ONC FACA HIT Standards Committee
Clinical Operations Workgroup

Medical Device Hearing on

Barriers and Enablers for Medical Device Interoperability

Washington, D.C. ~ March 28, 2011

Respondent: ***Todd Cooper***

Principal, 80001*Experts*, LLC
Convenor, ISO TC215 Health Informatics – Devices
Co-Chair, ISO/IEC Joint Working Group 7 "80001"
Co-Chair, HL7 Health Care Devices Working Group
Chair, IEEE 11073 Medical Device Communication Working Group
Board of Directors, Integrating the Healthcare Enterprise (IHE) International, Chicago, IL
Co-Founder IHE Patient Care Device Domain
Former Board of Directors, ANSI Healthcare Information Technology Standards Panel (HITSP)
Co-Editor, HITSP Technical Note 905 – Common Device Connectivity

Panel: ***Device & Data Security***

Todd Cooper – *General Testimony*

Thank you for the opportunity to discuss the topic of medical device interoperability before the committee today, and especially the discussion of blockers and enablers for widespread adoption of open standards-based technologies that can have a significant impact on the use of rich medical device data to improve the meaningful use of EHRs and other health care technologies.

My written comments to the questions below provide more detailed responses for the general topic of the integration of medical devices into healthcare enterprise systems such as EHRs, as well as the specific topic of device data and system security. Here I would like to highlight the following key points:

- ✓ Basic integration of medical device data streams into EHRs is not a technological nor a standardization issue, but rather a decades old business model problem: lack of sustained market demand. The ONC can play a pivotal role in breaking this chicken-and-egg problem that has plagued the industry and blocked widespread deployment of open standards-based medical device interoperability technologies, both at the point-of-care and throughout the enterprise.
- ✓ Standards and standards profiles and frameworks from organizations such as HL7, IEEE, ISO, IHE and Continua exist today and are becoming increasingly deployed in commercially available products. If device interoperability meaningful use criteria are specified for Stage II and III, as has been indicated they will in the past, technology suppliers are ready to meet the call with interoperable products.
- ✓ The #1 requirement for integration of device data into EHR and other systems – whether local or remote – is that of semantic interoperability. This is being addressed by harmonization activities within IHE, HL7, ISO TC215, IEEE 11073, and IHTSDO. A key element of this is the IHE Patient Care Device (PCD) domain's Rosetta Terminology Mapping (RTM) profile that maps vendor proprietary semantics to a standardized ISO/IEEE 11073 representation. These in turn are also being mapped normatively to both SNOMED-CT as well as LOINC. Thus addressing the primary need for consistent medical device semantics regardless of the source.
- ✓ To successfully deploy and maintain networked medical device technology – safely, effectively and securely – healthcare delivery organizations must understand what is required (from hazards to controls to monitors), and implement a comprehensive, multi-stakeholder networked medical technology risk management program as provided for in standards such as IEC 80001-1. Without such an activity, systems may be deployed, meaningful use criteria met, checks mailed, only to see the resulting systems crash and burn as a result of patient safety incidents, technology failures (especially in a heterogeneous environment), or compromised security.
- ✓ The field of IT security is very mature, with a strong framework of standards, policies, guidance, infrastructure, and services. Though networked medical devices present increased patient safety risks (thus their categorization as "medical devices"), and challenges to ensure their effectiveness related to network connection is maintained, there is no need to create or profile security components that are unique to medical devices. What is important is to ensure that technology suppliers properly disclose their security needs, risks and controls, and then that a dialogue is engaged with end users to ensure that the security framework for deployed systems is properly implemented and provides reasonable protection for the network and its components. These requirements are discussed in the forthcoming IEC 80001-2-2 security technical report, and

embodied in documents such as NEMA's Manufacturer Disclosure Statement for Medical Device Security (MDS[2]) form. An IHE PCD Cyber Security white paper is also currently out for public comment[8].

Finally, these points along with may other considerations along with an analysis and mapping of meaningful use criteria to medical device informatics is provided in more detail in HITSP TN905 Common Device Connectivity[1].

I applaud the ONC for convening this hearing, and thank you again for the opportunity to participate in the discussions.

All Panels – General Questions

Question #1: *What is your experience with health care devices and device interoperability? Have you experienced specific problems where standards might contribute to solutions?*

Device Interoperability Experience:

Over 20 years specifying, engineering and deploying medical device systems, especially infusion pump and ventilator systems. All of these systems supported some level of integrated network capabilities, both providing comprehensive real-time data streams as well as supporting remote configuration and control functions. Networking solutions include simple serial connections to wired and wireless networking, including infrared-based technologies. Solutions also include company proprietary protocols as well as standards-based implementations. As Technical Director of the IEEE's Medical Device Communication Industry Group, Todd oversaw the development of multi-vendor standards-based medical device interoperability prototyping projects. This was continued as a co-founder and Technical Committee co-chair for the IHE Patient Care Device (PCD) group, where multi-standard solutions were defined, prototyped by multiple medical device product vendors, tested at IHE Connectathon events, and are now integrated into commercially available products.

In addition to leading numerous medical device informatics and interoperability standards activities – in IEEE, ISO, and HL7 – Todd has also been a co-chair of the ISO/IEC joint working group that recently published the IEC 80001-1 medical IT-network risk management standard, focusing on what is needed to ensure the safe, effective and secure deployment of networked medical technologies.

Problems Demanding Standards Solutions:

We have made significant profit from the continued lack of open standards-based medical device interoperability.

Integrating two systems from different vendors (e.g., a ventilator and a physiological monitor – for parameter display) can easily run well into six figures.

A major industry has resulted that provides middleware applications to adapt and translate medical device data streams to formats and protocols that can be consumed by enterprise applications such as EHR-S. This adaptation / translation always results in data quality issues, increased latency, reduced content, … and increased overall system complexity.

Why this lack of standardized interoperability? Inconsistent, uncoordinated end user demand!

To be sure, adding functionality to any medical device system represents considerable effort and expense, given the regulatory requirements put in place by the FDA to ensure that these systems are safe and effective and can be allowed on the market. Even relatively simple enhancements such as the addition of a standardized interface option, must be balanced between development costs vs. potential market, and to date open standards-based interoperability consistently comes up short.

There are always more features to be added to existing standards and new standards to be developed in order to support an ever evolving health care sector, but the primary reason that existing standards and standards profiles / frameworks are not widely utilized for integrating medical device technologies is a business model issue – not one of a lack of available standards. This includes standards that would support the previously published meaningful use criteria as analyzed and mapped to standards efforts in HITSP TN905 Common Device Connectivity[1].

The ONC can significantly impact the industry by adding Stage II and III criteria that reward the use of standardized medical device informatics and interoperability technologies, such as those based on ISO/IEEE and HL7 and profiled by IHE.

Question #2: *Are there areas where standards are more mature or less mature?*

Most standards leveraged in medical device interoperability frameworks and profiles are very mature:

- ✓ HL7 Version 2
- ✓ ISO /IEEE 11073 (terminology & information model)
- ✓ SNOMED-CT and LOINC terminologies (esp. for HL7 CDA documents that contain medical device information)
- ✓ NTP / SNTP for time synchronization
- ✓ Widely deployed IEEE 802-based LAN technologies

[1] HITSP TN905 is available at http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=5&PrefixNumeric=905

Additional standards were more recently published, but are based on many of the same standards above or other widely deployed technologies, including:

- ✓ ISO/IEEE 11073 Personal Health Device (PHD) Standards
- ✓ HL7 Personal Health Monitoring Report CDA
- ✓ (for Wide Area Networking – WAN) Web Services (including SOAP 1.2, WS-I Basic Profile (BP 1.1), WS-I Basic Security Profile 1.0 (BSP 1.0), Simple SOAP Binding Profile 1.0 (SSBP 1.0), and Transport Layer Security (TLS).

Most of the above standards support "intermediary architecture" – where the medical devices (e.g., ventilator) uses a proprietary direct connection to an intermediary system (e.g., a gateway) that then uses a standard interface to other enterprise-based applications. Some devices (such as anesthesia workstations) have integrated support for the above standards directly into their "first link" interfaces.

The greatest lack of maturity is in the implementation and deployment of point-of-care "first link" standardized interfaces, that are still dominated by proprietary technologies. Again, though, this is primary due to business model issues and not a lack of standardization.

The ISO/IEEE (CEN) 11073 standards provide for these connections; however, primarily business issues have hindered their widespread implementation and deployment.

The more recent "ICE" standard[2] provides a framework for establishing essential safety requirements for a patient-centric point-of-care integrated clinical environment; however, it is too early to determine whether or not this standard will have a broad impact on the industry and see significant availability of commercially available systems, especially over the next 5+ years.

The recently published IEC 80001 risk management standard for medical IT-networks[3] may also have a significant impact on the management of networked medical technologies, especially across heterogeneous shared infrastructure, but its adoption is only starting to be considered by technology suppliers and end users. Given that it is based on existing and widely used medical device risk management and IT service management standards, it is well positioned to meet the unique challenges presented by convergent networks, ensuring that the resulting system of systems are safe, effective and secure.

---

[2] ASTM International #F2761 – 09 (2009) *Medical Devices and Medical Systems — Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE) — Part 1: General requirements and conceptual model .*

[3] IEC 80001-1:2010 *Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities*

Question #3: *What standards or standards-related capabilities are most relevant and important to the meaningful use of EHR technology?*

Standards Relevant to Meaningful Use of EHR Technology:

For medical device communication, focusing on non-imaging systems (e.g., physiological monitors, infusion pumps, ventilators, real-time clinical decision support systems, etc.), the primary relevant standards are identified in the response to Question #2 above.

Standards-related Capabilities Relevant to Meaningful Use of EHR Technology:

#1 – Semantic Interoperability with high resolution, device-sourced semantics, as opposed to the higher-level semantics provided by terminologies such as SNOMED-CT. Without consistent semantics across medical device technology manufacturers and consumer applications such as EHRs, it will be very difficult to achieve meaningful use objectives. Non-medical device terminologies often have a 20:1 or greater ratio of original device-sourced semantics mapped to their more generic counterparts in other systems. That said, many applications require use of these clinical terminologies; whereas, device manufacturers desire to use as precise a term as possible. As a result, it is important to maintain the originally acquired semantics as well as any clinical terminology mappings. For example, a personal health device will supply ISO/IEEE 11073 semantics; however, when this information is captured in a CDA document, the SNOMED-CT "equivalent" must be supplied.

Note that there are numerous projects that have completed or are in process to provide this semantic interoperability, including the IHE PCD Rosetta Terminology Mapping (RTM) project that maps from proprietary medical device terminologies to standardized ISO/IEEE 11073 concepts. This includes the capturing of "co-constraints" that specifies the valid units of measurement (both ISO/IEEE 11073 & UCUM representations), and value enumerations. There are also active projects to establish normative mappings between ISO/IEEE 11073 terminology, SNOMED-CT and LOINC.

#2 – Comprehensive risk management should be employed to assess the potential hazards and hazardous situations that can result from the integration of medical device data flows into an EHR, as well as distributed medical device applications that include EHR System components (such as CDSS). This is necessary to ensure that the resulting integrated technologies – leveraging shared infrastructure, both public and enterprise-based - maintain the safety and effectiveness established by system manufacturers and approved to be marketed by the FDA, as well as the needed security to ensure confidentiality, integrity and availability. With out this in place, systems

could meet meaningful use criteria (as stated today), but unintended consequences could result in overall system failures that would nullify any gains toward improved safety, quality of care, and clinical workflow efficiency. Examples of these system failures are very well documented, including misidentification of patient data resulting in delayed or mistreatment, system downtime (such as losing wireless infrastructure for … days, weeks, or longer), or compromised security that can result in medical device systems becoming infected with viruses and taken off line.

The IEC 80001-1 standard provides a key element to achieving this comprehensive medical IT-network risk management. Since it is based on the same standards used by medical device manufacturers to meet regulatory requirements (e.g., ISO 14971), it can also play an important role in meeting the FDA's MDDS requirements. Other key standards in this area include ISO 20000 (all parts) for IT service management, ISO/IEC 15408 IT security techniques, to name a few.

Question #4: *What do you see as key barriers to effective use of health care devices to advance health and wellness?*

The primary barrier is a lack of products that support existing standards-based solutions, both to achieve technical as well as semantic interoperability. As stated above, this is the result of a decades old chicken-and-egg standoff: Manufacturers have a very significant investment in their current proprietary technologies and do not see the sustained market demand or other funding sources that would enable them to deploy interoperable products. End users – healthcare providers – specify interoperability in their RFPs; however, given the lack of product availability, as well as the lack of consistency and sustained demand between providers, it is often dropped or falls down the priority list.

It should be noted that there are proprietary solutions that support some level of health care device integration to advance health and wellness, along with middleware systems that support movement toward more standardized integration (e.g., converting proprietary intefaces to standardized technologies such as ISO/IEEE 11073 and HL7). But as mentioned above, there are significant downsides to these approaches.

Groups such as IHE PCD with their Users Guide[4] and the CIMIT / MDPnP program with their "MD FIRE"[5] provide template RFP language that if adopted, can provide the market pressure that manufactures need to justify investment in interoperable solutions.

[4] Available at http://www.ihe.net/Resources/handbook.cfm
[5] Available at http://www.mdpnp.org/MD_FIRE.php

Note that sections 3 & 4 of HITSP TN905 Common Device Connectivity[1] provide a more comprehensive discussion of issues related to achieving widespread integration of health care devices in health care. For example, the importance of differentiating between medical and non-medical health care devices.

By including Stage II & III criteria that requires use of open standards-based medical device interoperability solutions (as described above), the ONC can change the status quo that has crippled the industry for decades, and remove the key barrier to effective use of health care devices to advance health and wellness.

Question #5: *If you could wave a magic wand to effect one change to enable more effective and widespread use of health care devices, what would that be?*

See answer to Question #4 – final paragraph.

Waving a wand to push interoperability back from gateways and intermediary systems to achieve ***plug-and-play interoperability and the "first link" device interface is clearly the ultimate end game.*** Positive patient identification and device association, automatic discovery, configuration and network integration, wired and wireless, patient-aware, etc. … along with the high level of patient safety, system effectiveness and data & system security … health care devices would be used everywhere (as evidenced by analogous systems in other industries).

Given the increased patient safety, design and regulatory challenges associated with patient-connected device development, solving this problem is much more difficult than integration of device data into an EHR, especially using intermediary systems. That said, including Stage III criteria that recognizes this level of health care device interoperability can also greatly impact the effective use of medical device informatics.

Device & Data Security Panel Questions

Question #17: *What are the security requirements for devices in different care settings, e.g. SNIF vs. Hospital vs. Home or other remote monitoring?*

IEC 80001-1 defines DATA AND SYSTEM SECURITY as an operational state of a medical IT-network[6] in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability. This security is assured through a ***framework of policy, guidance, infrastructure, and services***

[6] This is a network into which at least one medical device has been connected.

designed to protect information assets and the systems that acquire, transmit, store, and use information in pursuit of the organization's mission.

A follow-on security guidance technical report in development within ISO / IEC JWG7, namely IEC 80001-2-2, focuses on the disclosure of medical device security needs, risks and controls. It then goes on to present a standard semantic framework in which this ***disclosure*** and subsequent ***dialog*** may proceed, including the use of security capabilities (e.g., audit controls, malware detection/protection, and UUIDs), along with stated goals for each capability and associated end user needs. Another method to achieve this disclosure is the use of NEMA's Manufacturer Disclosure Statement for Medical Device Security (MDS[2]) form[7].

Care contexts – hospital, home, skilled care, etc. – are not explicitly mentioned in the security definition above but are factored in as part of the overall 80001 risk management process, along with the networking technologies used (wired, wireless, BAN/PAN/LAN/WAN), therapeutic / diagnostic services being supported, patient characterization, etc.

Security requirements do vary based on the care context, intended operators, systems (medical and non-medical) being integrated, infrastructure, etc., but the key is to analyze the application, and properly manage the identified risks and vulnerabilities through a "framework of policy, guidance, infrastructure, and services."

Per the question above, a key issue is to understand those elements of the network infrastructure that are within control of the responsible organization and those that are not, and thus pose a unique set of challenges. For example, the use of public vs. private infrastructure, or end users being patients or professionals delivering care. In each of these cases, unique risks and requirements must be considered and addressed.

Question #18: *How do existing security standards support network-enabled devices today?*

There are many publications that detail the security standards that can be leveraged in support of networked technologies in a health care context, including the emerging IHE PCD Medical Equipment Management and Cyber Security white papers[8].

The key is to recognize that systems and software applications are classified as "medical devices" based on their intended use and their potential impact on patient safety. If they have a network connection, then the manufacturer must disclose the potential hazards and

[7] Available at http://www.nema.org/stds/hn1.cfm

[8] The MEM white paper is available at http://www.ihe.net/Technical_Framework/#pcd, and the Cyber Security WP is open for public comment at http://www.ihe.net/Technical_Framework/public_comment.cfm#pcd.

required security risk control measures that must be maintained in order to ensure that the medical device operates in a safe and effective (i.e., in accordance with its intended use) manner.

This field and industry is very mature, and existing security standards and technologies support networked-enabled medical devices … today; however, they are only effective to the degree that the network and device connection to that network has been properly analyzed and that both the technology suppliers as well as the responsible organization for the overall operation of the network collaborate to ensure that the appropriate security policies, procedures and risk control measures are implemented and maintained.

Question #19: *What network and connectivity issues relate to remote monitoring with intermittent connectivity?*

Network resiliency and availability are classes of hazards that must be considered during any analysis activity. Appropriate system design elements and network risk control measures must be deployed and continuously monitored for effectiveness.

The following figure illustrates an 80001-based risk management risk analysis and evaluation process. Note the role of security hazards and harms or unintended consequences.

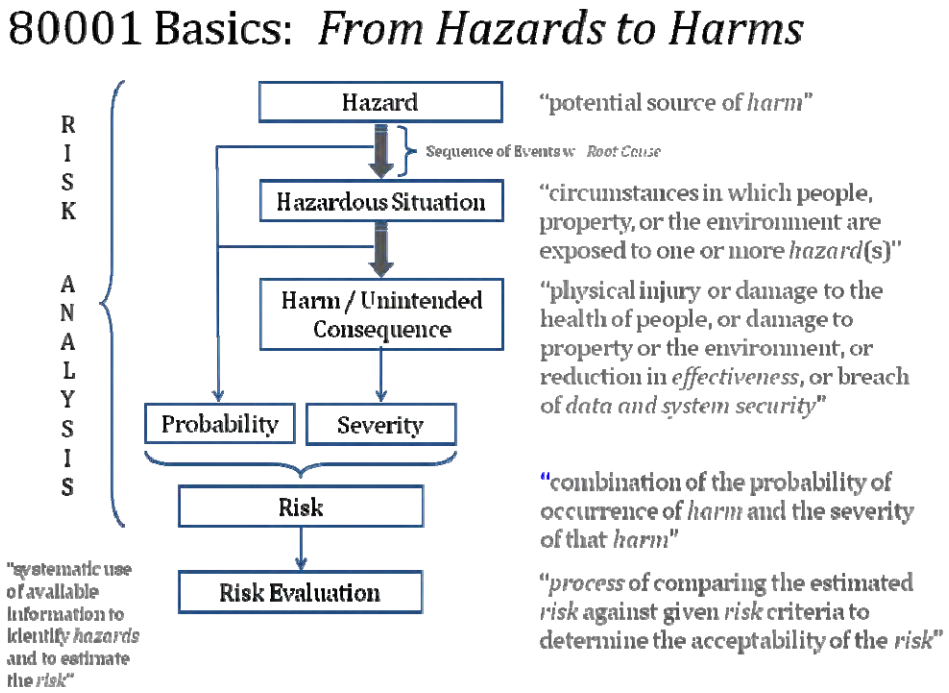

Figure 1 Risk Analysis & Evaluation[9]

[9] From AAMI "Getting started with 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks."

As a result of the above activities, the following sample process (not complete) illustrates the kinds of networking issues that might be considered (including, for example, unauthorized access to private data), and how this is then subject to risk control activities, risk-benefit analysis (RBA), and ultimately the decision to "go live" … or abort!

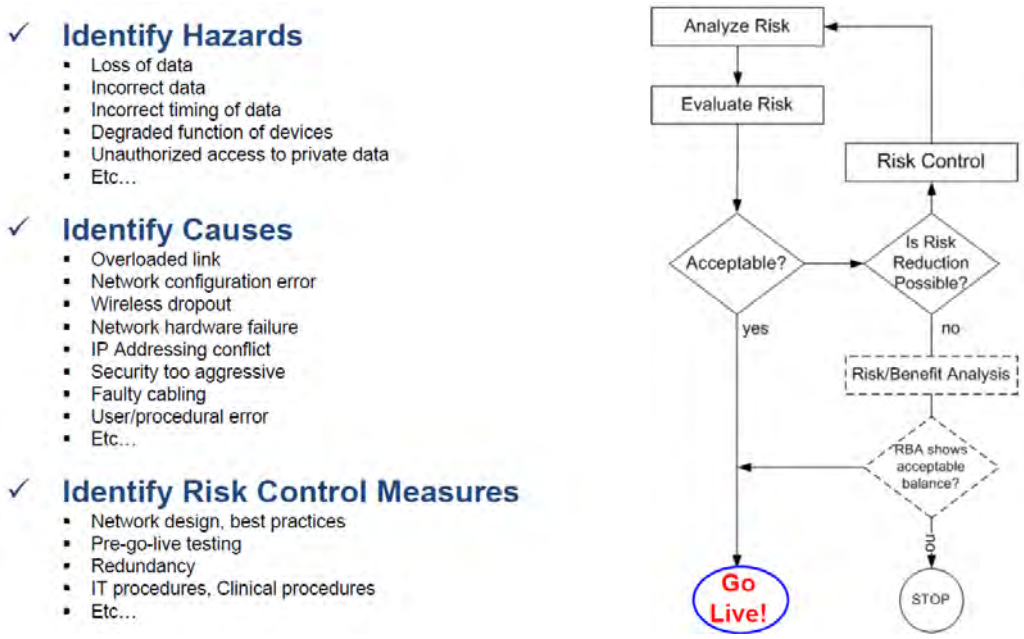

Figure 2 Risk Analysis, Evaluation and Control with Examples[10]

[10] From AAMI webinar, January 19, 2011, "Understanding and Benefiting from AAMI / IEC 80001-1."