Risk Managers and IEC 80001-1

February 2011

Tom Judd
National Project Director, Clinical Technology

Brian Birch
Enterprise Architect, Information Technology
The bottom line ....

- A new Risk Management standard emerged in 2010

- It is based on interactions between technology and care delivery; this challenge will continue to grow

- We have an opportunity to proactively prepare for its coming further adoption; we need your help!
Background

80001-1: New Risk Management Standard in 2010
- Application of RM for IT-networks with medical devices
  - Safety, Effectiveness, and Security are key measures
- Approved by IEC, ANSI, and AAMI so far (standards & device entities)
- Example clinical use cases in 80001-1 documents*
  - Remote ICU / Distance Medicine (iPhone issues, etc.)
  - Ultrasound Imaging

Biomedical Device Integration Council oversees
- Physician leaders
- Patient Care Services
- IT, Clinical Technology, Others

*80001-1 clarifying document #719
BDIC project: Urology Digital OR-Endoscopy Image Management Simulation

February 2011
FDA Testimony to Office of National Coordinator (ONC) 2/25/10

- Patients, clinicians, and user facilities have voluntarily reported Health IT (HIT)-related adverse events.

- In the past two years, received **260 reports of HIT-related malfunctions with the potential for patient harm** – including **44 reported injuries** and **6 reported deaths**.

- Because these reports are purely voluntary, may represent only the tip of the iceberg in terms of the existing HIT-related problems.

- Reported by Dr. Jeffrey Shuren, Director FDA/CDRH to ONC HIT Policy Committee Adoption/Certification Workgroup

Further information re data cited:

- Errors of commission, such as accessing the wrong patient’s record or overwriting one patient’s information with another’s (this sometimes can be an issue in incidents involving medical identity theft);

- Errors of omission or transmission, such as loss or corruption of vital patient data;

- Errors in data analysis, including medication dosing errors of several orders of magnitude;

- Incompatibility between multi-vendor software applications and systems, which can lead to any of the above.
We are trying to determine the best approach ...
- Need your help!

Voluntary standard; The Joint Commission and FDA reviewing; perhaps 2-3 years before more controls

Raises visibility of issues with our IT Network & Clinical Technology (aka Clinical Engineering)

The standard raises need for a Health IT Risk Manager (HIT RM) to monitor & review Risk issues
- Implementation of 80001-1 very process-driven
- Ensure that care providers in medical centers have input before Network changes are made
IEC 80001-1 Concerns

- **Recent HIT RM Challenges** (for us & HDOs nationally)
  - Alarm Management
    - Alarm to sent to caregiver via various technologies
  - Infusion Pumps
    - Adverse events

- **Changing Network**
  - Clinical Implications
  - How technology interfaces with care providers
What does BDIC want from Clinical Risk Managers

**Players**

- Clinical Risk Managers
- Clinical Technology medical device experts
- Centralized IT “Network” monitoring group
  - Analysis? Information Spread?
- Existing Product Safety Council
  - Locally managed is best
  - Use their Escalation model?

**Next Steps?**

- BDIC: Security analysis underway
- Clinical Risk Managers: Safety & Effectiveness leaders
Questions?

Tom.Judd@kp.org

Brian.Birch@kp.org
Appendix

Clinical Use Case Details

Source: IEC 80001-1 (Clarifying Document #719) 2010
Application of risk management (RM) for IT-networks incorporating medical devices: Step by Step RM of Health IT-Networks; Practical Applications and Examples
Remote ICU - Distance Medicine

Use Case
- A Network is used to transfer real-time patient data from a remote site to be used by a local clinician for purposes of monitoring, diagnosing and determining treatment.
- PATIENTS being monitored are those in a post heart surgery step-down unit. Acuity is typically lower than critical care units.
- The “local clinician” in this case is a telemetry clinician (technician, nurse, doctor, etc) who is geographically separated from the remote PATIENT. In this case, the clinician’s site is connected to the PATIENT’s site via a Network. [KP will increasingly link to remote providers via iPhones.]

Network Analysis
- The network under analysis includes an enterprise level access switch to which the patient monitors are attached in the step-down unit, a Network with a guaranteed bandwidth of 12 gigabytes for all traffic from this site (includes other applications besides the remote monitoring), and an enterprise level access switch at the clinician side.
- Based on bandwidth and delay requirements from the MEDICAL DEVICE Manufacturer, the Network has been provisioned to accommodate the traffic from the monitors as well as that predicted to be used by other applications sharing the link. The Network provider has guaranteed a minimum service level which includes bandwidth sufficient for these applications (current use)

Risks Identified
- Intermittent connectivity
  - Unplanned non-real-time traffic attempting to use link causes overloaded Network link. Waveform display is choppy and incomplete. Delay in provision of care because remote clinician is unable to evaluate PATIENT ECG waveform. ... Or ... Alarm data not received. Delay in provision of care because clinician is unaware of patient in need of treatment.
- Complete loss of connectivity
  - Remote clinician must determine treatment without access to real time patient data.
Ultrasound Imaging - Software Updates

Use Case

- A new Ultrasound (US) system periodically has manufacturer software updates (aka “patches”) to enable better care delivery. The US system uses a Microsoft (MS) Operating System (OS).
- MS releases a patch to their OS closing an exploitable (MS reports a worm exists) vulnerability on a US. Impact to the delivery of care could result (reduced speed; unusable functions) if US exposed.
- The US manufacturer requires time to verify and validate the patch before it can be applied to the MEDICAL DEVICE. The worm has been found on Network-connected devices. The Network is used to retrieve PATIENT information and schedule procedures from an HIS/RIS system (e.g., DICOM Modality Worklist Server). The Network provides means to archive US studies from an US to PACS.
- As a final step, the Network is used to report back to the HIS/RIS successful study completion. A workstation component can be added to pull the US Images from a PACS server in order perform other processing such as measurements and reporting off the US system, to create an efficient workflow for PATIENTs and Radiologists.

Network Analysis

- The Ethernet network covers the entire hospital and supports 100 MB / Gigabit network speeds.
- The US is a mobile MEDICAL DEVICE and tends to move between catheterization suite, ED, and clinical rooms throughout the hospital. There are VLANs defined to create enclaves (protected networks) where MEDICAL DEVICES are used, and to separate MEDICAL DEVICE from desktop PCs.

Risks Identified

- Unauthorized access to data (PATIENT info or org. info) & loss of connectivity (access to procedure data limited/ denied)
  - (Security of Data) Unknown to the clinician a virus or worm can automatically mine for PHI and export login and PHI to an unauthorized location.
  - (SAFETY) During a clinical scan (OB, CARD, GI) consumption of hardware resources by the malicious software degrades performance resulting in the imaging procedure failing or treatment compromised (e.g., amniocentesis needle navigation impossible).
  - (Effectiveness) Access to a Modality Worklist Server is denied due to heavy network congestion; or System is not able to access a PACs to store acquired image data for use in off cart or other medical procedures. Scheduling system failure and clinician/technician must resort to manual methods...