Part 1 of 3: Best Practices for Medical Device Cybersecurity Management

Stephen L. Grimes, FHIMSS FAIMBE FACCE
Principal Consultant
Strategic Healthcare Technology Associates, LLC
Stephen.Grimes@SHCTA.com

CE-IT Collaboration Town Hall Series
March 23 - 24, 2016
About the Speaker

Stephen L Grimes, FHIMSS FACCE FAIMBE

Managing Partner & Principal Consultant
Strategic Healthcare Technology Associates, LLC

Mr. Grimes is recognized as one of the industry’s first and most prominent experts on the issue of medical device security. He originally drew the industry’s attention to the growing risks associated with medical device security compromises through a series of articles, presentations and national symposia beginning in 2001. In 2004, Mr. Grimes authored the ACCE/ECRI Information Security for Biomedical Technology: A Compliance Guide ... the industry’s first definitive guide for healthcare delivery organizations (HDOs) on identifying and mitigating medical device security risks. Also in 2004, he conceived of and managed the development of the Manufacturer’s Disclosure Statement for Medical Device Security (MDS²) while chairing HIMSS’ Medical Device Security Task Force. He later participated on the NEMA standards committees that led to the adoption of the 2005 and 2013 versions of the MDS² as formal industry standard. He also served as a member of the US/TAG to ISO/TC 215 HEALTH INFORMATICS and Joint Working Group 7 that developed the 2010 ISO/IEC/AAAMI standard IEC 80001-1: Application of risk management for IT-networks incorporating medical devices.

Over the years to the present, Mr. Grimes has continued to speak and write on how healthcare delivery organizations (HDOs) need to address the evolving medical device security threat. During his eight-year tenure (2007-2015) at ABM Healthcare Support Services in the capacity of Chief Technology Officer and senior consultant, he has also developed programs, procedures and tools for that organization’s 300+ clients (with medical device inventories totaling over 500,000) that addressed data security management in the device life cycle.
Medical Devices & Systems:
~ 10 Million in U.S. Hospitals today

Exponential growth of medical devices (including consumer platforms & wearables running medical applications) in hospitals, clinics, medical offices, workplace, schools, homes, etc.

You can’t manage what you can’t measure
Factors complicating Security Management of Medical Devices
Medical Devices & Systems: Differences in Impact of Failure

Security (i.e., data confidentiality, integrity or availability) compromise can
✓ have serious financial impact
✓ have serious operational impact
✓ have serious reputation & legal impact

Security compromise of Medical Device can result in death or serious injury
Medical Devices & Systems: Who has Responsibility?

**INFORMATION TECHNOLOGY**

IT knows data security

BUT ...
IT generally has limited knowledge of type, number and vulnerabilities associated with medical devices

**CLINICAL / BIOMEDICAL ENGINEERING**

CE knows number/location of medical devices & understands criticality, lifecycle, and supportability issues

BUT ...
CE generally has limited knowledge of data security issues
Medical Devices & Systems: Degree of Integrated Support

Currently 40% Networked (and rapidly growing)

Systems of Systems

Overlapping Responsibility?

INFORMATION TECHNOLOGY

CLINICAL / BIOMEDICAL ENGINEERING

Still significant disconnect ... resulting in coverage gaps
Medical Devices & Systems:
Examples of Commonly Connected Categories of Equipment

Examples of networked medical equipment types:

- Physiologic monitors ............... hundreds
- Defibrillators ..................... scores
- Infusion pumps ..................... thousands
- Anesthesia units ................... scores
- Ventilators ......................... scores
- Extracorporeal Assist ............... up to dozen
- Vital sign monitors ............... hundreds
- CT & MRI scanners ............... up to score
- Fetal monitors ..................... scores
- Laboratory analyzers ............. scores
- Diagnostic ultrasound .......... scores
- Patient beds ....................... hundreds
- Electrocardiographs ............. scores
- Injectors, contrast media ........ scores

~10 to 15 medical devices per bed
typical 500 bed hospital may have 7,500 medical devices
Medical Devices & Systems:
Examples of how PHI and other data is acquired, maintained or transmitted
Medical Devices & Systems:
> 5% are considered Critical (i.e., can compromise can result in death or serious injury)

Examples of data that is subject to compromise:

- images from x-ray, CT, MRI, ultrasound,
- waveforms from ecg, bp, eeg
- demographic information
- vital signs (e.g., heart rate, BP, pulse ox, resp, temp)
- alarm parameters
- drug type & dosage
- control and configuration settings (e.g., infusion rates, therapy timers, anesthesia & radiation delivery settings)
- laboratory (e.g., chemistry) results
- sounds from blood flow, respiration
Medical Devices & Systems:
Common Types of Network Connections

Types of connections via wired or wireless networks:

- Connect to electronic medical record (EMR)
- Connect to image/data storage (e.g., PACS)
- Remote access to data/images (e.g., physician, clinicians)
- Remote service (e.g., manufacturer updates, troubleshooting, repair)
- Remote management (e.g., clinical updates like drug libraries for infusion pumps)
- Remote control (e.g., modify alarms, configuration settings, level of therapy)
- Intra-communication between medical devices (e.g., diagnostic device “informing” therapeutic devices .... e.g., monitor controlling opioid delivery)
Medical Devices & Systems:
Differences in Development, Updates, Management

- As it currently stands, medical devices typically have a **7-8 year product development cycle**
  - features including OS & software are “baked” in years before product release ... and often years after consumer equivalent of software and hardware has moved to next generation
- Medical devices generally cannot be safely patched with OS updates or have virus software applied until patches have been specifically tested & approved by the device manufacturer
- Medical devices cannot have agents (e.g., SNMP) installed to facilitate network management
Actions Required by Healthcare Delivery Organizations
Get data to determine the extent of the exposure .... *can’t effectively manage what you can’t identify and measure!* 

- Identify numbers, types and locations of medical devices & systems ... look to computerized maintenance management systems (CMMS)
- type of data transmitted, stored (e.g., PHI?)
- determine configuration
  - OS & applications (including versions)
  - networkable, network MAC & IP addresses, protocol
  - existing connections (e.g., with what other services & devices are “authorized” to exchange data? ... including remote access)
  - default device settings
- identify security features (MDS²)
**Medical Devices & Systems:**
*Identify gaps and establish processes to address medical device security issue*

**Security Related Processes** – *close gaps between IT & Medical processes!*

- educate all stakeholders regarding risks
- acquisition processes (i.e., acquire with security in mind)
- security & risk assessment processes ... engage appropriate stakeholders to determine
  - criticality of system & data
  - probability of failure
- establish & implement mitigation plan to identify, prioritize and address risks using administrative, technical & physical safeguards ... and monitor effects.
  - define roles, responsibilities (CE/HTM, IT, vendor/mfg, leadership)
  - build for resilience (e.g., backups, redundancy)
  - business associate agreements (BAA) for vendors that service medical equipment
  - medical grade networks that provide high bandwidth & security
- disposal processes (e.g., data sanitizing)
Resources for Healthcare Delivery Organizations
Resources for Managing Medical Device Security: 
Manufacturer Disclosure Statement for Medical Devices Security (MDS²)

- MDS² contains security related information from the device manufacturer (revised in 2013 to comply with ISO 80001-1)
- Most major manufacturers (e.g., Philips, GE, Siemens, etc.) offer completed MDS² on each of their medical equipment models
- Information on the MDS² is intended for use by medical device owners who want to use device’s security features effectively
- Originally developed by HIMSS and now a NEMA standard

http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
Medical Devices & Systems:
FDA’s role

FDA provides
- Guidance for manufacturers and hospitals ... and requirements for manufacturers
  ... on digital health and cybersecurity issues

FDA requires manufacturers
- have their devices cleared or approved (depending on Class) by FDA
- to remain vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity
- to be responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance

FDA recommends that hospitals & providers
- work with manufacturers to evaluate their network security and protect their installed systems
With respect to medical device cybersecurity, FDA primarily focuses on regulations and guidance for manufacturers ...

Manufacturers are encouraged to take appropriate precautions
✓ to ensure that vulnerable products they produce are designed to be secure
✓ to work with healthcare delivery organizations (HDOs) and other stakeholders as necessary to ensure they remain secure throughout their life-cycle

The FDA has produced a series of Guidance
✓ Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software (Jan 2005)
✓ Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct 2014)
✓ Draft Guidance for Industry: Postmarket Management of Cybersecurity in Medical Devices (Jan 22, 2016)
Resources for Managing Medical Device Security:
*Medical Device Innovation, Safety, and Security (MDISS) Consortium*

- Medical Device Risk Assessment Platform (MDRAP) Tool [https://mdrap.mdiss.org/](https://mdrap.mdiss.org/)
  - Based on tool developed for evaluating both application and device risk
  - Provides a risk score by category and allows comparative studies across several different devices
  - Useful in pre-purchase assessment of security risks (helps in selection process and in preparing risk mitigation steps)
  - Latest version of MDRAP builds on operational questions onto MDS² to help manufacturers and healthcare systems better understand the security profile of their devices
Resources for Managing Medical Device Security:
Focus of ANSI / AAMI / IEC 80001-1 : 2010

Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities & activities

- The new standard focuses on how to manage risks associated with
  - **safety** ... preventing physical injury or damage to people, property or the environment
  - **effectiveness** ... insuring the intended result is produced
  - **data & system security** ... insuring that information “assets” (i.e., data & systems) are reasonably protected from compromises to confidentiality, integrity and availability

- Defines roles & responsibilities
- Defines key activities
Resources for Managing Medical Device Security
Application of Risk Management for IT-Networks Incorporating Medical Devices
Supplemental Guides

- ISO/IEC 80001-2-1:2012 *Step by step risk management of medical IT-networks; Practical applications and examples*
- ISO/IEC 80001-2-2:2012 *Guidance for the disclosure and communication of medical device security needs, risks and controls*
- ISO/IEC 80001-2-4:2012 *General implementation guidance*
- ISO/IEC 80001-2-5:2014 *Guidance for distributed alarm systems*
- ISO/IEC 80001-2-7:2015 *Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*
- ISO/IEC 80001-2-8: under development *Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*
The introduction of *connected medical devices* are growing at nearly exponential rates in healthcare organizations.

Significant cultural and process gaps still exist between most those supporting traditional Information Technology (IT) and those clinical engineering (CE) / healthcare technology management (HTM) services supporting medical devices & systems.

Traditional data security measures are often not safe or appropriate for use on medical devices ... special precautions must often be taken.

Healthcare organizations should be proactive and begin addressing medical device security by assessing the numbers and kinds of devices involved ... and then evaluating the risks associated with the use of those devices.

Healthcare organizations should learn to use the tools (e.g., MDM software, MDS2, ANSI/AAMI/IEC 80001, MDISS MDRAP) that are designed to help identify and mitigate any security risks.
Thank You

CE-IT Collaboration Town Hall Series
March 23 - 24, 2016

Stephen.Grimes@SHCTA.com
Medical Device Cybersecurity
Theory into Practice

Scot Copeland, BSITSEC, MCP, SEC+
Medical I.T. Network Risk Manager
Scripps Health San Diego, CA
Medical Device Risk Management

• Instituted formal role- Medical I.T. Network Risk Manager
  • Clinical Systems Specialist Program
  • I.T. industry certification incentives

• IEC80001 Tool Kit for Risk Management
  • Risk Register
  • Change Permit
  • Risk Analysis Template
  • Risk Report

• Development and implementation of Medical Device Security organizational group
  • Medical Device Information Security Committee
  • Medical I.T. Risk Management Plan
Socialize Your Program-Get Invited!

- Involvement with I.T. functions
  - Information Architecture Solution Designs/I.T. Technical Reviews
  - Capital Purchase Review RFI/RFP (IEC 80001 summary, MDS2)
  - I.T. Change Management
  - I.T. Project Management

- Involvement in I.T. Management and Administrative committees
  - I.T. Risk Management
  - Information Security Steering Committee
  - I.T. Policies and Standards Committee
  - Security Risk Management Committee
Emerging Medical Device Security Challenges

- **Cloud/ASP**
  - Medical devices requiring web support for backend application, licensing, data housing for user access, etc.
  - Extensive vetting required for Business Partners for web support
  - Medical Device often provided without security control capabilities now with ePHI and internet access.

- **Vendor/Partner EHR integrations**
  - Medical Device systems provided and operated by Vendors needing EHR access and/or web access
  - Same issues as Cloud/ASP but with added risk due to data systems integration

- **Software as a Medical Device**
  - Non-Medical device becomes a medical device
  - I.T. system components take on added risk due to software

- **Unsecured data at rest (Privacy)**
  - Patient Databases local to medical device in (often unsecured) clinical environment (Portable devices, surgical, endoscopic, etc.)
  - Network data repository (shared drive) solution not simple answer

- **Medical devices as malware and intrusion vectors**
  - Many medical device systems have unsecured or duplicate paths through/around hospital perimeter defenses
  - Documented instances of network intrusion via unsecured medical devices/system
Current/Future Security Activities

• Philosophy to incorporate medical devices as fully as possible into current evolutionary flow of infrastructure security capabilities

• Mobile Device Management
  • Develop security solutions for mobile device based medical devices incorporating current MDM capabilities

• VPN access for remote support
  • Migrate all remote support to standard infrastructure VPN access

• Firewall/segmentation
  • Migrate medical devices into infrastructure firewall policy

• IPS/Threat Monitoring
  • Employ firewall monitoring and IPS data to develop threat data for medical devices

• Vulnerability Scanning
  • Develop Vulnerability Scanning program for medical devices to provide data for threat analysis

• Security Information and Event Monitoring (SIEM)
  • Incorporate Medical device servers into current SIEM program. (Log file aggregation and analysis)

• User Awareness
  • Developed Medical Device Security Awareness module as part of ongoing culture development
Medical Device Cybersecurity:

From Best Practices to Standards

Todd Cooper
Principal, Breakthrough Solutions Foundry
Co-Chair, IEC/ISO JWG7 “80001”
U.S. Head of Delegation, ISO/TC 215 Health Informatics
Co-Founder, HL7 Health Care Devices
Board, IHE International
Standards are about …

- Engaging top international experts
- Leveraging community experience
- Baking in best practices

... to enable & accelerate industry!
Medical device cybersecurity is ...

✓ More than medical devices
✓ More than security

... solutions must address the entire landscape – not just narrow verticals
Health Devices vs. Medical Devices

1. Consumer products for health monitoring: These devices -- such as FitBit, Nike FuelBand, or Withings -- generally communicate using Bluetooth to nearby personal mobile devices.

2. Wearable, external medical devices: This category includes portable insulin pumps which often use proprietary wireless protocols to communicate.

3. Internally embedded medical devices: Pacemakers and other medical devices are implanted in the patient but communicate wirelessly, either with proprietary wireless protocols or Bluetooth.

4. Stationary medical devices: These devices, such as hospital-based chemotherapy dispensing stations or homecare cardio-monitoring for bed-ridden patients, often use more traditional wireless networks, such as WiFi networks in hospitals or patients’ homes.

(Authors: Jason Healey, Neal Pollard, and Beau Woods; March 2015)
FIGURE 2 - Categories of Health IT Functionality

Health IT functionality can be broadly grouped into three categories: 1) administrative health IT functionality, 2) health management health IT functionality, and 3) medical device health IT functionality. Each of the three proposed categories can be designed for use by health care entities, health care providers, patients, and consumers. Administrative functionalities, including but not limited to admissions, billing and claims processing, practice and inventory management, scheduling, general purpose communications, analysis of historical claims data to predict future utilization or cost-effectiveness, determination of health benefit eligibility, population health management, reporting of communicable diseases to public health agencies and reporting on quality measures pose limited or no risk to patient safety. The Agencies believe no additional oversight of these types of products is necessary. Health management functionalities include but are not limited to health information and data exchange, data capture and encounter documentation, electronic access to clinical results, some clinical decision support, medication management, electronic communication and coordination, provider order entry, knowledge management, and patient identification and matching. Health management health IT functionalities are the primary focus of the framework described in this report. If a product with health management health IT functionality meets the statutory definition of a medical device, FDA does not intend to focus its oversight on it - because the Agencies' proposed strategy and recommendations for a risk-based framework for health management health IT can help to assure a favorable benefit-risk profile of these functionalities. FDA would focus its oversight on medical device functionality because, in general, these functions, such as computer aided detection software and remote display or notification of real-time alarms from bedside monitors, present greater risks to patient safety than health IT with administrative or health management functionality.
Medical Devices . . .

- 1,000’s – 10,000’s per facility
- 7–10 year Cycles => Legacy technology!
- Historically little to no security consideration
  - Software locked down vs. rapid-response patches
  - Security awareness/competency very low
  - Basic configuration management is a challenge
Plugging unauthorized devices or accessories into USB ports on medical devices can cause the medical devices to malfunction. Direct effects on medical device operation—for example, causing a physiologic monitor to reboot—have been observed in clinical practice.

Possible problems include instances in which:

- The device shuts down, and the patient does not receive therapy.
- The device settings are changed or performance is compromised.
- A patient monitor ceases to monitor the patient or fails to alarm for problems that require attention.

Uncontrolled access to medical device USB ports could also lead to a security breach, putting the patient’s data and the healthcare facility’s systems at risk.

Facilities need to develop and implement a policy on the appropriate use of USB ports on medical devices.
Standards Landscape
Supporting Medical Device Cybersecurity
ISO/IEC 80001 Standard & Guidance provides a framework for applying proven risk management principles to networked medical technology deployment & use
80001-1 Revision...

- New working title:
  Secure, safe and effective implementation and clinical use of connected medical devices and health software – Part 1: Application of risk management

- 80001 Focus is on “right”; 82304/62304 on left

- “Foundations” document covers topics across the tech. lifecycle

- Data quality / data life cycle to be integrated as well
80001 Key Properties

(in order of priority)

SAFETY:
Freedom from unacceptabe risk of physical injury or damage to the health of people or damage to property or the environment

EFFECTIVENESS:
Ability to produce the intended result for the patient and the responsible organization

DATA AND SYSTEM SECURITY:
An operational state of a medical IT-Network in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability

Note: ISO 14971 for medical devices is focused on patient safety risk management

Privacy?
Ask these 4 questions:

1. What could go wrong?
2. How can it happen?
3. What can we do about it?
4. How do we know that we’ve done enough?
ISO / IEC 80001 Guidance Documents

Guidance documents facilitate understanding & implementation:

80001-2-1 Step-by-Step Risk Management
80001-2-2 Communicating Security Needs, Risks & Controls
80001-2-3 Wireless Guidance
80001-2-4 HCO Implementation Guidance
80001-2-5 Distributed Alarm Systems
80001-2-6 Responsibility Agreements
80001-2-7 Conformance Self-assessment Guidance
80001-2-8 Mapping Security Controls to 19 Capabilities
80001-2-9 Security Assurance Case for 19 Capabilities

NOTE: 80001-2-9 is in final development …
ISO/IEC 80001 Security Documents

80001-1 Application of risk management for IT-networks incorporating Medical Devices – Part 1: Roles, responsibilities and activities

80001-2-2 Guidance for the disclosure and communication of medical device security needs, risks & controls

80001-2-8 Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

80001-2-9 Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities

+ MDS²:2013 Manufacturers Disclosure Statement for Medical Device Security (harmonized with 80001-2-2)
19 Capabilities from 80001-2-2 and disclosed in MDS²

<table>
<thead>
<tr>
<th>Capabilities</th>
<th>Concepts:</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALOF: Automatic logoff</td>
<td></td>
<td>2</td>
<td>2</td>
<td>-1</td>
<td></td>
</tr>
<tr>
<td>AUDT: Audit controls</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>AUTH: Authorization</td>
<td></td>
<td>2</td>
<td>2</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>CNFS: Configuration of security features</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CSUP: Cyber security Product upgrades</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>DTBK: Data backup and disaster recovery</td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMRG: Emergency access</td>
<td></td>
<td>2</td>
<td></td>
<td>-1</td>
<td></td>
</tr>
<tr>
<td>DIDT: HEALTH DATA de-identification</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGAU: HEALTH DATA integrity and authenticity</td>
<td></td>
<td>2</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>STCF: HEALTH DATA storage confidentiality</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLDP: Malware detection/protection</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>NAUT: Node authentication</td>
<td></td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>PAUT: Person authentication</td>
<td></td>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>PLOK: Physical locks on device</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>SGUD: Security guides</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SAHD: System and application hardening</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>RDMP: Third party components in product lifecycle roadmaps</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>TXDF: Transmission confidentiality</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TXIG: Transmission Integrity</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.13 Person authentication – PAUT

Applicable: 
Standard: IHE ATNA profile (Audit Trail and Node Authentication)
IHE EUA (Enterprise User Authentication)
IHE XUA (Cross-Enterprise User Assertion)

Policies: SANS Security Policy Project
Local HDO IT Policies

Reference material: N/A

Requirement goal: Authentication policies need to be flexible to adapt to HDO IT policy. This requirement as a logical place to require person authentication when providing access to HEALTH DATA.

User need: Capability of managing accounts on a modality to protect HEALTH DATA access.
Desirable to link to personal settings/preferences.
Support for stand-alone and central administration.
Single sign-on and same password on all workspots.
To detect and prevent person falsification (provide non-repudiation).
Role based access control (RBAC) capability desirable.
| **NIST SP-800-53** | Security and Privacy Controls for Federal Information Systems and Organizations |
| **IEC 62443-3-3** | Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels |
| **ISO/IEC 27002** | Information technology – Security techniques – Code of practice for information security management |
| **ISO 27799** | Health informatics -- Information security management in health using ISO/IEC 27002 |
### Person authentication – PAUT Controls

<table>
<thead>
<tr>
<th>ISO/IEC 27002</th>
<th>ISO 27799</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>Policies for information security</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Review of the Information Security Policy</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Mobile device policy</td>
</tr>
<tr>
<td>6.2.2</td>
<td>Teleworking</td>
</tr>
<tr>
<td>9.2.1</td>
<td>User registration and de-registration</td>
</tr>
<tr>
<td>9.2.4</td>
<td>Management of secret authentication information of users</td>
</tr>
<tr>
<td>9.4.2</td>
<td>Secure log-on procedures</td>
</tr>
<tr>
<td>10.1.1</td>
<td>Policy on the use of cryptographic controls</td>
</tr>
<tr>
<td>10.1.2</td>
<td>Key management</td>
</tr>
<tr>
<td>12.1.1</td>
<td>Documented operating procedures</td>
</tr>
<tr>
<td>12.1.2</td>
<td>Change management</td>
</tr>
<tr>
<td>12.4.1</td>
<td>Event logging</td>
</tr>
<tr>
<td>12.4.3</td>
<td>Administrator and OPERATOR logs</td>
</tr>
<tr>
<td>12.7.1</td>
<td>Information systems audit controls</td>
</tr>
<tr>
<td>18.1.1</td>
<td>Identification of applicable legislation and contractual requirements</td>
</tr>
<tr>
<td>18.1.5</td>
<td>Regulation of cryptographic controls</td>
</tr>
<tr>
<td>18.2.2</td>
<td>Compliance with security policies and standards</td>
</tr>
</tbody>
</table>

Example of mapping from 27002 / 27799 to fulfill the PAUT security capability
3.6 SECURITY CASE

reasoned, auditable artefact created that supports the contention that its top-level CLAIM (or set of CLAIMS) is satisfied, including structured and explicit argumentation and its underlying evidence and explicit assumptions that support the CLAIM(s)

Note 1 to entry: As SECURITY CASE contains the following and their relationships:

- one or more CLAIMS about the critical property security;
- ARGUMENTS that logically link the evidence and any assumptions to the CLAIM(s);
- a body of evidence and possibly assumptions supporting these ARGUMENTS for the CLAIM(s);
- justification of the choice of the top-level CLAIM and the method of reasoning.

[Source: Adapted and amended definition of "ASSURANCE case" from ISO/IEC 15026-1:2013, definition 3.1.3 – specifically addressing security as the critical property]

4 ASSURANCE Case

An ASSURANCE case is a structured, evidence based ARGUMENT used to demonstrate CONFIDENCE that a system holds a particular critical property. ASSURANCE cases have been commonly applied to the safety domain, specifically addressing safety concerns for systems, however the use of ASSURANCE cases has expanded and nowadays address other critical properties such as dependability, reliability and security across a range of safety critical domains such as automotive, railway, defence, aviation etc. An ASSURANCE case is called a safety case when used to argue the safety of a system. Similarly they are referred to as SECURITY CASES and dependability cases when arguing security and dependability respectively.
80001-2-9 Top Level Security Case

Figure 7 - Leading components – Steps 1 - 9
80001-2-9 PAUT Security Case Pattern

Figure A.1 – Examplar SECURITY PATTERN

Note: Leverages PAUT Security Controls from 80001-2-8
Manufacturer Disclosure Statement for Medical Devices Security (MDS2)

- Medical Device Security should be part of the Procurement Process:
  - RFP Language
  - Request NEMA MDS2
- Developed in cooperation by HIMSS and NEMA
- New version Oct. 2013
- More detailed (2 -> 6 pages)
- Now harmonized with IEC 80001 technical controls

http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
IEEE: Building Code for Medical Device Software Security

- Nov. 2014 Workshop
- Released May 2015
- Addressing device manufacturers’ secure SW design needs.
- Key Elements:
  - Avoid vulnerabilities
  - Cryptography
  - SW integrity
  - Impede attackers
  - Enable detection
  - Safe degradation
  - Restoration
  - Maintain operations
  - Support privacy

MEM Whitepapers:
- Cybersecurity (2011: Education & Problem Baseline)
- Medical Device Patching (2015)
co-authored by MDISS and IHE
## Table 1—New Entries to the List of Recognized Standards

<table>
<thead>
<tr>
<th>Recognition No.</th>
<th>Title of standard</th>
<th>Reference No. and date</th>
</tr>
</thead>
</table>

(See U.S. Federal Register/Vol. 78, No. 151/Tuesday, August 6, 2013; Docket No. FDA–2004–N–0451)
Postmarket Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Document issued on: January 22, 2016

(See http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm)
Standards Applied
Program: Archimedes

✓ Leading researchers for device cybersecurity (Dr. Kevin Fu)
✓ Working in collaboration with government and healthcare providers
  o FDA CDRH
  o Mayo and University of Michigan Health
Program: NCCCOE (NIST)

Health IT Sector

- Consumer/Retail
- Energy Sector
- Financial Services Sector
- Health IT Sector
- Transportation Sector

The center is conducting projects to help improve the cybersecurity postures of health care organizations. Find out more below.

**Securing Electronic Health Records on Mobile Devices**

An platform for health care providers to securely document, maintain, and exchange electronic patient information among mobile devices.
> Find out more and download the NIST Cybersecurity Practice Guide, SP 1800-1.

**Wireless Medical Infusion Pumps**

Helping health care providers secure wireless medical infusion pumps on an enterprise network.
> Find out more about this project.

To stay up-to-date on project milestones, sign up for our Health IT email topic, or participate in our discussion forums.
Program: MDISS

Medical Device Innovation, Safety and Security Consortium

Medical Device Risk Assessment Platform

✓ Dr. Dale Nordenberg, lead researcher
✓ Working closely with the FDA

www.MDISS.org
Program: NH-ISAC

NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE I
NH-ISAC | NATIONAL HEALTHCARE & PUBLIC HEALTH CRITICAL INFRASTRUCTURE PROTECTION

National Critical Infrastructure Information Sharing & Analysis Centers (ISACs) represent a public/private partnership comprised of critical infrastructure sector-specific ISACs, recognized by their respective sector critical infrastructure owners and operators, federal sector-specific agencies (SSAs), Sector Coordinating Councils (SCCs), intelligence agencies and the National Council of ISACs (NCI Directorate). The National Council of ISACs's provides the framework for valuable interaction across critical infrastructures (between and among the ISACs), the private sector and with government.

Safe harbor information exchange?  www.nhisac.org
Dr. Anita Finnegan, Lead
Developed 80001-2-8 & -2-9 Guidance
www.novaleah.com/select-evidence/
Tools: GessNet

- Automation of the risk management process
- TurboAC includes support for …
  - Risk Management Process Automation
  - Assurance Case Development
  - Evidence (Supporting Document) Management
- Increasingly used by medical device vendors
- [www.gessnet.com](http://www.gessnet.com)
Fuzz Testing, Protocol Test Suites, etc.

Threat intelligence platform / situational awareness

(www.codenomicon.com)
Asset Management
- Asset Discovery & Inventory
- Configuration Tracking
- Security Testing
- Risk Classification

Procurement
- Security Requirements:
  - Security Properties
  - Vulnerability Updates
  - Supply Chain Mgmt.

Security Risk Analysis
- HIPAA: C-I-A of PHI
- Joint Commission:
  - Medical equipment safety risks
  - Inventory; categorize; incidents
  - Maintenance, inspection, testing

Lifecycle Mgmt.
- Onboarding -> EOL
- Maintenance & Repair
- Change Mgmt. & Patching
- Remediation

Risk Mitigation
- Network Segmentation (VLAN)
- Network Threat Detection
- Incident Response
- Procedures & Handling

Risk Management
- Ongoing Process
- Recovery & Forensics
- Decision Making
- Stakeholder Engagement

Incident Analysis
- Impact & Technical Analysis
- Manufacturer Feedback
- Enablement & Training

Product support for each of these Best Practice Areas
Conclusions
Standards are foundational ...

– Engaging all stakeholders & SMEs – You!!!

– Trust & Information Sharing must be achieved

Elliot: “How hard can it be?”

Todd: “What could possibly go wrong?!”
Additional Information
9. Cybersecurity: Insufficient Protections for Medical Devices and Systems

The growing trend toward the networking and connectivity of medical devices is associated with a corresponding increase in the vulnerability of these devices to malware and malicious attacks. Despite little evidence to date of direct harm to patients from the exploitation of cyber vulnerabilities, cybersecurity is nevertheless a patient safety consideration that will require increased attention in the coming years.

As noted by FDA, cybersecurity protections are intended to prevent the exploitation of medical device cyber vulnerabilities that otherwise could lead to device malfunctions, the disruption of healthcare services, inappropriate access to patient information, or compromised data integrity within an electronic health record (FDA 2014 Sep).
Events such as the following illustrate the need for such protections:

- Devices that became infected with malware caused a hospital to have to temporarily shut down its catheterization lab.
- Many healthcare organizations have had to inform patients and the community at large that protected health information (PHI) had been released inappropriately or even stolen. Breaches such as these compromise the security and privacy of patient data, and they can lead to large fines and negative publicity for the healthcare organization.
- A few researchers have identified specific vulnerabilities in some medical devices, voicing concerns about malicious actors hacking into patient care devices and harming patients directly. ECRI Institute is not aware of any instance of patient harm resulting from a device being hacked. Thus, while the theoretical risks warrant observation, the actual risk to patient safety from device hacking—considering the workflow and protective measures typically applied in clinical practice—appears to be minimal at this time.

Protecting medical devices against malware that could potentially affect the functionality of the device or the integrity of patient data is one key cybersecurity measure. Unfortunately, healthcare facilities face a variety of obstacles that complicate the process of keeping medical devices up to date with the recommended operating system (OS) patches and anti-malware protections. These include:

- The sheer effort required—in terms of resource allocation—to manage the ever-increasing number of networked medical devices.
- Delays in the availability of OS patches because of the need for device manufacturers to test and validate the patches before deploying them.
- The inability to apply OS patches or anti-malware software to certain medical devices (typically legacy devices) out of concern that the modification will affect the functionality of the device or void its warranty.
RECOMMENDATIONS

Clinical engineering, IT, and risk management departments should collaborate on reviewing and, if necessary, updating cybersecurity management policies. Steps that healthcare facilities can take to mitigate cybersecurity threats include:

- **Proactively assessing medical device cybersecurity risks**, working with medical device manufacturers as appropriate.

  In our January 15, 2014, *Health Devices* posting, we described Methodist Hospital of Southern California’s program for proactively identifying and addressing risks related to (1) medical data availability and integrity and (2) the security of private patient information on its networked and software-driven medical devices and systems. This initiative, which earned the facility the 2013 Health Devices Achievement Award, involved new processes and procedures both for incoming medical device inspections and for the ongoing management of devices throughout their useful life.

- **Keeping up with the latest updates and patches for OSs and anti-malware software.** This effort can be facilitated by adding security requirements into the prepurchase process (e.g., in the requests for proposal and requests for information), and making cybersecurity a factor in the selection process, as well as including language in purchase contracts regarding management of OS patches and any anti-malware software.

- **Limiting network access to medical devices through the use of a firewall or virtual LAN.** Furthermore, consider limiting the numbers and types of equipment with access to the healthcare facility IT network to only those devices requiring such connections. Segregated or “air-gapped” networks carry additional costs, but provide greater security than firewalls or virtual LANs alone and are recommended for critical infrastructure.*

- **Auditing the log-in access to all medical devices and ensuring that an appropriate password policy (or other access-control method) has been established and is being followed.**

- **Setting up a process for monitoring and reporting cybersecurity threats and events.** Events that affect medical devices and information systems (e.g., electronic health records) should be reported to entities such as FDA and ECRI Institute. In addition, if there is reason to believe the event is related to a deliberate malicious attack, it should also be reported to law-enforcement authorities such as the FBI.

More broadly, a medical device security program should parallel—or possibly even be incorporated into—the organization’s IT security program. A comprehensive plan should include:

- **A cybersecurity risk assessment** based on the facility’s current inventory of medical devices and systems and its network infrastructure.

- **Reliable safeguards against cybersecurity threats.**

- **A mitigation plan** in the event of network infiltration and malware infection.
These are the elements of 80001

1 Scope

Recognizing that MEDICAL DEVICES are incorporated into IT-NETWORKS to achieve desirable benefits (for example, INTEROPERABILITY), this international standard defines the roles, responsibilities and activities that are necessary for RISK MANAGEMENT of IT-NETWORKS incorporating MEDICAL DEVICES to address SAFETY, EFFECTIVENESS and DATA AND SYSTEM SECURITY (the KEY PROPERTIES). This international standard does not specify acceptable RISK levels.

NOTE 1 The RISK MANAGEMENT activities described in this standard are derived from those in ISO 14971 [4]. The relationship between ISO 14971 and this standard is described in Annex A.

This standard applies after a MEDICAL DEVICE has been acquired by a RESPONSIBLE ORGANIZATION and is a candidate for incorporation into an IT-NETWORK.

NOTE 2 This standard does not cover pre-market RISK MANAGEMENT.

This standard applies throughout the life cycle of IT-NETWORKS incorporating MEDICAL DEVICES.

NOTE 3 The life cycle management activities described in this standard are very similar to those of ISO/IEC 20000-2 [10]. The relationship between ISO/IEC 20000-2 and this standard is described in Annex D.
80001 Processes

1. Hazard Identification
2. Hazardous Situations & Root Cause Analysis
3. Harm Identification + Severity Estimation
4. Harm Probability Estimation
5. Risk Acceptability Evaluation
6. Risk Control Measure ID & Residual Risk Eval.
7. RCM Implementation
8. Verify RCMs
9. RCM Risk Evaluation
10. Residual Risk Evaluation & Report

Note: Though generally sequential, these steps iterate until acceptable completeness has been achieved.

(from IEC 80001-2-1, Step by Step Risk Management)
# 80001-1 Probability & Severity Scales

<table>
<thead>
<tr>
<th>Improbable</th>
<th>Very unlikely that use will result in any Unintended Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
<td>Not likely to result in any Unintended Consequence</td>
</tr>
<tr>
<td>Occasional</td>
<td>Somewhat likely to result in any Unintended Consequence</td>
</tr>
<tr>
<td>Probable</td>
<td>Very likely to result in any Unintended Consequence</td>
</tr>
<tr>
<td>Frequent</td>
<td>Unintended Consequences occur frequently or occur every time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scale</th>
<th>Safety</th>
<th>Effectiveness</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Severe injury, death</td>
<td>Planned operation is no longer possible</td>
<td>May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of information or services.</td>
</tr>
<tr>
<td>High</td>
<td>permanent impairment of body function or permanent damage of a body structure</td>
<td>Planned operation is disrupted or delayed</td>
<td>May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of information or services.</td>
</tr>
<tr>
<td>Medium</td>
<td>Temporary and minor injury, medical intervention required</td>
<td>Inconveniencing to disrupted effect on operation</td>
<td>Will result in some tangible consequence, albeit negligible and perhaps only noted by a few individuals or agencies. May cause embarrassment. Will require some expenditure of resources to repair.</td>
</tr>
<tr>
<td>Low</td>
<td>Temporary discomfort, reversible without medical intervention</td>
<td>Very limited or inconveniencing effect on operation</td>
<td>Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.</td>
</tr>
<tr>
<td>Negligible</td>
<td>Minor and short term discomfort</td>
<td>No or very limited impact on operation</td>
<td>Will have no impact if threat is realized and exploits vulnerability.</td>
</tr>
</tbody>
</table>

**NOTE:** Security included with Safety & Effectiveness