Biomedical Devices: Could Lack of Security Harm Patients?

Monday, February 29, 2016
12:45pm – 1:45pm

Stephen L Grimes, FHIMSS FAIBME FACCE
Principal Consultant
Strategic Healthcare Technology Associates, LLC
Stephen.Grimes@SHCTA.com
Conflict of Interest

Stephen L Grimes, FHIMSS FAIBME FACCE

- Has no real or apparent conflicts of interest to report.
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/AAMI 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.
Session Description & Learning Objectives

Today’s medical devices are increasingly complex, integrated and ubiquitous; securing them can be daunting. Safeguards that are appropriate for IT equipment can have disastrous effect on medical devices. This session provides an overview of the problem and offers specific guidance and tools appropriate for addressing medical device security.

Learning Objectives:

- Describe the digital security challenges presented by a largely unmitigated fleet of connected biomedical devices
- List examples of how data compromised to medical devices can have a major impact on patient safety
- Estimate the number of medical devices existing in their organizations that are vulnerable to data compromise using typical industry benchmarks
- Describe major reasons why data on microprocessor-based medical devices can be both more vulnerable and significantly more difficult to secure than data found on most IT equipment
- Identify best practice guidelines and tools available to help healthcare delivery organizations identify and mitigate medical device security risks
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
Understanding the Evolution of Medical Technology ...

including the effect of Medical & Information Technology convergence
Evolution of Medical Devices & Systems

Up until the past 10-20 years Medical Devices were *discrete* …
i.e., *one device – one patient*

Over the past 10-20 years Medical devices and systems are being designed and operated as special purpose computers … *more features* are being automated, *increasing amounts of medical data* are being collected, analyzed and stored in these devices.
Evolution of Medical Technology – Enterprise Systems

Most Systems of Systems (SoS) are unique (non-standard)

Systems of Systems (SoS) integrating:
- medical & non-medical,
- new & legacy

Radical variations in SoS from organization to organization
(no real standards for integration yet)
The nature of connectivity, inflexibility in configuration and disparity of types make medical systems particularly vulnerable.
Evolution of Medical Technology –
The Not-So-Distant Future: Migration of Apps & Data to the Cloud

Medical Applications & Data will increasingly migrate to “the Cloud”

Medical Applications will increasingly become hardware agnostic ... operating on a variety of fixed, mobile and personal platforms

Medical “device” manufacturers will become primarily software developers and makers of specialized sensors & actuators
Factors complicating Security Management of Medical Devices
Medical Devices & Systems: Differences in Impact of Failure

**INFORMATION TECHNOLOGY**

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

**MEDICAL TECHNOLOGY**

- **LIFE CRITICAL**
  - Security compromise of Medical Device can result in death or serious injury
Medical Devices & Systems: Potential Effects of Security Compromise

<table>
<thead>
<tr>
<th>Security Element</th>
<th>Description</th>
<th>Typical Priority (NIST)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability</strong></td>
<td>Systems &amp; data should be available/accessible and usable on demand by authorized persons or processes or conditions</td>
<td>First</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Systems &amp; data should not be subject to alteration or destruction by unauthorized persons or processes or conditions</td>
<td>Second</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Systems &amp; data should not be available or disclosed to unauthorized persons or processes</td>
<td>Third</td>
</tr>
</tbody>
</table>

Compromised care, injury, or death (as well as compromised operations, finances)

Critical Data (not just PHI)

Privacy compromised, identify theft, financial loss

PHI
### Medical Devices & Systems: Examples of Security-Related Harm

**Relevant Security Element** | **Examples of Harm**
--- | ---
**Availability ...**<br> *Data should be accessible and usable on demand by authorized persons or processes* | device & data unavailable due to DoS attack or jamming wireless network<br> device & data unavailable due to device theft, device damage, device failure or utility outage<br> device & data unavailable due to bad software patch or unsuccessful software upgrade
**Medical Devices & Systems: Examples of Security-Related Harm**

<table>
<thead>
<tr>
<th>Relevant Security Element</th>
<th>Examples of Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrity</strong> ...</td>
<td>“bad” data caused by electromagnetic inference (EMI) ... e.g., from cell phones, transceivers, wireless access points or other EMI –generating devices</td>
</tr>
<tr>
<td><em>Data should not be subject to alteration or destruction by unauthorized persons or processes</em> ...</td>
<td>“bad” data caused by miscalibration yields incorrect diagnostic data .. or delivers incorrect type or amount of therapy</td>
</tr>
<tr>
<td></td>
<td>“bad” data from an invalid source (e.g., changed dose or alarm settings, diagnostic data, therapeutic settings modified by unauthorized persons with physical or remote access)</td>
</tr>
</tbody>
</table>
# Medical Devices & Systems: Examples of Security-Related Harm

<table>
<thead>
<tr>
<th>Relevant Security Element</th>
<th>Examples of Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong> ...</td>
<td>PHI can be electronically accessed or downloaded (e.g., locally via USB or remotely via network “eavesdropping”)</td>
</tr>
<tr>
<td>Data (PHI) should not be available or disclosed to unauthorized persons or processes ...</td>
<td>PHI can be accessed by agents physically or remotely servicing devices</td>
</tr>
<tr>
<td></td>
<td>PHI can be recovered by unauthorized personnel from transferred, discarded, lost or stolen devices</td>
</tr>
</tbody>
</table>
Medical Devices & Systems: Who has Responsibility?

IT knows data security

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

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:

<table>
<thead>
<tr>
<th>Equipment Type</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physiologic monitors</td>
<td>hundreds</td>
</tr>
<tr>
<td>Defibrillators</td>
<td>scores</td>
</tr>
<tr>
<td>Infusion pumps</td>
<td>thousands</td>
</tr>
<tr>
<td>Anesthesia units</td>
<td>scores</td>
</tr>
<tr>
<td>Ventilators</td>
<td>scores</td>
</tr>
<tr>
<td>Extracorporeal Assist</td>
<td>up to dozen</td>
</tr>
<tr>
<td>Vital sign monitors</td>
<td>hundreds</td>
</tr>
<tr>
<td>CT &amp; MRI scanners</td>
<td>up to score</td>
</tr>
<tr>
<td>Fetal monitors</td>
<td>scores</td>
</tr>
<tr>
<td>Laboratory analyzers</td>
<td>scores</td>
</tr>
<tr>
<td>Diagnostic ultrasound</td>
<td>scores</td>
</tr>
<tr>
<td>Patient beds</td>
<td>hundreds</td>
</tr>
<tr>
<td>Electrocardiographs</td>
<td>scores</td>
</tr>
<tr>
<td>Injectors, contrast media</td>
<td>scores</td>
</tr>
</tbody>
</table>

~ 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

- Input / Acquisition
  - Keyboard or keypad
  - Scanning
    - bar code
    - magnetic
    - OCR
    - RFID
  - Imaging
    - photo
    - medical image
  - Biometrics
  - Voice Recognition

- Maintain / Store
  - Component, Device, or System
  - Hard Disk
  - including SSD
  - Memory (e.g., RAM)
  - Disk
  - Tape
  - USB Storage & Digital Memory Card
  - Optical disk, CD-ROM, DVD

- Transmit / Receive
  - Disk
  - Tape
  - USB Storage & Digital Memory Card
  - Optical disk, CD-ROM, DVD
  - Wired Networks
    - Private or Public, Leased or Dial-up lines, Internet
  - Wireless Networks
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

![Medical Devices Product Life Cycle Diagram](image)

- **7-8 year Product Life Cycle**
- **Software update patches & antivirus**
- **Management agents**

©HIMSS 2016
Actions Required by Healthcare Delivery Organizations
Medical Devices & Systems:  
Determine the scope of the medical device security issue

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 is data being exchanged? ... 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 (MDS\textsuperscript{2})

- MDS\textsuperscript{2} 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 MDS\textsuperscript{2} on each of their medical equipment models
- Information on the MDS\textsuperscript{2} 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 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*
**Summary**

- 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.
Questions

Thank You

Stephen.Grimes@SHCTA.com