
Stephen L. Grimes, FACCE FHIMSS FAIMBE
Chief Technology Officer
ABM Healthcare Support Services

Wednesday, Nov 5, 2014
10:30 am – 12:00 noon
At the end of the session, participants will be able to:

- describe the patient safety-related benefits of this emerging standard
- define the roles and responsibilities as required by the standard and
- suggest how those new roles and responsibilities can be integrated with current CE staffing models
Overview

Presentation Outline
– Background & Rationale

- Issues that lead to 80001
- History of 80001 development
- What is 80001
- Enforcement of 80001
- Focus of 80001
  - Roles & Responsibilities defined in 80001
  - Major Activities defined in 80001
- Plans for future 80001-2 guidelines
- Next steps for healthcare providers
- Useful References, Standards & Guidelines
Recognition of a growing issue

- In the past 10-20 years, the number of integrated & networked medical device systems has rapidly proliferated.
- And our dependence on the clinical information maintained and transmitted by systems for effective & timely diagnosis and treatment is likewise increasing.
- This dependence on integrated systems can have major implications on our ability to deliver patient care and on our business operations if those systems should fail.
- The development of adequate practice guidelines, standards, supporting resources and infrastructure has not been keeping pace with the evolving integrated & networked systems.
- As a consequence of rapid system proliferation and the lack of appropriate support guidelines & infrastructure, there have been a growing number of reported system failures with serious consequences since the year 2000.
Recognizing this problem, in December 2005 Brian Fitzgerald (FDA) convened a meeting with expert representatives from medical device manufacturers, healthcare providers (clinical engineering) and other relevant parties to discuss the problem (i.e., how to deal with increasing number of systems with new vulnerabilities).

The meeting concluded that

- while manufacturers had guidelines for effectively risks associated with the development and manufacture of medical devices/systems (e.g., ISO/IEC 14971),
- there were no comparable, adequate guidelines that healthcare providers could employ to insure the medical devices/systems they deploy.
**The Birth of 80001**

Outcome of the 2005 FDA meeting was the establishment of new workgroup under the auspices of the ISO/IEC. This workgroup was to

- include representatives from world community of medical device manufacturers, healthcare providers, standards development organizations
- develop *guidelines for healthcare providers* on how to best manage risks associated with the rapidly growing number of critical systems they deploy
US and international experts (including medical device manufacturers, government & regulatory authorities, clinical and information technology specialists from the healthcare provider community) met regularly over the next 4 years to develop a practical, *high level guideline* that could be *adopted by healthcare delivery organizations* and that would be *scalable to any size organization*

In the summer of 2010, the final draft of ISO/IEC 80001-1 was formally approved by ISO/IEC and the final document was released in October 2010.
What is ANSI / AAMI / IEC 80001-1?

- **International Standard**
  (i.e., means that it has been developed with widespread, international participation and widely adopted by international standards bodies)

- Primarily a standard for Health Delivery Organizations (HDO) ...
  i.e., healthcare providers

- Specifically designed to assist HDOs in identifying and managing “new” risks associated the increased deployment of medical devices onto IT networks.
Enforcement of ANSI / AAMI / IEC 80001-1?

Standards like 80001 are not de-facto regulations but ...

- Standards may be given the “force of law” if adopted by federal, state, local government agencies
- Standards may be be adopted and referenced by accrediting agencies (e.g., Joint Commission, DNV) ... and therefore relevant to accreditation ... or certification (i.e., ISO 9001)
- Standards may be “best practices” ... when endorsed and by relevant professional organizations (e.g., ACCE, HIMSS, AAMI) or referenced by authorities like the FDA
Focus of ANSI / AAMI / IEC 80001-1

- 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
Roles & Responsibilities defined in 80001

- Responsible Organizations
- Responsible Organization’s Top Management
- Medical IT network risk manager
- Medical device manufacturers
Roles & Responsibilities defined in 80001

**Responsible Organization**

- Healthcare delivery organization (e.g., provider)
- 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 & Responsibilities defined in 80001

**Responsible Organization’s 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
Roles & Responsibilities defined in 80001

Medical IT network risk manager
(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 mfg
  - IT suppliers of equipment, software, services
  - Clinical users
  - Technical departments responsible for medical device support
Roles & Responsibilities defined in 80001

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
Major Activities defined in 80001

- 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
Establish risk management policy that

- 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
Establish the 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
Major Activities defined in 80001
– 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
Major Activities defined in 80001 – Document Medical IT networks

Document Medical IT-networks ... for example

- physical & logical network configurations
- applied standards & conformance statements
- client / server structure
- network security (i.e., reliability, integrity, confidentiality) provisions
- any planned changes, upgrades, enhancements
Major Activities defined in 80001 – Creating 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/disconnecting device from network and for performing risk analysis)
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

- criteria for risk acceptability based on established policy
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
**Major Activities defined in 80001**

– *Conduct Risk Management*

### Risk management elements include

- Risk analysis
- Risk evaluation
- Risk control
  - ✓ option analysis
  - ✓ identify measures
  - ✓ implement measures
  - ✓ verify measures
  - ✓ identify any new risks
- Residual risk evaluation & reporting
Plans for future Guidance (80001-2)  
Technical reports scheduled and/or contemplated

Guidance for:

- Implementation Guidance for Healthcare Delivery Organizations  
  ANSI/AAMI/IEC TIR80001-2-4:2012

- Step-by-step risk management (with examples)  
  ANSI/AAMI/IEC TIR80001-2-1:2012

- Security  

- Healthcare Delivery Organizations

- Wireless networks  

- Development of responsibility agreements
Where Medical IT Network Risk Manager Role fits in the Clinical Engineering Professional Paradigm

Clinical Systems Engineer

Clinical Systems Support Specialist

RF Spectrum Manager

Clinical Engineering Domain
- analysis & application of scientific theory to create & improve technology & related processes

RF Spectrum Manager

Procedural Engineering Domain
- practical application & support of engineered devices, systems & related processes

Biomedical Equipment Technician

Vendor & Contracts Manager

Biomedical Equipment Specialist
- Imaging, Laboratory, Cardiology, Neurology, OR/Gyn, GI, etc.

Technical Service Manager

Technology Management Domain
- Planning, organizing, staffing & leading to support organization’s goals

Healthcare Technology Manager

sgrimes '09
Preliminary Role Definition of “Clinical Systems Engineer”

The **CSE** coordinates an enterprise-wide program to insure the **effective deployment, integration, and support of interconnected medical 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.
Preliminary Role Definition of “Clinical Systems Support Specialist”

Working with the CSE, the CSSS specializes in and manages the operation & support of integrated systems in areas such as imaging, OR, cardiology, obstetrics, neurology, etc.

Description of new (service or department specific) role ...

- Provides operational and service training to clinicians and support personnel on networked medical systems in assigned area(s)
- Provides consultation to clinical staff on technical capabilities and limitations of available technologies
- Monitors medical device hazard/recall reports for their assigned area(s) and insures appropriate follow-up (i.e., communication, corrective action, follow-up)
- Monitors regulatory developments affecting devices/systems in assigned area(s) and identifies/coordinates appropriate compliance measures
- Maintains technical library and database information critical to the support of devices/systems in assigned area(s)
- Participates in the development and maintenance of a capital equipment plan (for existing and new operations for assigned area(s). Examples of plan elements should include:
Preliminary Role Definition of “Radio Frequency Spectrum Manager"

The RF Spectrum Manager is responsible enterprise-wide management and monitoring of the radio-frequency environment.

*Description of new (enterprise wide) role...*

- Maintain an **inventory of all R/F systems operating in or affecting the clinical environment**
- **Manage deployment and operation of R/F systems** so as to **insure regulatory compliance** and to **minimize adverse interactions** between devices/systems
  - Advise in selection compatible R/F systems
  - Plan for R/F allocation, deployment, integration and upgrades as necessary
  - Obtain requisite **licenses/permits** and insure all are kept current
  - Investigate reports of possible adverse R/F affects on devices/systems and identify appropriate corrective action as necessary
- **Educate users and monitor user practices** associated with R/F systems in order to assure their safe and effective operation
NEXT STEPS

- 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.
Other Useful References, Standards & Guidelines

- ISO/IEC 60601-1: 2005 *Medical Electrical Equipment* requires manufactures to include some information in accompanying documents if medical equipment is to be connected to an IT network
- ISO/IEC 14971:2007 *Application of risk management to medical devices*
- ISO/IEC 20000-1:2005 *IT Service Management System*
- *Information Technology Infrastructure Library* (ITIL v3)
- HIMSS/NEMA HN 1-2008 *Manufacturer’s Disclosure Statement for Medical Device Security* (MDS²)
- ACCE ECRI *Security Guide for Biomedical Technology* [www.ECRI.org](http://www.ECRI.org)
- The Joint Commission *Sentinel Event Alert #42: Safely implementing health information and converging technologies*, December 11, 2008
Useful References, Standards & Guidelines

National Institute of Standards and Technology (NIST)
http://csrc.nist.gov/publications/nistpubs/

- SP 800-61: Computer Security Incident Handling Guide
- DRAFT SP 800-53: Recommended Security Controls for Federal Information Systems
- SP 800-50: Building an Information Technology Security Awareness and Training Program
- SP 800-42: Guideline on Network Security Testing
- SP 800-35: Guide to Information Technology Security Services
- SP 800-34: Contingency Planning Guide for Information Technology Systems
- SP 800-30: Risk Management Guide for Information Technology Systems
- SP 800-26: Security Self-Assessment Guide for Information Technology Systems
Thank you!

Stephen.Grimes@ABM.com

ABM Healthcare Support Services