The New ISO/IEC 80001 Standard for Risk Management

Rick Hampton
Wireless Communications Manager
Partners HealthCare System

Wednesday, September 29, 2010
What is IEC 80001?

- It is an international standard
- It is a process standard; it tells you what to do, not how to do (how comes later)
- It is a voluntary standard – unless formally adopted by regulatory authorities
Future Documents

- Technical Reports (guidance documents) to be published soon:
  - Guidance for Healthcare Delivery Organizations
    - An implementation guide for HDOs of all sizes
  - Step by Step Risk Management
    - Still not a bullet-list of steps to accomplish, but rather a simple explanation of concepts from ISO 14971 and how they might be adopted by Responsible Organizations
  - Security
  - Use of Wireless Technologies

- With more to come
Why do we need IEC 80001?

- Currently, many healthcare medical systems operate on isolated networks which (in the US) are viewed as a component of a regulated medical device. Medical device manufacturers are held responsible for performing risk assessment and mitigation activities under current federal requirements and thus ensuring these systems are safe and effective for their intended use.

- Emerging technologies hold the promise to allow medical device manufactures and healthcare facilities to begin combining these systems on the healthcare information systems (HIS) network.

- When healthcare facilities use their HIS networks for medical device connectivity instead of the manufacturer-provided networks, the healthcare facility now become responsible for ensuring the proper operation of those medical devices.
A “Medical Device” is:

- Any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article*:
  - intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:
    - diagnosis, prevention, monitoring, treatment or alleviation of disease, or compensation for an injury,
    - support of the anatomy or of a physiological process,
    - supporting or sustaining life,
    - control of conception,
    - disinfection of medical devices
  - And is not a pharmacological, immunological or metabolic agent.

- Note: This definition is nearly identical to those used by FDA and other regulatory agencies around the world.

- *In the US, FDA adds, “including a component part, or accessory”
Origins of 80001

- Core ideas drawn from:
  - ISO 14971 – “Application of risk management to medical devices”
    ◊ Applies ONLY to medical device manufacturers
  - ISO 20000 – “IT Service Management Standards”
  - ITIL – IT Infrastructure Library
Risk Management

“Risk management is a more realistic term than safety. It implies that hazards are ever-present, that they must be identified, analyzed, evaluated and controlled or rationally accepted.”

— Jerome Ledere, director of the Flight Safety Foundation for 20 years and NASA's first director of Manned Flight Safety
The Key Properties

- **80001 defines three Key Properties to be managed. They are, in this order of priority:**
  - Safety (freedom from unacceptable 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)

- **80001 does not specify acceptable risk levels.**
80001 Structure

- Section 1 Scope
- Section 2 Terms and definitions
- Section 3 Roles and responsibilities
- Section 4 Life Cycle Risk Management In Medical It-Networks
- Section 5 Document Control
- Annex A (informative) Rationale
- Annex B (Informative) Overview Of Risk Management Relationships
- Annex C (Informative) Guidance On Field Of Application
- Bibliography
80001 SCOPE

- Defines roles to ensure the Key Properties
  - Does not specify acceptable risk levels

- Applies after a medical device has been acquired by a Responsible Organization for incorporation into an IT-network
  - Does not cover pre-market/pre-purchase risk management

- Applies throughout the life cycle of IT-network incorporating medical devices.
Applies where there is no single medical device manufacturer assuming responsibility for addressing the Key Properties of the IT-network incorporating a medical device
- Does not apply to complete systems that include a network specified by a single manufacturer
- Does apply to complete systems that include a network specified by a single manufacturer if that system is modified, added to, or connected to another network
80001 SCOPE – Continued

- Applies to Responsible Organizations, Medical Device Manufacturers, and Providers of Other Information Technology
  - Does not apply to personal use applications where the Patient, Operator, and Responsible Organization are one and the same person

- In cases where a medical device is used at home under the supervision or instruction of the provider, that provider is deemed to be the Responsible Organization.
  - Does not apply for personal use where the patient acquires and uses a medical device without the supervision or instruction of a provider.
Section 3 – Roles and Responsibilities

- The Responsible Organization
  - Entity accountable for the use and maintenance of a Medical IT-Network
    - A few examples of Responsible Organizations include a hospital, a private clinician, or a telehealth organization.
  - Top Management
    - Person or group of people who direct(s) and control(s) the Responsible Organization accountable for a Medical IT-Network at the highest level
    - Significant responsibilities to establish policies, specify acceptable risk levels, and provision required resources
  - The Medical IT-Network Risk Manager
    - The person accountable to the Responsible Organization for Risk Management of a Medical IT-Network
    - Significant responsibility for overall management, implementation, and monitoring of risk management process, reporting to Top Management, and go-live authorization

- Medical Device Manufacturer(s)
  - Shall make available information describing the intended use and instructions necessary for the safe and effective use of the Medical Device.
Section 3 – Roles and Responsibilities – Continued

- Providers of Other Information Technology
  - Providers of other (not MEDICAL DEVICES) information technology may provide:
    - infrastructure components;
    - infrastructure services;
    - client devices not being MEDICAL DEVICES;
    - servers;
    - application software; or
    - middleware.
  - Each provider of other information technology (equipment and/or software) shall make available documentary information as follows:
    - technical descriptions and technical manuals;
    - required IT-NETWORK characteristics;
    - recommended product configurations;
    - known incompatibilities and restrictions;
    - operating requirements;
    - product corrective actions and recalls; and
    - cyber security notices (warnings of known security vulnerabilities).
Role Relationships

Medical Device Manufacturer

Providers of Other Information Technology

Responsible Organization
Top Management
Medical IT-Network Risk Manager
Importance of Top Management

“No matter how interested individual employees might be, or what assistance a manufacturer offers, or how insistent a certificating authority might be — none of these factors will have a significant effect on safety without support from top management.”

— John O'Brian, ALPA's Engineering and Air Safety Department.
Section 4 – Life Cycle Risk Management – Continued

- **Responsible Organization Risk Management**
  - Policy For Risk Management For Incorporating Medical Devices
    - *Created by Top Management to establish balanced risk criteria for each of the Key Properties, describe processes for Event, Change-Release, Configuration, and Monitoring Management in terms that can be interpreted throughout all Risk management activities.*
  - Risk Management Process
    - *Implemented by Medical IT-Network Risk Manager*
Section 4 – Life Cycle Risk Management – Continued

- Medical IT-Network Risk Management Planning And Documentation
  - Risk-Relevant Asset Description
    - Information on each IT and Medical Device component of the IT infrastructure, including operational characteristics, configurations, identifiable patient data, security description
  - Medical IT-Network Documentation
    - Physical & logical configurations, conformance statements, security, reliability, and data integrity information, etc.
  - Responsibility Agreement
    - Defines (e.g. by contract) roles & responsibilities of all relevant stakeholders, activities and equipment covered, and information required from each party
  - Risk Management Plan For The Medical IT-Network
    - Identifies stakeholders, defines uses and benefits, reasons for creation, monitoring requirements and criteria for acceptable risk
Section 4 – Life Cycle Risk Management – Continued

- Medical IT-Network Risk Management
  - Risk Analysis
    - Hazards must be identified and assigned risks
  - Risk Evaluation
    - Each hazard with unacceptable risks must have Risk Controls applied
  - Risk Control
    - Includes (in this order) Inherent Control by Design, Protective Measures, and Information for Assurance
    - Risk controls must be evaluated for reviewed for new risks and their effectiveness validated
    - If risk reduction is not practicable, a risk/benefit analysis must be conducted and documented
  - Residual Risk Evaluation And Reporting
Section 4 – Life Cycle Risk Management – Continued

- Change-Release Management And Configuration Management
  - Change-Release Management Process
    - Created by the Responsible Organization, documented and implemented by the Medical IT-Network Risk Manager
  - Decision On How To Apply Risk Management
    - Change Permits may be approved for routine changes, if risk management shows negligible/acceptable risks
    - New projects or substantial changes require full review
  - Go-Live
    - Before approval the Medical IT-Network Risk Manager reviews, approves, and documents residual risks and specified changes
Section 4 – Life Cycle Risk Management – Continued

- Live Network Risk Management
  - Monitoring
    - Monitoring is required to detect emerging risks, effectiveness of risk, and accuracy of original estimations of risk
    - Monitored items include environmental changes, operational/performance feedback, information about components or similar networks, reported events, and audit results of policies and procedures
  - Event Management
    - Negative events shall be captured, documented, evaluated, and changes proposed, with corrective and preventive actions tracked and reported
Life Cycle Risk Management is neither Easy nor Impossible, but Necessary.

“Take nothing for granted; do not jump to conclusions; follow every possible clue to the extent of usefulness . . . . Apply the principle that there is no limit to the amount of effort justified to prevent the recurrence of one aircraft accident or the loss of one life.”

Section 5 – Document Control

- **Document Control Procedure**
  - All relevant documents in the Medical IT-Network life cycle shall be revised, amended, reviewed, and approved in accordance with a document control procedure.

- **Medical IT-Network Risk Management File**
  - Provide traceability for each identified hazard to:
    - the risk analysis;
    - the risk evaluation;
    - the implementation and verification of the risk control measures; and
    - the assessment of the acceptability of any residual risk(s) with approval.
  - Need not physically contain all the records and other documents; however, it should contain at least references or pointers to all required documentation.
Final Thoughts

In flying I have learned that carelessness and overconfidence are usually far more dangerous than deliberately accepted risks.

— Wilbur Wright in a letter to his father, September 1900
Contact Information

Rick Hampton
Wireless Communications Manager
Partners HealthCare System
One Constitution Center, Suite 200
Charlestown, MA  02129
Office: 617-726-6633
Cell: 617-968-2262
RHampton@Partners.org