The Role of Healthcare Technology Management in Facilitating Medical Device Cybersecurity

Mike Busdicker and Priyanka Upendra

Abstract: This article discusses the role of healthcare technology management (HTM) in medical device cybersecurity and outlines concepts that are applicable to HTM professionals at a healthcare delivery organization or at an integrated delivery network, regardless of size. It provides direction for HTM professionals who are unfamiliar with the security aspects of managing healthcare technologies but are familiar with standards from The Joint Commission (TJC). It provides a useful set of recommendations, including relevant references for incorporating good security practices into HTM practice. Recommendations for policies, procedures, and processes referencing TJC standards are easily applicable to HTM departments with limited resources and to those with no resource concerns. The authors outline processes from their organization as well as best practices learned through information sharing at AAMI, National Health Information Sharing and Analysis Center (NH-ISAC), and Medical Device Innovation, Safety, and Security Consortium (MDISS) conferences and workshops.

In May 2017, The Ponemon Institute shared the findings of a survey that showed only 15% of healthcare delivery organizations (HDOs) and 17% of medical device manufacturers (MDMs) were taking significant steps to prevent cyberattacks.[1] A majority of them responded that an attack is likely in the next year (Figure 1), yet only 22% of HDOs and 41% of MDMs have an incident response plan in place in the event of an attack on vulnerable medical devices.[1] This report surveyed 500 people who work actively in medical device security. Today, cyberattacks threaten to go beyond stealing confidential patient information. The situation has reached a point where patients and caregivers can be harmed.

May and June 2017 also saw worldwide cyberattacks by WannaCry and Petya ransomwares. These attacks targeted systems running on Microsoft Windows operating systems. The WannaCry cryptoworm affected more than 300,000 systems across 150 countries

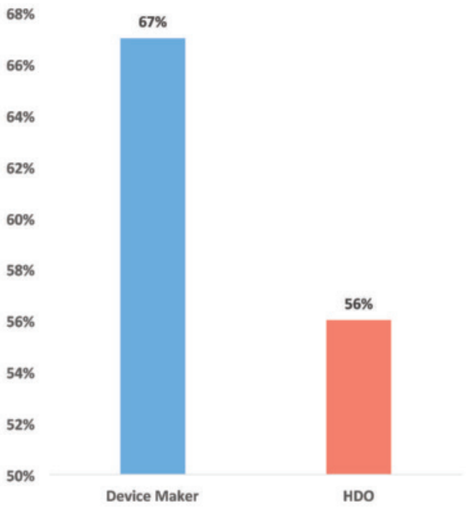

Figure 1. Results from a Ponemon Institute survey asking device makers and healthcare delivery organizations (HDOs) how likely an attack on their medical devices is in the next 12 months. Source: reference 1.

About the Authors

Mike Busdicker, MBA, CHTM, is the system director of Clinical Engineering Support Services at Intermountain Healthcare in Midvale, UT. Email: mike.busdicker@imail.org

Priyanka Upendra, BSBME, MSE, CHTM, is the compliance manager of Clinical Engineering Support Services at Intermountain Healthcare in Midvale, UT. Email: priya.upendra@imail.org

Healthcare Delivery Organization or Integrated Delivery Network?

- **Healthcare delivery organization (HDO).** A HDO is an organization, or a group of related organizations, that are involved with the delivery of healthcare services. A hospital is an example of an HDO, as are a group of physician practices acting in concert in an area.[4]
- **Integrated delivery network (IDN).** According to the Advisory Board, an IDN "is a formal system of providers and sites of care that provides both healthcare services and a health insurance plan to patients in a defined geographic area. The functionalities included in an IDN vary, but can include acute care, long-term health, specialty clinics, primary care, and home care services—all supporting an owned health plan."[5]

An IDN is a network of HDOs under a parent holding company that shares a vision and mission of improving the quality of care and patient satisfaction. This alignment positions IDN members to negotiate competitive payer contracts, physician relationships, and enhanced supplier relationships and to drive contract compliance for products and services by leveraging the combined influence and buying power of the entire group.[6]

by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.[2] The Petya malware affected systems by encrypting the hard drive's file system, preventing Windows from booting, and demanding payments in Bitcoin to regain access to the system.[3]

According to the Food and Drug Administration (FDA), a medical device is "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

- Recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
- Intended for use in the diagnosis of disease of other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
- Intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes."[7]

In this article, a connected medical device is defined as any medical device that possesses HDO network or Internet connectivity, is connected to an external storage device or external media (e.g., USB, compact disc), or has any other cyber capability. Because the protection of local data is important for mobile medical devices, this article will also consider medical devices that can store data internally but are not connected to the HDO network or Internet.

Common connected medical device types include:

- **Diagnostic** (e.g., blood analyzers, virus detection systems, immuno-assays, electrocardiographs, ultrasound systems)
- **Monitoring** (e.g., physiological monitors, weighing scales, ventilators, heart rate monitors)
- **Therapeutic** (e.g., infusion pumps, anesthesia units, pacemakers, dialysis units)

Healthcare technology management (HTM) departments in a HDO or integrated delivery network (IDN) face a daunting task of managing numerous service offerings (Figure 2). This includes[8]:

- **Strategic planning** of healthcare technology acquisition and replacement.
- **Clinical consultation and education** on the safe and effective use of healthcare technology.
- **Effective maintenance of healthcare technology** through in-house expertise and service contracts.
- **Disaster preparedness** and other issues that impact patient safety.
- Ensuring hospital **compliance with accreditation surveys and other regulations.**

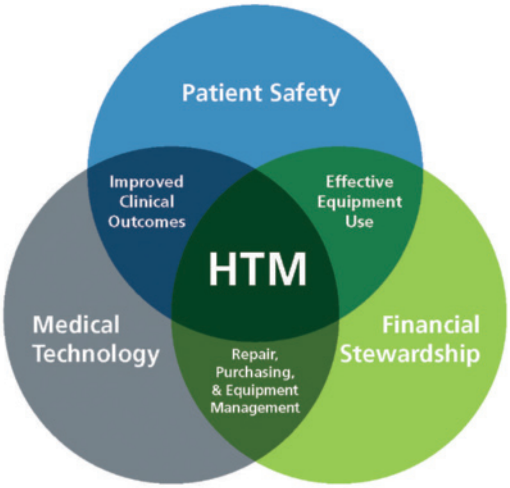

Figure 2. The overlapping roles of the healthcare technology management (HTM) profession. Source: reference 8.

Operationalizing Cybersecurity in HTM

Environment of Care (EC) standards established by The Joint Commission (TJC) require HDOs to develop a plan to manage the risks associated with provisions of care, treatment, and services.[9] One such functional area concerns the use of medical devices for patient care. The standards established in this area promote a safe, functional, and supportive environment within a HDO so that quality and safety are preserved.[9] HTM departments and, in some cases, independent service organizations manage medical devices and the associated risks.

A large percentage of HTM departments inspect, maintain, and repair general biomedical equipment, (e.g., infusion pumps, physiological monitors, weighing scales, ventilators, anesthesia units, electrocardiograms, electroencephalograms, warmers, incubators). Some HTM departments manage diagnostic and therapeutic imaging equipment (e.g., ultrasound systems, computed tomography scanners, magnetic resonance imaging systems, linear accelerators) through full or shared service agreements with MDMs or authorized service providers (ASPs). Laptops, computers, servers, and other information systems associated with the medical devices are also often managed by the MDM, ASP, or through a shared agreement among the MDM, ASP, and the organization's information technology (IT) department.

HTM and IT departments operating within an HDO or IDN must lay a strong foundation for managing cybersecurity risks in the medical device ecosystem. The following actions are essential:

- Improve the processes pertaining to the identification and validation of medical devices used for patient care
- Improve the life cycle management procedures and processes used to review and manage cybersecurity risks
- Accurately inventory, categorize, classify, and remediate medical device cybersecurity risks
- Harden the cybersecurity of medical devices through identification and implementation of common cybersecurity controls
- Establish contractual arrangements that obligate vendors to deliver on their security, quality, and compliance commitments
- Maintain proper change control procedures throughout the system life cycle
- Build relationships with partners and members in the healthcare community to foster information sharing as related to medical device security

An effective approach to achieving these essential actions is enhancing the medical equipment management plan as established in EC.01.01.01 with cybersecurity concepts. The policies and procedures that support the HTM department should incorporate cybersecurity aspects throughout the life cycle of the medical device: during planning and procurement; inspection, inventory, and documentation; commissioning and acceptance; ongoing operation and monitoring of use; and performance, maintenance, and decommissioning. Effective life cycle management processes serve as a foundation to build cybersecurity risk management processes uniformly and holistically.

HTM and IT departments operating within an HDO or IDN must lay a strong foundation for managing cybersecurity risks in the medical device ecosystem.

The Importance of Knowledge in a Changing Landscape

In the past, HTM professionals were not required to learn about cybersecurity or work in the information system security domain. That has changed in the past few years. HTM professionals are now asked to learn networking and cybersecurity concepts and to apply them when managing healthcare technologies. To keep up with this changing landscape, HTM leadership should make sure their staff are versed in networking and cybersecurity concepts. This includes working knowledge of the Health Insurance Portability and Accountability Act privacy and security rule,[10] networks and servers, security controls from the National Institute of Standards and Technology (NIST), implementation of network segmentation, scanning of medical devices on the network, and so on.

Security concepts should be introduced to HTM professionals and clinical caregivers in the following policies, procedures, and processes:

- **Medical equipment inventory policy.** Gives a high-level view of the inventory process, documentation of equipment records in the computerized maintenance management system (CMMS), maintenance strategies for equipment regardless of its ownership type, and collection and documentation of network information.
- **Medical equipment inspection procedure.** Describes the process for proper receipt and inspection of medical equipment prior to initial use. It also outlines the receipt of cybersecurity documentation and completion of a cybersecurity risk assessment before the initial use.
- **Medical equipment maintenance procedure.** Discusses when and how major inspection and preventive maintenance (IPM) on medical and participant equipment is performed and documented. This procedure also discusses the inclusion of cybersecurity controls in the IPM protocol based on the cybersecurity risk assessment, as mentioned in the medical equipment inspection procedure.
- **Medical equipment disposition procedure.** Explains how to properly dispose of medical equipment. This procedure also stresses the importance of media sanitization as outlined in NIST 800-88, *Guidelines for Media Sanitation,*[11] and Department of Defense 5220.22-M, *National Industrial Security Program Operating Manual.*[12]
- **Alert recall policy.** Discusses the timely removal, service, quarantine, or replacement of medical device products and supplies due to an FDA or manufacturer recall or alert. The same process is followed for advisories that are posted on Industrial Control Systems Cyber Emergency Response Team or shared through National Health Information Sharing and Analysis Center alerts and Medical Device Innovation, Safety, and Security Consortium councils.

HTM professionals should be trained to obtain the IT/network information from the medical devices. This information should be documented in the CMMS.

Effective Risk Management and Mitigation

For hospitals that use TJC accreditation for deemed status purposes, EC.02.04.01, EP2 provides guidance on managing risks associated with medical equipment. It is necessary to maintain a written inventory of all medical devices. As specified in EC.02.04.03, EP1, the hospital should perform safety, operational, and functional checks before initial use of the medical device. HTM departments should use this standard as an opportunity to modify their inventory policy and inspection procedure, train their technicians and engineers to document the IT- and network-related information in the CMMS, and perform checks to ensure adequate security controls are in place.

A basic course in cybersecurity is a good place to start. HTM professionals should familiarize themselves with IT's service management and cybersecurity management processes. They should be familiar with the organizational structure within IT and the go-to people for medical device integration, biomedical-device interface support, cybersecurity, identity and access management, and the security operations center. If the organization lacks an on-site IT team, then HTM should still become familiar with whom they should work on IT-related issues.

HTM professionals should be trained to obtain the IT/network information from the medical devices. This information should be documented in the CMMS:

- Underlying operating system
- Network capability (wired or wireless; if wireless, include the type of wireless protocol)
- Software and firmware version levels
- MAC (media access control) address

- Host name
- Internet Protocol (IP) configuration
- IP address for medical devices that are not mobile
- Device-associated IT components or parts

Documenting this information increases HTM's visibility and knowledge of the devices that are present in the health IT environment, helps in the assessment of cybersecurity risks, and helps bridge the gap among asset management, HTM, and IT. This information is useful to various teams within IT, who can use it when monitoring activity on the hospital network, communicating with outside IPs, scanning devices that are connected to the hospital network, and more.

EC.02.04.01, EP 3-7 and EC.02.04.03, EP 2-5 provide guidance on identifying risks, activities, and frequencies to maintain, inspect, and test medical devices in the environment of care. In addition to classifying the risk inclusion factor or asset criticality in the CMMS to be compliant with these standards, HTMs should include cybersecurity risk assessments when risk inclusion factor is evaluated. These cybersecurity risk assessments at a minimum should include evaluation of the MDS2 (Manufacturer Disclosure Statement for Medical Device Security) form. Quantitative and qualitative risk analyses should be performed to discover cybersecurity control gaps and to establish effective risk mitigation or management plans. These plans do not alter the manufacturer-recommended maintenance or testing activities; instead, they are in place to enhance the safety and quality of the medical device.

The risk mitigation or management plan should include five core activities:

1. **Identification of the risks.** Risks are identified by reviewing the cybersecurity documentation provided by the medical device manufacturer and the clinical caregiver who is using the healthcare technology for patient care. Many HDOs and IDNs use the Medical Device Risk Assessment Platform to perform risk assessment on connected medical devices. The scoring results from this assessment can be used for a deeper dive into the application and management of controls.

Many HDOs and IDNs use the Medical Device Risk Assessment Platform to perform risk assessment on connected medical devices.

2. **Application of common controls.** Based on the risk assessment and scoring results, cybersecurity and HTM teams can work with the MDMs to apply common security controls as the medical device will support.
3. **Identification of control gaps.** The risk assessment will help identify the control gaps. These must be documented and readily available for audit purposes.
4. **Application of compensating controls.** For medical device cybersecurity management, compensating controls need to be applied without causing problems in clinical workflow. Organizations need to look at alternatives if the controls are not supported and/or if they obstruct the device's intended performance. Exception requests need to be documented according to the organization's cybersecurity management processes. That way, the controls in the medical device are evaluated on a routine basis.
5. **Management of residual and uncontrolled risks.** This should be a continuous process throughout the life cycle of the medical device.

HTM and IT should plan a strategy with the medical device manufacturer if a medical device is no longer supported or has been depreciated by the manufacturer or the creator of the device's software.

Using an "All Hands on Deck" Approach

HTM and IT teams should work with the entities externally (e.g. the MDM or ASP) and internally (e.g., supply chain, legal, clinical users, the business owner) to understand how the medical device is used in a patient care setting. A multidisciplinary approach allows HTM to evaluate all aspects that support safety, confidentiality, integrity, and availability of the medical device. This is also very useful when procurement decisions are being made and service agreements are being reviewed. If the organization decides to go ahead with purchasing a new medical device with inadequate security controls, these risk mitigation or management plans should be included as additional checks during a maintenance procedure (scheduled and unscheduled).

In accordance with FDA guidance released on Dec. 28, 2016, *Postmarket Management of Cybersecurity in Medical Devices*, medical device software, operating systems, and other components should receive cybersecurity updates and patches in a timely manner.[13] Appropriate patch management strategies should be discussed with the MDM or ASP, included as part of maintenance procedures, and be a part of the service contract if the device is being serviced by the MDM or ASP. In addition, HTM and IT should plan a strategy with the MDM if a medical device is no longer supported or has been depreciated by the MDM or the creator of the device's software.

EC.02.04.01, EP 9 mandates that hospitals maintain written procedures to follow when medical equipment fails. In addition to aspects of clinical interventions and availability of backup equipment, HTM teams should develop an incident response plan in the event of a cyberattack on vulnerable medical devices in their inventory. The information systems department in a HDO or IDN must have an information systems security incident response procedure as required in 45 Code of Federal Regulations 164.308, *Administrative Safeguards*.[14] This procedure outlines how the HDO or IDN responds to and tracks information security incidents appropriately and consistently to mitigate harm and minimize future incidents. HTM professionals need to train with information systems security personnel and also participate in table-top exercises. This will allow HTM teams to be ready during such an incident.

Medical device security plays a critical role during equipment planning. HTM and IT should be included during capital acquisition or capital review discussions. Devices running software that is no longer supported or used should be upgraded prior to the official end of support of the software component. If the medical device cannot be patched or updated to remediate a known security vulnerability, HTM and IT should collect appropriate documentation from the MDM. Legal, IT, and compliance departments should review these instances and assess the potential risks. The document from the MDM should state the reasons why the patch or update would invalidate the FDA approval(s) or cause patient safety concerns. This information should then be recorded in the CMMS. This document must be readily available when reviewing exception requests and during equipment replacement planning.

Protecting Data When Disposing of a Device

Effective disposal of medical devices ensures that patient data collected during the device's life cycle remains confidential. This includes securely wiping or destroying residual data on the medical device prior to discarding, selling, or otherwise relinquishing physical control of the device. Appropriate methods to sanitize the data should be outlined in a medical device disposition or decommissioning policy. This may include physical destruction of any components that can store data or using of secure wipe techniques described in NIST 800-88[11] or DOD 5220.22M.[12] HTM is responsible for collecting this documentation and recording it in the CMMS. This applies even when devices are being transferred and moved between facilities and in and out of them for service operations at the MDM or ASP site.

All records of security controls, patch updates, and data destruction should be recorded for audit purposes. The appropriate length of log retention is defined in the medical device disposition or decommissioning policy. Logs must be kept and should contain the following, at a minimum:

- Medical device asset identifier
- Date of secure wipe
- Name of technician or engineer (or MDM or ASP) performing the data destruction
- Reason for data destruction
- Method of data destruction
- Outcome of data destruction and/or the disposition process

The WannaCry and Petya ransomware attacks, among others, have increased attention for ensuring that connected medical devices are secure. With the advances in technology and advent of electronic health records (EHRs), medical devices no longer exist in a vacuum. Increased EHR adoption by providers, a need for integration, and connectivity tools to improve clinical workflow, patient care solutions, and overall hospital operations will continue to drive rapid growth in the connected medical device market. Going forward, the call will only get louder for HDOs and MDMs to upgrade their health IT infrastructure and improve their design and development methodologies. HTM will play a critical role in this cybersecurity future. ■

References

1. **Ponemon Institute.** Medical Device Security: An Industry Under Attack and Unprepared to Defend. Available at: www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf. Accessed Sept. 28, 2017.

2. **Larson S.** Why Hospitals Are So Vulnerable to Ransomware Attacks. Available at: http://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html. Accessed Sept. 28, 2017.

3. **Kaspersky Lab Daily.** New Petya/NotPetya/ExPetr Ransomware Outbreak. Available at: www.kaspersky.com/blog/new-ransomware-epidemics/17314. Accessed Sept. 28, 2017.

4. **KEMP Application Delivery.** Health Delivery Organization (HDO). Available at: https://kemptechnologies.com/glossary/health-delivery-organization-hdo. Acessed Sept 28, 2017.

5. **Advisory Board.** Post-Acute Care Cheat Sheet: Integrated Delivery Networks. Available at: www.advisory.com/research/post-acute-care-collaborative/members/resources/cheat-sheets/integrated-delivery-networks. Accessed Sept. 28, 2017.

6. **Healthcare Market.** Why is the Integrated Delivery Network one of your keys to success in Healthcare? Available at: www.paho.org/blz/index.php?option=com_docman&view=download&alias=206-why-is-integrated-delivery-networks-a-success&category_slug=technical-documentation&Itemid=250. Accessed Sept. 28, 2017.

7. **Food and Drug Administration.** What Is A Medical Device? December 28, 2015. Available at: www.fda.gov/aboutfda/transparency/basics/ucm211822.htm

8. **Association for the Advancement of Medical Instrumentation.** HTM: A Critical Role in Healthcare Delivery. Available at: http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/HTM/AAMI_HTM_GENERAL_low.pdf. Accessed Sept. 28, 2017.

9. **The Joint Commission.** Comprehensive Accreditation Manual for Hospitals: Environment of Care. January 2017. Available at: www.jcrinc.com/2017-comprehensive-accreditation-manuals/2017-comprehensive-accreditation-manual-for-hospitals-camh-. Accessed Sept. 28, 2017.

10. **Department of Health & Human Services.** The Security Rule. Available at: www.hhs.gov/hipaa/for-professionals/security/index.html. Accessed Sept. 28, 2017.

11. **NIST 800-88.** *Guidelines for Media Sanitation*. Gaithersburg, MD: National Institute of Standards and Technology; 2006.

12. **DOD 5220.22M.** *National Industrial Security Program Operating Manual*. Washington, DC: Department of Defense; 2006.

13. **Department of Health & Human Services.** *Postmarket Management of Cybersecurity in Medical Devices*. Silver Spring, MD: Food and Drug Administration; 2016.

14. **Department of Health & Human Services.** 45 CFR 164.308. Available at: www.gpo.gov/fdsys/pkg/CFR-2009-title45-vol1/pdf/CFR-2009-title45-vol1-sec164-308.pdf. Accessed Sept. 28, 2017.