Gathering Basic Information in Support of Medical Network Risk Management

Scot Copeland

In addition to “privacy” risks related to the protection of electronic protected health information (ePHI), healthcare technology management (HTM) professionals are presented with operational “security” risks related to patient safety and network security. For instance, we must be concerned with the privacy of the ePHI that may be stored inside a medical device, as well as with systems that may relay alarm data through annunciation and communication devices and provide physiological data to the electronic health record (EHR). Further, a medical device can have network security vulnerabilities that can place other network devices (both information technology [IT] and medical) at risk. A vulnerable medical device with an Internet connection can become compromised by an attacker or malware and used as a pivot point to begin attacking network resources horizontally, from inside the network.

Consider an integrated drug delivery system that programs and monitors an infusion pump: Something as small as a decimal point error can cause lethal dose changes. An attacker with access to a drug library or order entry application in a pharmacy system or interfaces could perform any number of malicious tasks that could be life-threatening in a clinical environment. Networking technology and mobile device integrations allow caregivers to be alerted and respond to patient situations, both common and critical. Malware in a mobile device alarm/alert integration could undetectably cause any number of failure modes that could seriously delay or prevent proper clinical response from caregivers. Delays in clinical response may escalate common care situations to critical ones.

Attackers and malware gain entry to networks, elevate their privileges, and propagate malicious activities through network devices that have cybersecurity vulnerabilities (e.g., outdated operating systems [OSs], weak security controls, systems that are not fully integrated or are misconfigured with security management systems) and have access to the Internet. This describes the majority of networked medical devices used in healthcare today.

Where to Start?
Modern security management tools are likely already in place for our enterprise IT environment. But for us to begin to apply these methods to our networked medical devices and systems, we need to understand the device properties that affect network security. Where is the device in the network (e.g., Internet protocol [IP] address, virtual local area network [VLAN])? What are its potential vulnerabilities (e.g., OS/version, medical device application, off-the-shelf software, communication methods, ePHI capability, dependencies)? Who/what has access to it (e.g., cloud connection, Internet access, remote support, dependencies)?
How does it communicate (e.g., IP ports, wireless configuration)?

When a vulnerability or threat advisory is received, our computerized maintenance management system (CMMS) needs to have the network or system properties that the advisory will reference—often a software revision, OS version, or software patch level. When enterprise network security controls alert on a compromised device or suspicious network activity, the alert often is associated with an IP address, media access control (MAC) address, or hostname. Without the corresponding information in our CMMS, we have no way of assessing our risk or planning a remediation because we don’t know which devices are affected.

In addition to tracking data that are useful for risk analyses, our CMMS should help propagate IT policy down to the medical device fleet and communicate patient safety needs up to the IT enterprise. For example, when our organization’s IT governance policy states that all patient information repositories are properly secured, do we know which medical devices/systems store patient information, the type of information that is stored, and where the information is kept? During an IT network change, we may experience a downtime that affects medical device integrations. Without knowing which devices are served by which VLANs, we will not know the full clinical impact of the outage or be able to properly prepare the clinical staff for the downtime.

In a large enterprise network, medical devices are one of the users of network resources, exchanging information with other medical and IT systems. Typically, the IT department is responsible for the IT network security policy and controls on the enterprise network, which may or may not take into account the special privacy and security requirements for medical devices and systems. Firewall and intruder detection/prevention systems (IDs/IPs) may be tuned according to enterprise standards, assuming complementary malware protection on IT endpoints. To provide the best level of protection, medical devices/systems without standard enterprise-managed endpoint protection may require external security controls, such as additional firewall configuration. The IT patient database security policy may rely on special security and central monitoring applications to ensure reliability and integrity. Without the ability to add third-party software applications to a medical device, the benefits of the IT database security policy may not translate to the medical device databases. To develop a more comprehensive and efficient security policy, both the HTM and IT departments need to fully understand the network properties of medical devices and the associated vulnerabilities and constraints regarding their configuration and implementation.

Within the ecosystem of medical device and IT networks, HTM professionals are uniquely qualified to understand and provide input regarding risks of devices and systems. Information about security controls, vulnerabilities, and network implementation are well within the HTM realm. Just as we use equipment data (e.g., manufacturer, model, and device classification; clinical application) to drive risk-based maintenance programs, we should begin to collect, maintain, and use information such as IP address, ePHI capability, OS, and software versions to act as risk indicators for our security management plans.

Prepare Your CMMS

The modern CMMS can manage information related to the network properties and implementation of medical devices. The following section describes a suggested set of CMMS data fields that can help facilitate privacy and security risk management processes.

ePHI Capability

To assess privacy risk, it’s critical to know whether a medical device/system has the ability to contain ePHI, the type of information it contains, and what it does with the information. The Manufacturer Disclosure Statement for Medical Device Security (MDS²) form outlines characteristics of the ePHI generated, transmitted, received, and stored by the medical device/system.³ ePHI capabilities contribute to varying degrees of risk depending on how the device is implemented and configured in the clinical environment and the workflows it supports.
Documenting the type and amount of ePHI (including the maximum) the device/system is likely to hold at any given time is important. In the event of a breach, malware, unauthorized access, or other security event, these elements are critical in assessing whether the events are subject to regulatory, legal, or other reporting requirements. It’s important to check with your information security or privacy officer to determine the requirements of your organization’s policies for security incident response—and to document those requirements.

System Dependencies
Medical devices/systems increasingly are being integrated and interconnected, thereby presenting us with interdependent “systems of systems.” The documentation of dependencies is common in Information Technology Infrastructure Library configuration management or, in our case, for systems that are dependent on information provided by medical devices/systems.

Knowing the effect that a change or failure of a medical device may have on other medical or IT systems and workflows is vital. The health of interdependent systems may have varying degrees of effect on the overall risk of the medical device system, and vice versa. For example, it is common within the clinical environment to have a downtime procedure ready for when the admit, discharge, transfer (ADT) system is down, as requiring manual entry may cause delays in care.

It’s also important to understand the risk imposed by failure of the medical device to a dependent system, such as a clinical decision analytics or alarm/alert system. For instance, an interface failure between an ADT and a mobile device alerting system could generate a patient alert associated with the wrong patient.

Cloud Connection
By allowing direct access to specialized data centers for clinical data processing and reporting, advances in cloud applications can help reduce the costs of providing healthcare. Cloud sites using Hypertext Transfer Protocol Secure (HTTPS) and leveraging Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols for secure web communication use secure encrypted transmission and authentication for each Web session, thereby providing protection from man-in-the-middle, masquerading, and snooping attacks. SSL/TLS protocols are “proven and effective methods of securing sensitive communications.”

Cloud connections, however, may present new security and regulatory challenges. The Internet connection method, workflow, and URL need to be clearly documented and fully understood. The benefits of HTTPS can be a drawback if not integrated into the enterprise security management systems correctly. Most enterprise security controls are installed at a data center, whereas Cloud connections may be made at the medical device itself and reach the Internet without passing through enterprise security controls. SSL/TLS prevents visibility into the data stream as it traverses the enterprise network perimeter, preventing intrusion detection/prevention, event monitoring, and anti-malware systems from detecting malware, malicious connections, or data exfiltration without special processing.

Further, exposing medical device patient data to a remote data center managed by a vendor or other third party may present additional privacy issues that are governed by HIPAA (Health Insurance Portability and Accountability Act of 1996)/HITECH (Health Information Technology for Economic and Clinical Health) Act data security regulations.

MDS²
It is recommended that medical device manufacturers provide the MDS² form to healthcare providers. The MDS² helps users implement the device safely in their networking environment by outlining the ePHI/security capabilities and other system design data of the device. Further, the MDS² should describe constraints to what the user is allowed to do when modifying the system for integration into current network security policies, including adding or removing software components.

When collecting and associating these documents with your CMMS records, it’s important to verify that you have the most current MDS² form and that the software
version for which the form is written matches the software revision levels of the medical device.

**Remote Support Method**
The manufacturer’s method of remote network access to a medical device/system, including remote network information, should be documented. If the IT department has configured a VPN (virtual private network) tunnel or other secure access path through the enterprise network, then that configuration documentation likely resides in IT. Many legacy remote support solutions rely on less secure access methods (e.g., DSL, phone modem). These confer relatively high risk due to the fact that remote service connectivity can set up an alternative path into the enterprise network that is possibly undocumented and/or unmanaged and potentially can be exploited by malicious parties or malware. For new installations, certain remote software solutions may not be supported on the enterprise network or may have vulnerabilities or configurations that can compromise network security controls. Certain remote support workflows can add risk to the computing environment (e.g., user on demand versus on all the time.)

**IP Address**
“IP address” doesn’t only refer to the IP of the medical device asset or equipment record stored in your CMMS. It means the IP addresses of all of the network devices that make up the asset. It’s important to include the subnet mask, gateway, any domain name server (DNS) settings, and whether the addressing is static or dynamic. In most cases, only one network component—a network interface card (NIC)—will be embedded in your medical device or system. Other medical devices may be systems (e.g., a computed tomography [CT] scanner) that are made up of multiple network components. A CT scanner may involve several workstations, a picture archiving and communication system worklist/radiology information system workstation, printers, local storage devices, the gantry itself, and maybe even the table and a network router. Network security scanners may detect all networking components of these devices. Some method for reference them in the CMMS, whether as equipment records themselves or as system components associated with a master medical device asset record, will be needed. Firewalls, routers, and other network devices operating at the Open Systems Interconnection (OSI) network level may only report traffic by IP address. If it’s necessary to correlate back to other device traffic or to locate the device physically, your CMMS should have that information.

IP address also may affect your inventory policy. Even though a router or switch is not medical device, you may want to make an equipment record in your CMMS for it. Networking components may not have any maintenance or regulatory requirements, but like any other network device, they have software and firmware levels, may contain vulnerabilities, and are subject to threats. Including the network components of medical systems in your CMMS (or elsewhere) may facilitate a more comprehensive risk profile.

**MAC Address**
The hardware, or MAC, address is burned into the NIC. The ranges for the address are specific to the NIC manufacturer; they are traceable and cannot be changed. This address is required for OSI MAC level communication, which is common between the NIC and the network switch or hub. Knowing the MAC address is important because it specifically identifies the hardware device. IP addresses can, and often do, change in a dynamic IP environment; therefore, if you need to associate network traffic to a specific device, MAC may be the only way. Network access control (NAC) protocols, TCP/UDP protocol filtering, and some local routing depend on MAC. MAC is critical to wireless network function.

**VLAN/Network Identifier**
A best practice in networking is to divide the larger network into subnets that can be managed separately for security and to help reduce the risk of an attacker or malware spreading to/from other network resources. This is commonly implemented via VLANs, though over time, additional physical LANs may be installed in an area. Isolated networking components may not have any maintenance or regulatory requirements, but like any other network device, they have software and firmware levels, may contain vulnerabilities, and are subject to threats.
Features

(air-gapped) LANs that are meant to be separate from the larger network and/or Internet also may be implemented. Network security controls for mitigating vulnerabilities often affect the entire segment. When network changes, maintenance, or outages occur, your CMMS should allow you to know which devices were affected. Segmenting medical devices in their own network allows for accurate risk assessment and management methods to be efficiently applied.

Medical Device Software
The software that the manufacturer packages to run over the OS should be documented, including the version and any patch or upgrade levels. Any off-the-shelf software that is used in the operation of the medical device also should be documented. For example, if Microsoft Word or Adobe Acrobat are required to generate reports from the medical device, include the version of that software. Any software added during installation in the networking environment (e.g., antivirus or other system management agents) should be documented as well. Vulnerability notices and threat alerts often are associated with software version. Properly documenting the software version will support efficient identification of affected devices when assessing risk of the vulnerability or threat.

Communication Ports/Protocols
The TCP/UDP ports associated with IP traffic are used by firewalls, switches/routers, and security systems to identify the type of communications occurring in a computer network conversation. Port 104, for example, typically is associated with the DICOM (Digital Imaging and Communications in Medicine) protocol. More than a thousand other ports are associated with common communication protocols. Typically, several ports will make up the communication requirements of a medical device/system. These ports should be documented in order to identify and manage medical device/system network traffic to and from devices.

Network Diagram (Topology)
Network diagrams of systems should be documented, including dependencies, all interacting systems, and redundancies. During repairs, reconfigurations, or other change events, dependencies should be managed to minimize disruption or downtimes. Documentation should include physical as well as logical data flow diagrams.

Wireless Network Configuration
Along with MAC and IP address, authentication and encryption protocols are critical for wireless networking. A misconfigured wireless device or system can increase the risk of an attacker or malware accessing critical network resources. Depending on the protocols supported on your organization’s wireless infrastructure, a client username and password may be required for the device to properly associate with the network. (Note: Check your organizations security policy before entering any login credentials/passwords into your CMMS.) The SSID (service set identifier) should be verified to ensure that the medical device associates with the proper wireless network, as most wireless networks are logically segmented to allow for separate management policies. If your medical device system relies on encryption in transit, it’s important to understand that wireless encryption protocols only pertain to the wireless portion of the communications. Eventually, the data may be transmitted along the wired portion of the network, which may or may not have encryption of its own.

OS
The OS version, including any applicable service pack add-ons or upgrades, should be documented. Also, it should be noted whether the OS is custom, embedded, and/or proprietary. Documenting special configurations, such as hardening methods or “whitelisting,” can be useful for evaluating risk. OSs with special hardening or other security capabilities need to be separable when vulnerability or exploit communications are received, as their built-in capabilities may render them immune. Cybersecurity threats often target the OS of a computer device. When a vulnerability notice or threat alert is issued, having this data is critical to providing a timely and accurate remediation.
Patch Levels

Patch levels of all applicable OS and medical device software used in the asset should be documented. When vulnerability notices or threat alerts are received, they often apply to certain versions of OS or application software; therefore, you will need to know the versions to understand your risk and remediation options. Although common network vulnerability scanning utilities can generate a detailed list of OS, software, and configuration vulnerabilities for a computer, a medical device/system may be too sensitive for invasive automatic scanning to be performed safely. If so, a manual list may be necessary.

ISO/TR 80001-2-6:2014

ISO/TR 80001-2-6:2014 (Application of risk management for IT-networks incorporating medical device—Part 2-6: Application guidance—Guidance for responsibility agreements) recommends a manufacturer disclosure of the topology, data flow, and ports/protocols used by the medical device/system in a typical network implementation. This document is useful for understanding potential security vulnerabilities that may be introduced when new data are integrated into the organization’s network infrastructure, as well as the changes that may be needed to secure new and existing network data and systems. Information regarding required segmentation, data flow, and types will be critical in developing security zones for the system.

Hostname

If it has one, the device’s network or DNS name should be documented. If the device is a domain resource, the FDQN (fully qualified domain name) also should be recorded. Devices that participate in a domain can have user and machine policies dictated to them that may affect your ability to manage risk. You also may be able to take advantage of risk-mitigating policies such as role-based access control, patch management, or hard drive encryption.

Workgroup

Workgroup is a concept that configures a subset of participating devices that share resources within a network. If your system depends on workgroup settings, you may need to include it when reconfiguring the device after a repair or troubleshooting communication issues.

Jack Identification

Documenting your network drop, wall jack, computer port, or another local term for the Ethernet jack in your CMMS also is important. VLANs, MAC filtering, and NAC can be associated with a specific switch port in the data closet (i.e., intermediate distribution frame). After being connected to the cable facility, the wall jack by extension becomes a specially configured switch port. There may be multiple networks in a single wall plate, with some designated for medical devices (e.g., diagnostic ultrasound, electroencephalogram).

Prepare HTM Staff

HTM has thrived on its capacity for gaining knowledge about current, new, and evolving health technologies. As HTM has experienced increased demand for supporting IT network–based devices, the IT community has gained awareness of the privacy and network security issues presented by medical devices and systems on the enterprise network. Traditionally, biomedical equipment technicians have attended manufacturer training courses for a specific modality, thereby learning how to fill the clinical support gap between the user and the manufacturer support agreement. For simpler systems, knowledge gained “on the job” may be leveraged to fully support devices and systems in-house.

At least some of the training budget for HTM professionals should go toward basic networking, networking security, computer database principles, privacy regulations, Internet, and other related skills. Some knowledge can be obtained through medical device manufacturer training on a generic level, but IT training tracks (e.g., local college courses, certification entities like CompTIA) may provide the most rounded training.

Some HTM operations rely on “EHR integration specialists” or “that one tech who’s interested in networking,” but with the coming wave of personal medical devices, software as a medical device, and
cloud services for medical device back-end support, everyone needs to be learning about IT technologies and applying it to their areas of responsibility.

Get Involved
The management of medical IT network risk may be considered a distributed role. Everyone has a part, from clinical users choosing strong passwords and properly managing storage media, to the IT firewall manager, to the privacy officer who enforces policy on database access—and so on. The specific role for HTM professionals should be tailored to allow efficient collaboration with other members to complete the distributed role. HTM’s effort should involve being an advocate to ensure the safety, effectiveness, and security of the data and medical device/systems in the patient and networking environments.

HTM should maintain the data discussed and any data associated with information security and risk operations necessary to support the organizational information security and risk plans. As the source of record for the data related to information security, the CMMS may be interfaced with or provide configuration data to enterprise security systems, including firewalls, IDS/IPSs, event monitoring, and antimalware software. ePHI capability, MDS\textsuperscript{2}, ISO/TR 80001-2-6:2014, and network diagrams can inform risk analyses by documenting gaps in device security capabilities and security control coverage.

HTM professionals are encouraged to share their knowledge of the security capabilities or vulnerabilities associated with medical devices in an effort to improve clinical workflow policies. This can be especially useful when developing downtime procedures and clinical response. HTM’s knowledge of system dependencies may help expand the awareness of the scope and impact of a potential system failure, allowing an appropriate response to be developed. HTM professionals also can share knowledge by providing medical device security training through a user-awareness program or training module. Remember: We’re all in this together.

References


Get the Most Out of Your CMMS


In this book, authors Ted Cohen, MS, FACCE, and Matthew Baretich, PE, PhD, provide guidance and best practices for:

- Proper setup of your CMMS
- Generating meaningful data
- Performing better equipment maintenance

To purchase a print or PDF copy, visit www.aami.org/Store.
Product Codes: CMMS or CMMS-PDF