Application of Risk Management for IT Networks
Incorporating Medical Devices
Part 1: Roles, Responsibilities, and Activities

- AND -

Effect of new FDA regulations covering
Medical Device Data Systems (MDDS)
on Healthcare Providers

Moderator:
Elliot B Sloane, PhD CCE FHIMSS
Executive Director, Center for Health Information Research

Speaker:
Stephen L. Grimes, FACCE FHIMSS FAIMBE
Chief Technology Officer
ABM Health

CE-IT Community Town Hall Meeting
Feb. 8, 2012
CHAPTER ONE

Application of Risk Management for IT Networks
Incorporating Medical Devices
Part 1: Roles, Responsibilities, and Activities

Moderator:
Elliot B Sloane, PhD CCE FHIMSS
Executive Director, Center for Health Information Research

Speaker:
Stephen L. Grimes, FACCE FHIMSS FAIMBE
Chief Technology Officer
ABM Health

CE-IT Community Town Hall Meeting
Feb. 8, 2012

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 a meeting was convened at FDA headquarters 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 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, licensing or certification agencies ... and therefore relevant to certification (i.e., ISO 9001)
- Standards may be “best practices” ... particularly when endorsed and by relevant professional organizations
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)
- HDO is 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
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
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
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
Risk Management for Medical Devices/Systems

Risk Management Process

Iterative Review & Re-assessment Process
The “Clinical Systems Engineer” as the Medical IT Network Risk Manager

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

- maintains enterprise inventory of “systems”
- coordinates security management process (risk & vulnerability analysis)
- coordinates a process to prioritize, develop and implement plan to manage/mitigate identified risks
- maintains the medical device integrity for interconnected/integrated systems
- works to insure effective selection, deployment, integration, and support of new medical systems into legacy systems
- manages enterprise software upgrades, security patches
- does Root Cause Analysis (RCA) & Failure Mode Effects Analysis (FMEA)
- monitors and adopts industry “Best Practices”
Plans for future Guidance (80001-2)
Technical reports scheduled and/or contemplated

Guidance for:

- Step-by-step risk management (with examples)
- Security
- Healthcare Delivery Organizations
- Wireless networks
- Development of responsibility agreements
- Causes of hazards associated with medical IT networks
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 you 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
- 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
CHAPTER TWO

Effect of new FDA regulations covering Medical Device Data Systems (MDDS) on Healthcare Providers

Moderator:

Elliot B Sloane, PhD CCE FHIMSS
Executive Director, Center for Health Information Research

Speaker:

Stephen L. Grimes, FACCE FHIMSS FAIMBE
Chief Technology Officer
ABM Health

CE-IT Community Town Hall Meeting
Feb. 8, 2012
What are Medical Device Data Systems (MDDS)?

Illustrations of MDDS

Background of FDA’s Role in Medical Device Regulation

Overview of FDA’s Medical Device Regulations

FDA’s Concerns about MDDS Risks

FDA’s Requirements for MDDS Manufacturers

Timetable for compliance with FDA’s new MDDS regulations

Summary

Next steps

Federal Register, February 15, 2011
The Objective of this Presentation

- The FDA published its Final Rule on Medical Device Data Systems (MDDS) on February 15, 2011. This Rule becomes effective on April 18, 2011.
- This Rule has been anticipated for 3 years and is meant to address some real patient safety issues associated with the new “connected” medical technologies increasing deployed by healthcare organizations today.
- We believe this rule has major implications for healthcare providers ... many of whom will now find themselves de facto medical device manufacturers and therefore subject to certain FDA regulations for the first time.
- We believe that today most healthcare providers remain unaware of the MDDS rule and its implications for their organizations.
- The purpose of our presentation is to acquaint healthcare providers at a high level with
  - review the basic provisions of the MDDS rule
  - potential implications of the rule for their organizations and how begin assess the reality of those implications
  - reasonable first steps that can and should be taken now given the short timeframe
**What are Medical Device Data Systems (MDDS)?**

- **MDDS** is a category of medical device defined by FDA and subject to new FDA regulations that were finalized and published in Federal Register on Feb 15, 2011
  
  designated:  *Final MDDS Rule ( 21 CFR 880.6310)*

- FDA has defined MDDS as a device (or system that is connected to a medical device and) is

  1) ... intended to provide **one or more of the following uses, without itself controlling or altering the functions or parameters of any connected medical devices:**

  i. The electronic **transfer** of medical device data;

  ii. The electronic **storage** of medical device data;

  iii. The electronic **conversion** of medical device data from one format to another format in accordance with a preset specification; or

  iv. The electronic **display** of medical device data;
What are Medical Device Data Systems (MDDS)?

(continued)

2) MDDS may include software, electronic or electrical hardware such as a physical communications medium (including wireless hardware), modems, interfaces and a communications protocol. This ... does not include devices intended to be used in connection with active patient monitoring

(i.e., monitoring to facilitate immediate clinical actions ... because speed of data transmission or conversion are critical)

Medical devices that don’t meet definition of MDDS may be subject to more stringent regulations (e.g., systems designed to send alarms from physiological monitoring to wireless personal devices to facilitate IMMEDIATE clinical actions)
Connecting a device/system to a Medical Device for data transfer

All this is a *Medical Device* if put together or modified with intent (i.e., “labeled”) to connect to a medical device for data transfer.

It may be a MDDS, an accessory or another category of medical device.

ALL medical devices used/sold in US are regulated by FDA:

- Nature/extent of regulation depends on category & class of medical device.
- Identity of the “manufacturer” is determined by who put together components with intent of connecting to a medical device.
Complex, connected and integrated medical devices represent an rapidly growing segment of the healthcare technology environment

By virtue of their interconnections, integration and complexity, these medical devices often introduce unique vulnerabilities that can result in major compromises to patient safety when these devices fail

To address the challenges of one broad medical device category, the FDA just finalized a regulation pertaining to Medical Device Data Systems (MDDS).

This new regulation has been issued to address significant patient safety issues by insuring those who put together these systems (including many healthcare providers) adopt FDA’s relevant safeguards
Illustrations of Medical Device Data Systems (MDDS) Types
Electronic Transfer of Medical Device Data via MDDS

MDDS
If put together or modified with intent ("labeled") to use with (i.e., connected to) medical device

MDDS adds NO FUNCTION to a medical device (e.g., no alarms, no interpretation)

MDDS itself provides NO CONTROL over a medical device
BUT may transfer control data from one medical device to another
Electronic Storage of Medical Device Data via MDDS

MDDS

If put together or modified with intent (“labeled”) to use with (i.e., connected to) medical device

MDDS adds NO FUNCTION to a medical device (e.g., no alarms, no interpretation)

MDDS itself provides NO CONTROL over a medical device
BUT may transfer control data from one medical device to another
Electronic Conversion of Medical Device Data via MDDS

MDDS adds NO FUNCTION to a medical device (e.g., no alarms, no interpretation)

MDDS itself provides NO CONTROL over a medical device
BUT may transfer control data from one medical device to another
**Electronic Display of Medical Device Data via MDDS**

**MDDS**
If put together or modified with intent ("labeled") to use with (i.e., connected to) medical device

*MDDS adds NO FUNCTION to a medical device (e.g., no alarms, no interpretation)*

*MDDS itself provides NO CONTROL over a medical device*

*BUT may transfer control data from one medical device to another*
Individual Components are not Medical Devices

If individual components not specifically intended (i.e., not “labeled” or not advertised) for connection to medical devices ...

Data converted according to a fixed, unchangeable algorithm

the manufacturers of these types of individual components are not subject to FDA regulations
Systems of Connected Components are Medical Devices

If data from a connected medical device is transferred and/or stored and/or displayed and/or converted

- Wireless Access Point
- Router
- Display
- Optical disk, CD-ROM, DVD

a MDDS if it
• does not add functionality to medical device or
• does not itself control another medical device
• is put together with intention (i.e., “labeled” for purpose) of connecting to a medical device

Data converted according to a fixed, unchangeable algorithm

The organization that puts together a new MDDS or modifies intended use of an existing MDDS is a medical device MANUFACTURER ... and therefore subject to FDA regulations
MDDS can pass control data from one Medical Device to another

If data is transferred to a medical device

MDDS

If put together or modified with intent (“labeled”) to use with (i.e., connected to) to medical device

but the MDDS only transmits control data from the controller and does itself control the medical device

The organization that puts together a new MDDS or modifies intended use of an existing MDDS is a medical device MANUFACTURER ... and therefore subject to FDA regulations
System is a Medical Device (but not a MDDS) if part of “Active” Monitoring

Data from a connected medical device is used for active monitoring

Medical Device subject to FDA Regulation (but not a MDDS)

- Display and/or Sound (e.g., alarms, waveforms)
- Smart Phone (e.g., alarm notifications)
- Data converted according to a fixed, unchangeable algorithm

active monitoring (i.e., monitoring relied upon for immediate clinical action or continuous monitoring)
FDA Role in Medical Device Regulations

FDA given authority to regulate US sale and distribution of medical devices in 1976 Medical Device Amendments to the 1938 Food, Drug and Cosmetic Act

FDA definition of what constitutes a medical device:
SEC. 201. [321] For the purposes of this Act –

(h) The term “device” ... means an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or accessory, which is

1) Recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them,

2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease, in man or other animals, or

3) intended to affect the structure of any function of the body of man or other animals, and which does not achieve any of its principal intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its principal intended purposes.
FDA’s Mission, Approach and Focus

- **FDA’s Mission** is to “promote health and reduce risk of harm” by “assuring safety, efficacy and security of ... medical devices”

- **FDA’s Approach** is *risk based* to in assure medical devices are “reasonably” safe & effective

- **FDA’s Focus** is in two main areas
  - *Premarket*
    Oversight before a new product enters market or exposes patients
  - *Postmarket*
    Monitor safety and act as a feedback mechanism to industry, users and patients
FDA’s Premarket Oversight Depends on Risk Based Device Classification Scheme

**FDA has categorized MDDS as Class I**

- **Class I**
  - ✔ No Premarket review except in certain circumstances

- **Class II**
  - ✔ Premarket review required unless exempt
  - ✔ Demonstrate Substantial Equivalence (SE) to legally marketed devices in the US

- **Class III**
  - ✔ Premarket approval required

Increasing risk = increasing oversight & regulation
FDA’s Risk Based Approach to Oversight of Medical Device Manufacturing & Safe Usage

**MDDS**
Classification determines extent of regulatory control (i.e., Risk Based)

**Increasing Risk**

- **Class I**
  - General Controls

- **Class II**
  - General Controls
  - Special controls

- **Class III**
  - General Controls
  - Premarket approval (PMA)

**General Controls**
- Electronic establishment registration
- Electronic device listing
- Adulteration/misbranding
- Premarket notification [510(k)] *unless exempt*
- Quality systems
- Labeling
- Medical device reporting (MDR)

**Special Controls**
- Guidelines (e.g., Glove Manual)
- Mandatory Performance Standard
- Recommendations or Other Actions
- Special Labeling (e.g., 3825970, cranial orthosis)
### FDA’s Oversight “Tools”

<table>
<thead>
<tr>
<th>Registration &amp; Listing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Register:</strong> who is the manufacturer?</td>
</tr>
<tr>
<td><strong>List:</strong> what is the device?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Premarket Notification (510k) or Premarket Approval (PMA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidential independent review prior to commercial distribution</strong></td>
</tr>
<tr>
<td><strong>Provide cross product lessons learned</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Investigational Device Exemption (IDE) for clinical studies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allowing new technology creation</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quality System (QS) regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Non-prescriptive principles for good engineering &amp; manufacturing</strong></td>
</tr>
<tr>
<td><strong>Scalable for technology</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labeling requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Establishes clear user expectations</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Medical Device Reporting (MDR)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Understand device issues and impact on patients</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Correct defective product consistently</strong></td>
</tr>
<tr>
<td><strong>Periodic monitoring to assure device quality is sustained</strong></td>
</tr>
</tbody>
</table>

**MDDS**
FDA’s general concerns about medical device trends

Today, medical devices (hardware & software) are

- more complex
- contain additional functionality intended to reduce burden on clinicians or caretakers
- decentralized & mobile
- accessible & often in hands of more lay users
FDA’s concern with Medical Device Data Systems

- FDA wants to assure that clinical data generated by medical devices
  - can be used reliably after being transferred, stored, and/or displayed by a MDDS
  - maintains integrity after being transferred, stored, and/or displayed by a MDDS
  - is not changed during process of transferring, storing or displaying (note difference between changing and converting)

- FDA wants to set a solid foundation for all future advancement in health information technologies
FDA believes MDDS risks are
  ✓ Inadequate software quality
  ✓ Incorrect functioning of device

FDA sees failure that can result in incorrect treatment or diagnosis of patient
  ✓ Inaccurate or incomplete data transfer
  ✓ Inaccurate or incomplete data storage
  ✓ Inaccurate or incomplete data conversion (according to preset specifications)
  ✓ Inaccurate or incomplete display of medical device data

FDA believes the application of an effective quality system can significantly reduce the risks of inadequate design and unreliable performance associated with a MDDS
Manufacturers (including affected healthcare providers)

- must register with FDA as a manufacturer of medical devices
- must list their product(s) with the FDA
- are exempt from pre-market submission if
  - healthcare professionals or lay users
  - they include systems with irreversible data compression
- must implement adverse event reporting according to FDA’s Medical Device Report (MDR) requirements
- must establish and document a good manufacturing practice (GMP) according to FDA’s Quality System (QS) requirements. These include methods used in, and the facilities and controls used for,
  - design,
  - manufacture,
  - packaging,
  - labeling,
  - storage,
  - installation, and
  - servicing of devices
FDA Timetable for Compliance with MDDS Rule

- **Feb 15, 2011**
  FDA published it’s Final Rule on Medical Device Data Systems (MDDS) in the Federal Register

- **April 18, 2011**
  The MDDS regulation becomes effective

- **May 18, 2011**
  Manufacturers are required to register their organizations with FDA & list their MDDS

- **Apr 18, 2012**
  Manufacturers are to have a compliant quality system (QS) & and medical device reporting (MDR) system
A manufacturer is anyone who
  ✓ puts together a new MDDS or
  ✓ modifies an existing MDDS (i.e., a “modification” from original manufacturer’s intended use)

A MDDS is
  ✓ hardware or software or some combination thereof
  ✓ connected to (and acquires its data from) a medical device
  ✓ only communicates (i.e., transfers, stores, displays and/or converts) medical device data.

Medical device data is data available directly from a medical device or obtained originally from a medical device.
  ✓ manually entered into a medical device is not considered medical device data
  ✓ electronically transmitted data (even if originally entered manually) is medical device data

A MDDS does NOT
  ✓ modify, interpret, or add value to medical device data
  ✓ control the function or parameters of another medical device
  ✓ provide or is not used in connection with active monitoring
FDA estimates that compliance costs

- for Registration & Listing requirements are
  - $2,179 in 2011 ($2,364 in 2012) “user fee” for a manufacturer (including affected healthcare providers) to register and list their devices with FDA
  - 2 hours labor per year for organizations unfamiliar with the registration/listing process

- for Quality System (QS) and Medical Device Reporting (MDR)
  - one time $20,000 cost to initially establish QS & MDR systems
  - annual cost of $143,000 (salary & benefits) for full time employee to manage the QS & MDR systems
FDA is in the process of establishing an appropriate enforcement and compliance policy.

Hospital administrators and device makers should be aware that FDA
- does not intend to start enforcing quality system requirements before the one-year compliance schedule mentioned in the Federal Register announcement
- does expect manufacturers (including affected healthcare delivery organizations) to register and list their MDDS. Health care facilities should evaluate their current design/development practices for the portions of the systems modified or added by them. This evaluation should reference the principles outlined in CGMP/QSR to appropriately address any identified gaps

FDA is working with the Association for the Advancement of Medical Instrumentation (AAMI), hospitals, industry and other stakeholders to gather input and help us implement the MDDS regulation in a targeted and practical way.
**What should Healthcare Providers do now?**

- Review the final MDDS rule in detail with relevant stakeholders (e.g., administration, clinical engineering, IT, risk management, legal)
- Identify and inventory all MDDS in your organization (e.g., what is connected to your medical devices ... is the connected hardware and/or software an MDDS or another category of medical device?)
- Determine whether the FDA will consider you a manufacturer
  - Have you put together any of your MDDS? **or**
  - Have you modified any of your existing MDDS from original manufacturer’s **intended use**?
- If you meet the FDA’s definition of a MDDS manufacturer now
  - Register with FDA as a manufacturer by May 18, 2011
  - List any MDDS you “manufactured” with the FDA by May 18, 2011
  - Begin to establish/document your GMP & according to FDA’s QS requirements ... must have in place by February 18, 2012
- Assess the likelihood of your organization “manufacturing” MDDS in the future ... many organizations should take steps to insure they are prepared for compliance
References & Resources

- **Medical Device Data Systems: Final Rule** (Federal Register, February 15, 2011)

- **Medical Device Regulation: An Overview from the Food and Drug Administration** (HIMSS Webinar, April 13, 2011)

- **The Impact of FDA’s Ruling on Medical Device Data Systems**
  (2011 AAMI Conference and Expo, San Antonio, TX, June 27, 2011)
  [http://www.aami.org/meetings/aami2011/sessions.mon.html#monot3](http://www.aami.org/meetings/aami2011/sessions.mon.html#monot3)

- **ANSI/AAMI/IEC 80001-1: 2010 Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsibilities and activities**
  Association for the Advancement of Medical Instrumentation (AAMI) approved/published October 2010.

- **Sentinel Event Alert #42: Safely Implementing Health Information and Converging Technologies** (The Joint Commission, December 11, 2008)
References & Resources (continued)

- **2011 Top 10 Health Technology Hazards--Is Your Hospital at Risk?**
  ECRI Institute Webinar, February 23, 2011
  [https://www.ecri.org/Conferences/Pages/2011_Top_10_Hazards.aspx](https://www.ecri.org/Conferences/Pages/2011_Top_10_Hazards.aspx) (accessed 4/8/11)

- **Integrating the Healthcare Enterprise Patient Care Device Domain (IHE®-PCD)**

- **IHE®-PCD Alarm Communication Management Profile**

- **HIMSS Medical Devices and Patient Safety Task Force**
Questions?

Thank You!

Steve Grimes

Stephen.Grimes@LincHealth.com

SLGrimes@ACCEnet.org