ARAB bioclinic 3

BIOMEDICAL & CLINICAL ENGINEERING

The 3rd International Conference

ON Biomedical & Clinical Engineering

Cybersecurity

Risk Management of IT Networks incorporating Medical Devices

| AUTHORS: S.Ramnath, ECRI Middle East & Ahmad Jawhar, Healthcare Consulting & Planning, Lebanon

Objectives of this presentation

- Recognize threats posed to medical devices
- Describe successful approaches used by other facilities
- Design and implement policies and procedures for cybersecurity of medical devices based on proven approaches

Introduction

In a December 2012 episode of the popular television series Homeland, the Vice President of the United States was assassinated when a terrorist organization wirelessly hacked his pacemaker

Nowadays, numerous medical devices reside on hospital networks and / or are accessible through wireless networks. These include general devices such as patient monitors, infusion pumps, as well as life-sustaining devices such as ventilators, anesthesia machines and pacemakers

History

- 1970’s and 1980’s: R & D work performed in some large university teaching hospitals to capture data by connecting a medical device to a computer.

- 1992 – 1994: Commercially available Standalone or independent connectivity solutions: Serial interface cables connected ventilators and displayed data onto patient monitors using HL7. Eventually, using proprietary “plug-in” modules that connected the medical device serial ports to the patient monitor, non-monitoring parameters and waveforms from a number of devices were displayed in a correlated display along with the physiological monitoring data. Alarms were also processed via these types of connections and sent to the monitoring central station.

- 1996-1998: 8-port terminal servers were used for the first time to convert serial data to network servers (TCP/IP) using specific device drivers and HL7 interface to CIS application servers

History

- 2000-2003: CIS applications started to become more pervasive, but the two main methods continued to be either patient-monitor-centric or standalone solutions that leverage a terminal server/concentrator at the patient's bedside. The introduction of Smart IV Pumps, opened the door to interfacing directly to CIS/EMR's since connecting IV pumps and similar devices to the patient monitor did not make any sense both clinically and financially.

- 2004-present: Wireless (802.11/WiFi) and mobility evolved but created new challenges. Serial cabling is no longer desired. It was too messy and cumbersome both from an aesthetics and most importantly, clinical workflow perspective. The result is: more and more devices are "connected" and "WiFi enabled"

Terminology in Cybersecurity

- Cybersecurity refers to protection of information and information systems from intentional or unintentional unauthorized access, use, disclosure, disruption, modification, or destruction.
- Vulnerabilities are weaknesses in security controls affecting medical device (hardware, software, and implementation).
- Risk is a measure of potential harm emanating from adverse events that might occur and the likelihood of occurrence.
- Assets are data, devices, or other component of the environment that supports information-related activities. They constitute what must be protected from compromise to ensure patient safety and privacy. Assets may include hardware (servers and switches), software (applications and support systems) and confidential information, as well as the organization’s proprietary care protocols and medical devices.
- Threats are the potential for an intruder to violate security and cause harm to assets.
- Mitigation is an act or control that reduces risk if undertaken.

Potential risks associated with networked medical devices (FDA)

- Network-connected/configured medical devices infected or disabled by malware
- Presence of malware on hospital computers, smartphones and tablets, targeting mobile devices that use wireless technology
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical and maintenance personnel)
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices)
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals and poor coding/SQL injection.

Potential threats affecting networked medical devices (FDA)

1. Hacktivists (anonymous individuals) wishing to cause service interruption and harm

2. Thieves desiring to sell or monetize confidential information, engage in identity theft, commit financial fraud against individuals and/or the health care organization and / or its asociates

3. Malicious groups or individuals seeking to cause harm to patients (possibly targeting VIP patients) or seeking to damage the health care organization's brand.

4. Malware which evades existing antivirus engines and rules but is not specifically targeted at medical devices

Intentional threats (FDA draft guidance - June 2013)

The FDA draft guidance, Content of premarket submissions for management of cybersecurity in medical devices (June 2013), calls attention to “intentional” threats when designing a medical device

“Intentional" threats within a health care environment include:

- Malware and viruses infecting medical devices
- Organized crime attacking a VIP patient’s personal medical device
- Hackers targeting Distributed Denial of Service (DDoS) attacks against a hospital network
- Organized crime conducting exfiltration attacks against hospital medical devices
- Hackers testing their skills against a hospital’s vulnerable network (including networked medical devices)
- Disgruntled employees uploading Trojan horse code to networked medical devices

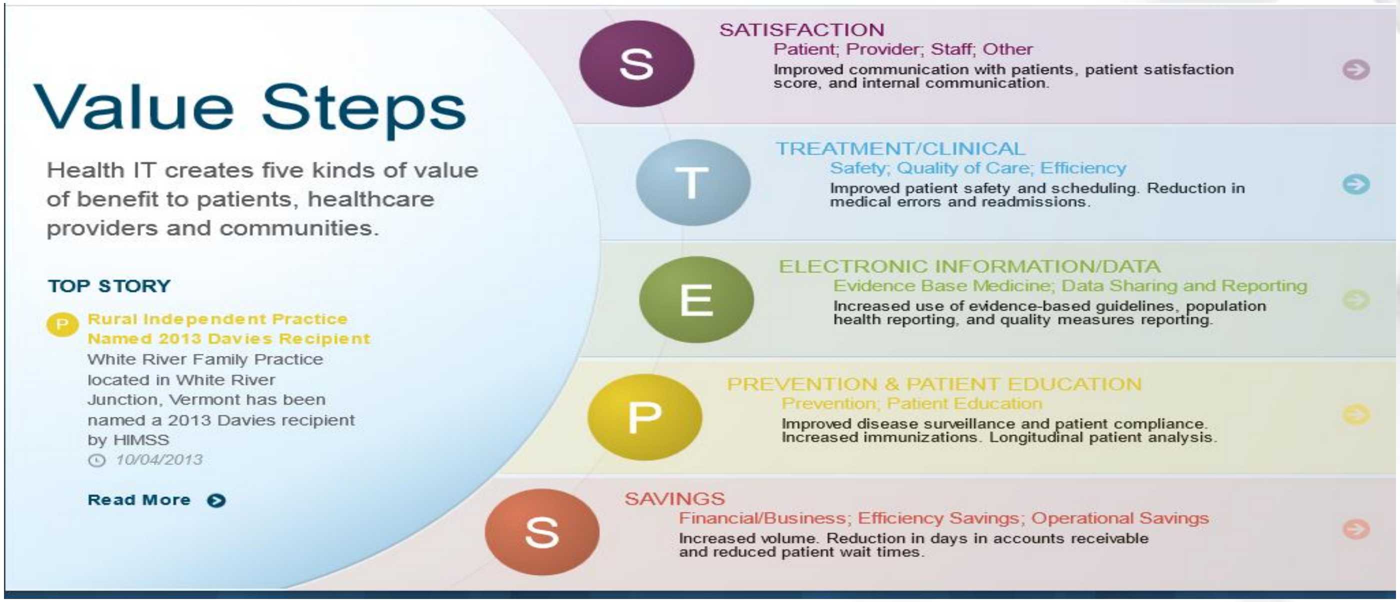
Overview of IEC 80001-1

Healthcare Consulting & Planning sal

ECRI Institute
The Discipline of Science. The Integrity of Independence.

An Introduction to the Benefits Realized for the Value of Health IT

- **Ensuring the availability and efficacy of networked medical devices is paramount to patient safety and prevention of medical errors.**



Value Steps

Health IT creates five kinds of value of benefit to patients, healthcare providers and communities.

TOP STORY

P **Rural Independent Practice Named 2013 Davies Recipient**
White River Family Practice located in White River Junction, Vermont has been named a 2013 Davies recipient by HIMSS
10/04/2013

Read More

S SATISFACTION
Patient; Provider; Staff; Other
Improved communication with patients, patient satisfaction score, and internal communication.

T TREATMENT/CLINICAL
Safety; Quality of Care; Efficiency
Improved patient safety and scheduling. Reduction in medical errors and readmissions.

E ELECTRONIC INFORMATION/DATA
Evidence Base Medicine; Data Sharing and Reporting
Increased use of evidence-based guidelines, population health reporting, and quality measures reporting.

P PREVENTION & PATIENT EDUCATION
Prevention; Patient Education
Improved disease surveillance and patient compliance. Increased immunizations. Longitudinal patient analysis.

S SAVINGS
Financial/Business; Efficiency Savings; Operational Savings
Increased volume. Reduction in days in accounts receivable and reduced patient wait times.

http://www.himss.org/ValueSuite

The (Very) High Level View

The ability of modern medical devices to connect to multiple platforms and devices create more targets for infiltration and exploitation

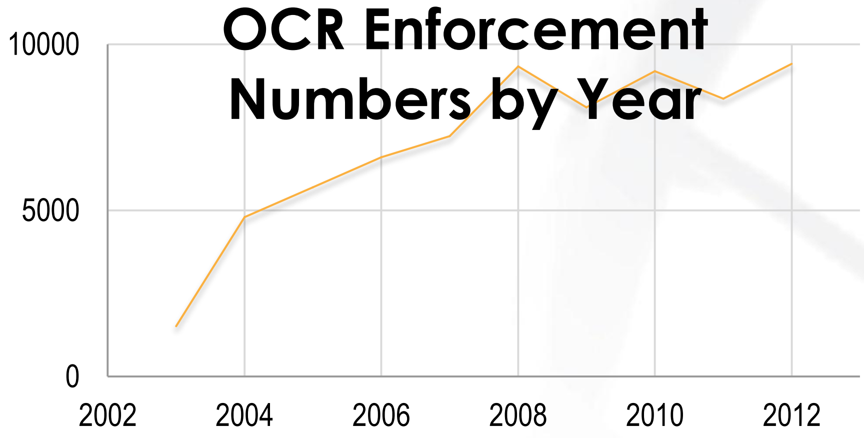
Consequences of Cybersecurity Attacks

- Disruption of patient care
  - Devices connected to the internet malfunction due to malware and viruses
  - Origins of the infection do not have to be medical device-specific

- Loss of protected health information (PHI)
  - PHI contains sensitive personal information
  - Healthcare organizations are attractive targets for phishing attacks

Importance of Cybersecurity

- Healthcare organizations are required to protect their medical devices and IT systems
- Consequences of cybersecurity breach are dire



The Discipline of Science. The Integrity of Independence.

IEC 80001-1 and Medical Devices

Sample Problem – 1
Central Monitoring Systems

- A call went in to Welch Allyn that a care area's guest-services wireless network was down. Guests could 'see' the network but not connect
- Upon troubleshooting, it was determined that a switch in their Cisco network switch had failed… and central monitoring wasn't being passed through either
- Remarkable that the problem was first discovered as an outage in guest network

http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Detail.CFM?MDRFOI__ID=3273711

Healthcare Consulting & Planning sal

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Sample Problem – 2
Physiologic Monitor

- Hospital installed GE MacLab physiologic monitors
- GE provides antivirus install instructions and validated versions of software to use. Unfortunately the versions GE validated are no longer available for purchase. GE does not validate current versions of antivirus software for this software version, even though they support it.
  - If the hospital loads the current version of antivirus software available on the device, it can invalidate the warranty
  - If the device gets infected and impacts patient safety, it will be their responsibility as they were supposed to load antivirus software
  - Hospital wishes to comply with FDA's June 13 safety communication on cybersecurity for medical devices.

http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Detail.CFM?MDRFOI__ID=3239402

Sample Problem – 3
Bronchoscopy

- Staff setting up for a procedure received an error message on its electromagnetic navigation bronchoscopy (ENB) system, which had recently received antivirus software
  - Had to convert to a different approach while the patient was under general anesthesia
- Troubleshooting found that during the installation of the anti-virus software, IT staff turned on the Windows firewall. The firewall disrupted communication and caused error messages
- Once the firewall was turned off, the system began to operate normally
- Supplier cautioned the hospital not to load antivirus software without supplier approval

http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Detail.CFM?MDRFOI__ID=2224751

Sample Problem 4 : Telemetry to Toasters

- Increasingly connected consumer devices comprise the "Internet of Things"
  - Televisions, multi-media centers, refrigerators, ovens, thermostats, lighting systems, locks, webcams, toys
- Often lack simple protections from cybersecurity threats
- Recent report (disputed) of a hacked fridge acting as a botnet
- http://www.proofpoint.com/about-us/press-releases/01162014.php
- http://www.technologyreview.com/news/517931/more-connected-homes-more-problems/
- http://www.networkworld.com/news/2014/012714-spam-appliances-278108.html?source=NWWNLE_nlt_daily_pm_2014-01-27

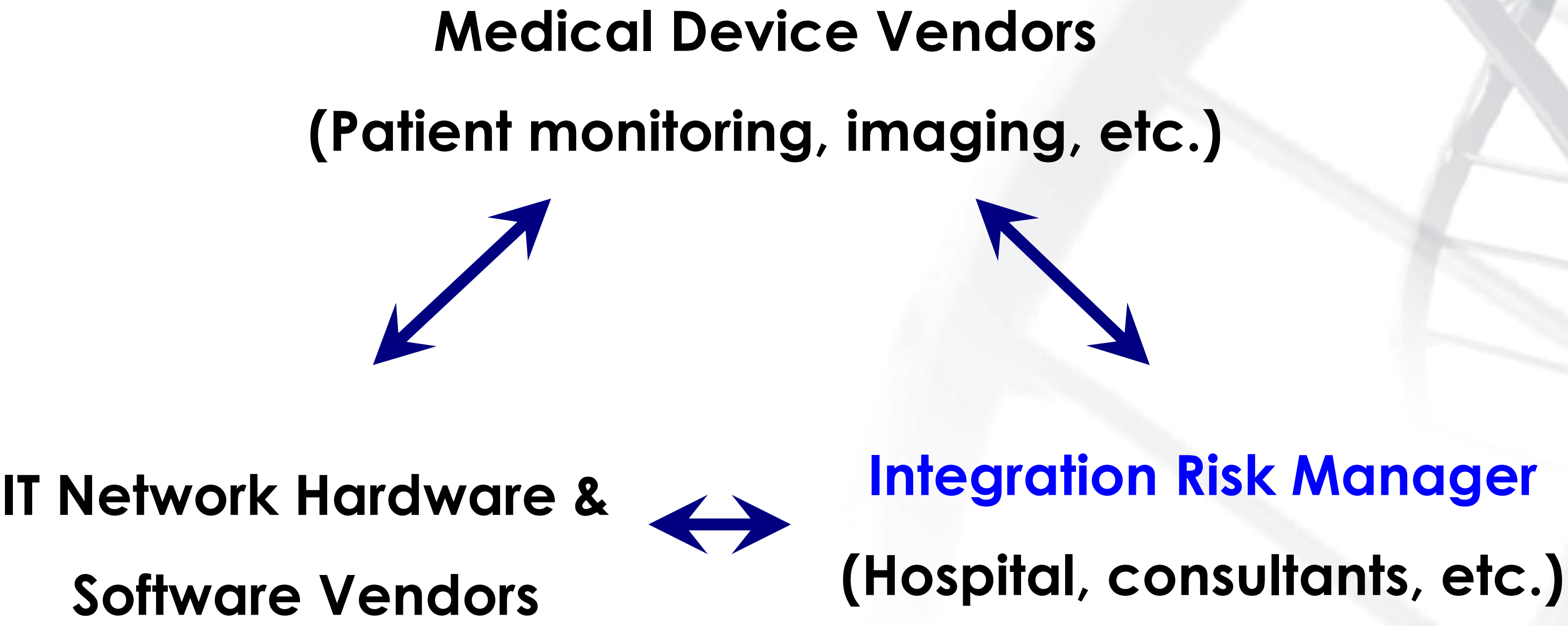
HCP Healthcare Consulting & Planning sal

ECRI Institute
The Discipline of Science. The Integrity of Independence.

IEC 80001-1’s Three “Key Properties”

- Risk management should be applied to address the balance of the key properties
  - Safety
  - Effectiveness
  - Data and system security
- Obtain from: http://www.aami.org/publications/standards/80001.html

Key Players : Relationship of Relevant Organizations



Medical Device Vendors

(Patient monitoring, imaging, etc.)

IT Network Hardware &

Software Vendors

Integration Risk Manager

(Hospital, consultants, etc.)

Healthcare Consulting & Planning sal

ECRI Institute

The Discipline of Science. The Integrity of Independence.

Medical Devices and Impact

Key Questions on Medical Devices

- Key questions and considerations covered in our article, which can aid in the process of purchasing networked medical devices and in assessing a device's impact on your facility's cybersecurity.
  - What data is stored on and generated by the device?
  - Does the device contain any USB ports?
  - What methods of encryption are available to ensure data privacy during transmission?
  - What are the different network interface card options?
  - Does the device server meet your facility's IT requirements, or will you need to manage exceptions to your requirements?
  - How does the device vendor support software/firmware/security patch updates?
  - Are logs kept of device or server access?
  - Does the manufacturer provide a detailed Manufacturer Disclosure Statement for Medical Device Security (MDS^2) form (2013 version) during the purchasing process for both the device and the device server?
  - Does the device have known and publicized software vulnerabilities?

Device Data

What data is stored on and generated by the device?

- List all data types or information that is a part of the medical device (stored on, transmitted to/from, or generated by the device).
  - Identify whether any protected health information (PHI) or personally identifiable information (PII) is stored or generated by the device.
  - How much data does the device retain—only the current patient's or also previous patients'?
- Some devices are capable of storing and exchanging extensive PHI/PII; however, others may only contain nonidentifiable information (e.g., alarm history).
  - f no PHI/PII is stored on or communicated with the device, data encryption may not be merited.
  - If PHI/PII is stored on or communicated with the device, methods of encryption may be required to protect that data.
- Can all data stored on the device be easily deleted when the device is decommissioned or leaves the facility's control?
  - Determine whether a convenient method of deleting the device data is available (e.g., through maintenance software, factory reset, or destruction of data after a set number of log-in attempts).
  - The decommissioning process is often overlooked in the initial device purchasing process due to the long expected life of medical devices. A convenient method for deleting data will make for easier data management at the device's end of life or when the device leaves the facility, such as for repair.
- Can PHI/PII stored on the device be deidentified?
  - Determine whether it's possible to deidentify data (e.g., through device settings).
  - Deidentifying patient data can be beneficial, especially if the data will be used for research purposes.

Device Connections

- Does the device contain any USB ports?
  - Determine whether any USB ports are available on the device and whether they can be disabled if desired.
  - USB ports are one of the most common ways to distribute malware. Controlling USB port access can provide an additional layer of security.

Encryption and Authentication

- **What methods of encryption are available to ensure data privacy during transmission?**
  - List the available methods of encryption, and identify whether encryption of data is required per your IT policy.
  - Does the provided encryption comply with the appropriate standards (e.g., Federal Information Processing Standard [FIPS] 140-2)?
  - If PHI/PII or other sensitive data is communicated by the device, data encryption is advised.
  - Encryption protects data and makes it virtually useless to an unauthorized party, even in the case of a data breach.
- **Is it possible to encrypt data at rest (i.e., when stored/static on the device memory)?**
  - Identify whether data encryption is available at rest.
  - This is especially important for devices that may contain extensive logs/databases of PHI/PII. Without at-rest encryption, the loss of a device with sensitive data/PHI/PII in its memory (e.g., stolen/lost laptop that connects to a medical device system) may be required to be reported as a data breach
- **What methods of authentication are available and actively used?**
  - List options for authentication, and ask the manufacturer to provide IT contacts at user facilities that are implementing the listed methods with their product.
  - Some devices offer standard EAP authentication methods, which are extensively used at the enterprise level. Using authentication measures ensures that a device communicating in a network is in fact authorized to do so.
  - We are aware that some healthcare facilities may even require that devices conform to a specific encryption and authentication protocol (e.g., WPA2 EAP-TLS) in order to be considered for wireless implementation.
  - (Antiquated wireless protocols with widely known vulnerabilities (e.g., WEP) should not be used.

Networking Features and Requirements

- What are the different network interface card options?
  - Identify all available network interface card options and the network interface standards they employ (i.e., Institute of Electrical and Electronics Engineers [IEEE] 802.11a/b/g/n/ac). Some manufacturers may offer different options for network interface cards for the same device, with cost implications.
  - Since different devices have different bandwidth requirements, the support of different technologies may aid in network configurability. The ability to use either the 2.4 or 5 GHz frequency band for wireless communication (IEEE 802.11 technology dependent) can, for example, aid in resolving wireless network overcrowding.
- Do the device networking features, requirements, methods, and protocols employed support your current network infrastructure?
  - Request that the manufacturer provide complete information about the device's networking features, requirements, methods, and protocols.
  - Determine whether these features are suitable for your current network infrastructure or whether modifications are required in order to support them.
  - Comprehensive information regarding device networking can assist in conducting an appropriate evaluation to assess conformity to a facility's networking practices and IT policy.

Device Server

- Does the device server meet your facility's IT requirements, or will you need to manage exceptions to your requirements?
  - Identify whether the device server conforms to your IT policy.
  - Identify and document nonconformance of the server operating system (OS), anti-malware support, virtualization, etc.
  - Review the minimum memory requirements and subscription policies for virtual servers.
  - Conformance to facility-wide IT policy can simplify server management and maintenance. Management of an exception is always more burdensome, as a standardized management approach may not apply (e.g., operating system updates).
- 2. Does the server require or recommend remote access for manufacturer support?
  - Identify whether remote server access by the manufacturer is required. If it is, ensure that access is tightly controlled such that only authorized users have access, and that access is closed at all times except when necessary.
  - Remote server access may be used for troubleshooting the system, continuous system monitoring, device calibration, update distribution, etc. It's important that this access be tightly controlled to reduce the risk of unauthorized access.
- 3. Does the server receive information from or transmit it to entities outside the facility or utilize cloud services?
  - Identify what data in the system, if any, is exchanged and/or stored outside your facility. Specifically, identify:
  - Exactly which parameters or data points will be transferred or stored
  - the purpose or product for which the supplier will use this data
  - Who else will or could have access to the data once it's outside the facility (for example, only employees of the supplier, or perhaps other facilities)
  - Who owns the rights to this transmitted or stored data once it exits the facility
  - The supported methods of secure communication (e.g., v [VPN])
  - Whether cloud services are offered and/or required
  - b) Some servers can hold patient-specific data on-site, but others may communicate information to servers outside the facility for aggregate analysis or other purposes. Facilities should be aware of all potential transmission methods, uses, and locations of their data so that they can identify any potential concerns about data security, availability, and ownership.

Healthcare Consulting & Planning sal

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Security Updates

- How does the device vendor support software/firmware/security patch updates?
  - Request that the manufacturer specify its methods and policy for notifying customers about and applying updates to the medical device (e.g., how frequently software updates occur, how customers are notified in the event of a critical security vulnerability).
  - Software updates are often difficult to conduct in the clinical setting because the device may be in continuous clinical use, there may be update-related device downtime, and conducting the update may require physically accessing the device. However, keeping devices and servers patched and up to date can help ensure that the system is secure. Appropriate plans for update and patch management are crucial for minimizing potential future risks.

Server Access Controls

- Are logs kept of device or server access?
  - Ask the manufacturer if accesses and any setting modifications are logged.
  - Such traceability can assist in event investigation and auditing.
- 2. Are all device passwords permanently set to default values, or can they be modified for each facility and changed periodically?
  - Identify which passwords are configurable on the system.
  - Some devices allow configuration of the passwords used to access configuration modes and other functions, whereas others do not provide means of changing any of the passwords (e.g., hard-coded passwords). Passwords may even be standard for all devices of a particular model. Facility-specific configurability of passwords can provide an added layer of security.
  - Password use can present difficulties in a clinical setting, especially with devices/systems that must be accessed quickly in emergencies. Clinical use requirements should not be ignored when developing device access and password policies.
- 3. Does the system support active user-based access management (e.g., Active Directory)?
  - Identify whether centralized user-based access management is available and supported by the system.
  - Utilizing user-based access management such as Active Directory can allow user-based control of access to network assets, including networked medical devices.
- 4. How is remote server access controlled?
  - Ask the manufacturer to specify the purpose of the remote access and to define how your facility can keep track of the manufacturer access to your medical device server (e.g., through use of two-factor authentication).
  - Some servers may require or benefit from remote manufacturer access to the medical device. Identifying supported methods of access control can aid in development of appropriate security measures for controlling manufacturer access.
  - ECRI Institute is aware of healthcare facilities that require independent control of any manufacturer access to their devices/servers.

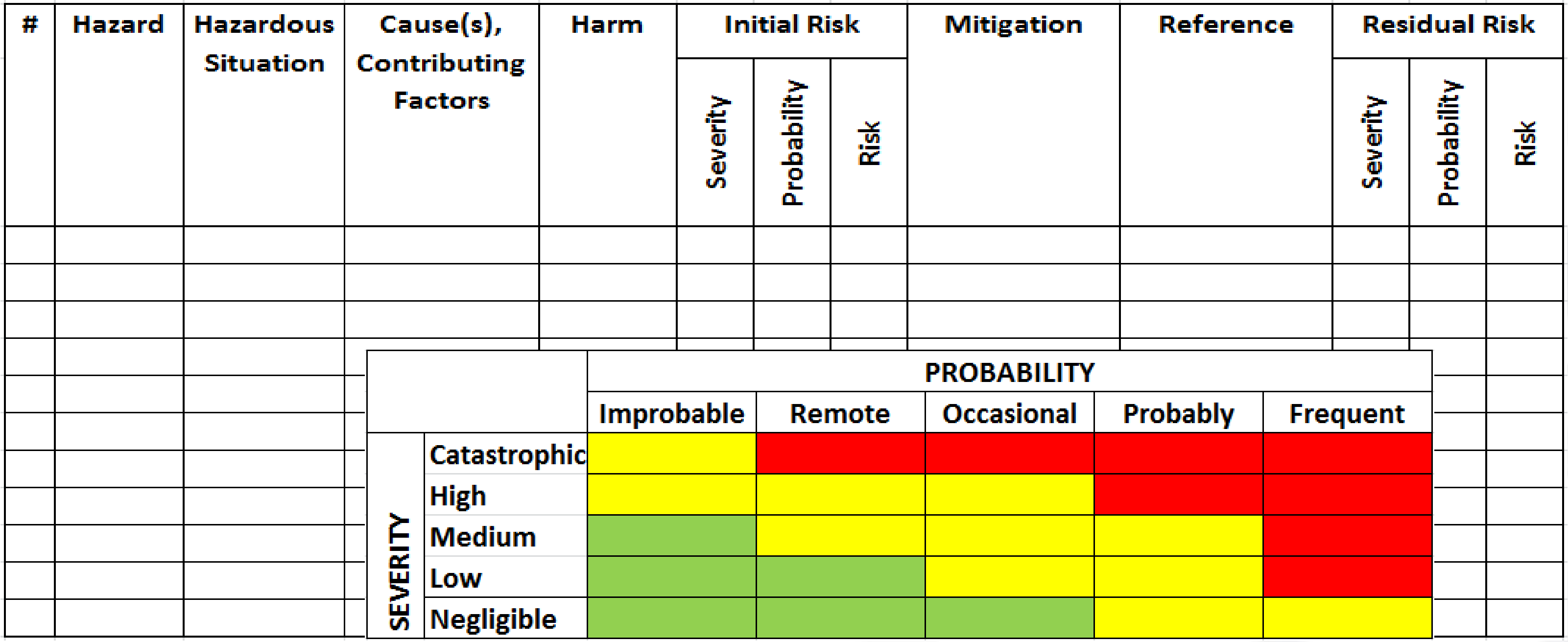
IT Information

- Does the manufacturer provide a detailed Manufacturer Disclosure Statement for Medical Device Security (MDS2) form (2013 version) during the purchasing process for both the device and the device server?
  - Obtain completed MDS2 forms from the manufacturer for both the device and the server. The latest version of the form can be downloaded: https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx.
  - The MDS2 is a standardized template available from most device vendors that is used to assess security-related device features and functionality.
  - MDS2 form submission and IT review should be integral to your future medical device purchases.
- Does the manufacturer provide, at minimum, information and instructions related to connecting their system to the IT network in accordance with IEC 80001-1?
  - Request that the manufacturer provide an IEC 80001-1 summary statement, including details and instructions related to connecting the device to an IT network.
  - Manufacturer responsibilities for providing information to assist healthcare facilities to support appropriate risk assessment are defined in IEC 80001-1.
- Does the manufacturer provide a full list of all software components (e.g., software bill of materials)?
  - Request that the manufacturer provide a list of all the software components contained by the device and any associated systems (such as servers), including all commercial off-the-self, open-source, and proprietary components and their version descriptors.
  - The availability of a complete list allows the facility to explore whether vulnerabilities may exist in any of the software components.
  - ECRI Institute is aware of some manufacturers that embrace complete information sharing with regard to the software components contained in their medical devices. However, not all manufacturers may be inclined to share this information.

Vulnerabilities

- Does the device contain software with known and publicized vulnerabilities?
  - a) Request that the manufacturer specify whether its system has any known vulnerabilities.
  - (1) Ascertain the manufacturer's committed vulnerability disclosure time.
  - (2) Identify the manufacturer's policy for receiving vulnerability reports from customers, researchers, government agencies, etc.
- b) Some devices may still have known vulnerabilities in their software (for example, in commercial off-the-shelf programs). Thorough knowledge of the different vulnerabilities can aid in risk assessment and risk mitigation.
  - Useful information about known vulnerabilities and mitigation measures may also be provided by the U.S. National Vulnerability Database (NVD), U.S. National Health Information Sharing and Analysis Center (NH-ISAC), and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).
  - The implications of any vulnerability need to be appropriately assessed. In many cases, discovered and published vulnerabilities either refer to older and no-longer-maintained medical devices or can be easily mitigated with compensating controls (e.g., securing the system at a higher level).
- 2. Can the device withstand normal network vulnerability scanning?
  - Identify whether the device or system can withstand normal network vulnerability scanning tools (e.g., Nessus).
  - Vulnerability scanning to identify weak points in the network is normal practice for IT assets. Some facilities are also actively monitoring the vulnerabilities on their medical devices.
  - Some medical devices react adversely to vulnerability scans. ECRI Institute is aware of an incident in which a medical device system malfunctioned and shut down because of vulnerability scanning.

HIT Risk Assessment under IEC 80001-1



#	Hazard	Hazardous Situation	Cause(s), Contributing Factors	Harm	Initial Risk			Mitigation	Reference	Residual Risk		
					Severity	Probability	Risk			Severity	Probability	Risk

		PROBABILITY				
		Improbable	Remote	Occasional	Probably	Frequent
SEVERITY	Catastrophic	🟨	🟥	🟥	🟥	🟥
	High	🟨	🟨	🟨	🟥	🟥
	Medium	🟩	🟨	🟨	🟨	🟥
	Low	🟩	🟩	🟨	🟨	🟥
	Negligible	🟩	🟩	🟩	🟨	🟨

Healthcare Consulting & Planning sal

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Roles and Responsibilities

Roles and Responsibilities of various groups

- Responsible Organizations
- Responsible Organization’s Top Management
- Medical IT network risk manager
- Medical device manufacturers

Responsible Group
Healthcare Delivery Organization (Hospital)

- Owner of the risk management process for medical IT network … a process spanning
- Planning
- Design
- Installation
- Device connection
- Configuration
- User/operation
- Maintenance
- Device decommissioning

Roles and Responsibilities – Top Management

Establish policies for

- Risk management process
- Determining acceptable risk (considering relevant standards & regulations)
- Balancing 3 key properties with mission of organization
- Ensure provision of adequate resources
- Assignment of adequate personnel including assignment of a medical IT network risk manager (maybe staff or contractor)
- Enforcement of responsibility agreements
- Review results of risk management activities to ensure continuing suitability & effectiveness of RM process

HCP Healthcare Consulting & Planning sal

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Medical IT Network Risk Manager (typically a Clinical Systems Engineer)

- Responsible for Design, maintenance & performance of risk management process
- Reporting risk management process to Top Management
- Managing communication between internal & external participants in risk management
  - Medical device manufacturers
  - IT suppliers of equipment, software, services
  - Clinical users
  - Technical departments responsible for medical device support

Medical Device manufacturers

- Provide responsible organizations with documents which give
  - intended use of medical device and its connection to IT network
  - instructions necessary for the safe & effective use of medical
  - equipment
  - required characteristics, technical specification & configuration of IT
  - networks on which medical device is to be incorporated
  - intended information flow between medical device, network
- Provide responsible organizations with information from
- manufacturer’s risk management file that
  - is necessary for that responsible organization to perform risk
  - management process
  - describes any residual risk that needs to be managed by responsible
  - organization

HCP Healthcare Consulting & Planning sal

ECRI Institute
The Discipline of Science. The Integrity of Independence.

Major Activities

- Establish Risk Management Policy
- Establish/maintain a Risk Management File
- Define assets
- Document medical IT networks
- Establish Responsibility Agreements
- Establish a Risk Management Plan for each network
- Conduct Risk Management

IEC 80001- Management Plan

Healthcare Consulting & Planning sal

ECRI Institute

The Discipline of Science. The Integrity of Independence.

Plan

- Rule #1: Assess your risks… ALL of your risks!
  - Use IEC 80001-1 – "Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities"
  - Addresses risk to the patient, medical device, and cybersecurity
  - Puts a "medical device spin" on existing IT best practices
- Derived from:
  - ISO/IEC 20000-1:2011 - Information technology -- Service management -- Part 1: Service management system requirements
  - Information Technology Infrastructure Library (ITIL) - a set of practices that focus on aligning IT services with the needs of business (Gave rise to ISO/IEC 20000)
  - ISO 14971:2007 - Medical devices -- Application of risk management to medical devices

Risk Management Policy

- balances 3 key properties (i.e., safety, efficacy, security) with hospital mission
- establishes risk acceptability criteria for each key property
- describes processes that apply to medical IT networks .. i.e.,
  - event management
  - change management
  - configuration management
  - monitoring

Risk Management File

- Contains documents including
  - risk management material supplied by manufacturer
  - asset information
  - configuration management info
- Responsibility agreements
- Provides traceability for each identified hazard to
  - risk analysis
  - risk evaluation implementation & verification of risk control measures assessment of the acceptability of residual risks with appropriate approvals

Inventory Critical System Assets

- **Inventory assets (i.e., essential hardware, software, data)**
  - specific components of medical IT network and all attached medical devices
  - operation characteristics of IT infrastructure (e.g., bandwidth)
  - configuration management information
  - medical application software
  - data maintained/transmitted
  - operating & service histories
  - relevant security information

Document Medical IT Networks

- Document Medical IT-networks
  - physical & logical network configurations
  - applied standards & conformance statements
  - client / server structure
  - network security
  - (i.e., reliability, integrity, confidentiality) provisions
  - any planned changes, upgrades, enhancements

Responsibility Agreements

- **Establish Responsibility Agreements …for each project (e.g., medical device incorporation, configuration change, planned maintenance) … a Responsibility Agreement is established that defines responsibilities of all relevant stakeholders**
  - **name(s) of persons responsible for risk management associated with activities covered by responsibility agreement**
  - **description of scope of activities covered by responsibility agreement**
  - **list of medical devices & other equipment associated with project**
  - **list of manufacturers & other organizations involved in project and the information they are required to provide (e.g., instructions for connecting and disconnecting device from network and for performing risk analysis)**

Risk Management Plan

- Establish Risk Management Plan for each medical IT network that includes
- description medical IT network
  - list of stakeholders to be informed of hazards to ensure risk awareness
  - defined use & expected benefits
  - reasons for incorporating medical devices
  - impact on mfg.'s intended use of any medical devices incorporation on IT network
- Description of activities, roles, responsibilities for all stakeholders involved in operating/maintaining medical IT network (including identification of new hazards)
- network monitoring requirements

Risk Assessment

Focus on critical clinical systems

- Manage to minimize risks to safety, efficacy & security… including potential harm to patients
  - before introducing medical device on IT network
  - during the device life-cycle
  - removal of device
  - change or modification of device, items, components

Clinical Systems Engineer

The CSE coordinates an enterprise-wide program to insure the effective deployment, integration, and support of interconnected medial systems

- Maintains current inventory of networked systems
- Coordinates security management process including risk (e.g., criticality & probability) and vulnerability analysis associated with networked systems
- Coordinates with stakeholders a process to prioritize, develop and implement plan to manage/mitigate identified risks
- Works with stakeholders to insure effective deployment, integration, and support of new medical systems into legacy systems.
- Identifies and manages appropriate software upgrades, security patches and anti-virus installs for interconnected/integrated medical systems according to industry best practices
- Conducts Root Cause Analysis (RCA) and Failure Mode Effects Analysis (FMEA) on incidents involving networked medical systems
- Monitors and adopts industry "Best Practices" to insure security of data maintained and transmitted across interconnected and integrated medical systems
- Educates stakeholders on security and other implications associated with the proliferation of networked systems.

The way ahead

- Engage device/system owners, clinical engineering, IT, risk management, medical device manufacturers, and other stakeholders in a discussion of this issue
- Begin gathering information (particularly on critical devices/systems) from owner/operators, clinical engineering, IT, MDMs, etc in order to begin what will be a reiterative and continually refined process
- Develop a Security & Risk Management process for your organization that is appropriately scaled and do-able. Look to IEC 80001-1 and other industry practices for guidelines
- Learn & improve as you go … but get started.

References

- Business Associate Agreements
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- Hospital Failure Mode Effects Analysis (HFMEA)
  - http://www.patientsafety.va.gov/professionals/onthejob/HFMEA.asp
  - http://www.ccdsystems.com/Products/RootCauseAnalyst/PapersandArticles/CommonErrorsinHFMEA.aspx
- Manufacturer Disclosure Statement for Medical Device Security (MDS2)
  - http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
- ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsibilities and activities*
  - http://www.aami.org/publications/standards/80001.html

References : continued

- IT Infrastructure Library – http://www.itil-officialsite.com
- DMZ's, VRF's and MPLS –
  - https://en.wikipedia.org/wiki/DMZ_%28computing%29
  - https://en.wikipedia.org/wiki/Virtual_Routing_and_Forwarding
  - https://en.wikipedia.org/wiki/Multi-protocol_Label_Switching
- Medical Device Definition - http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm
- Manufacturer Guidance on Cybersecurity - http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm077812.htm
- Healthcare Facility Guidance on Cybersecurity - http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070634.htm
- MedWatch Problem Reporting Program - http://www.fda.gov/MedicalDevices/Safety/ReportaProblem/FormsandInstructions/default.htm

Acknowledgements

- Erin Sparnon
  Engineering Manager, Health Devices Group
  ECRI Institute

- Rick Hampton
  Wireless Communications Manager
  Partners Healthcare System

Thank you

Healthcare Consulting & Planning sal

ECRI Institute
The Discipline of Science. The Integrity of Independence.