Form Medical Device Security Information Sharing Initiative. Available at: https://nhisac.org/announcements/nh-isac-and-mdiss-partner-to-form-medical-device-security-information-sharing-initiative. Accessed Dec. 6, 2017.

35. **Business Wire.** Promenade Software Launches MedISAO: Sharing Cybersecurity Information within the Medical Device Community. Available at: www.businesswire.com/news/home/20170118005332/en/Promenade-Software-Launches-MedISAO-–-Sharing-Cybersecurity. Accessed Dec. 6, 2017.

36. **HITRUST.** Cyber Threat XChange (CTX). Available at: https://hitrustalliance.net/cyber-threat-xchange. Accessed Dec. 6, 2017.

37. **International Organization for Standardization.** ISO/IEC 30111:2013: *Information technology—Security techniques—Vulnerability handling processes*. Available at: www.iso.org/standard/53231.html. Accessed Dec. 6, 2017.

38. **International Organization for Standardization.** License Agreement for standards made available through the ITTF web site. Available at: http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip. Accessed Dec. 6, 2017.

39. **FIRST.** Common Vulnerability Scoring System SIG. Available at: www.first.org/cvss. Accessed Dec. 6, 2017.