

Safety First! Safe and Successful Digital Network Wireless Medical Device Systems (WMDS)

HIMSS February, 2006 Annual Conference - San Diego, CA

Elliot B. Sloane, Ph.D.

MIS Faculty, Villanova University

Todd Cooper


President, Breakthrough Solutions



Annotation: Digital Network based Wireless Medical Device Systems (WMDS) are rapidly approaching the "ubiquitous" stage. Specification, procurement, installation, and management requires applying appropriate standards and best practices to ensure safe, reliable, and affordable systems.

Viewer Goals of this presentation:

1. Recognize the critical safety features that must be assured for any medical device network, including Quality of Service (QoS) and life-critical patient alarm integration
2. Identify the current and emerging wireless technologies that should be considered - and/or avoided - and list the critical limitations of each
3. Name and explain the appropriate AAMI, ANSI, IEEE, IEC, ISO, and HIMSS/IHE standards that must be considered for wireless medical device systems
4. List and define the key legal and technical requirements to ensure a secure wireless medical device network
5. Describe the critical success factors to ensure specification, procurement, installation, and management of safe, reliable, and affordable medical device systems



BioBrief: Elliot Sloane

**“Dual citizenship” in Clinical Engineering
and Information Systems and Technology!**

30+ Years of CE and IT/IS Expertise

- **Faculty, Department of Decision and Information Technologies, Villanova University, since 2000**
 - Teaching, research and publishing in databases, decision support, healthcare technology assessment and management, telecommunications, and health informatics.
 - Senior Member, IEEE
 - Board of Directors, IEEE EMBS
 - Past President, ACCE
 - Board of Directors, ACCE Foundation

Vice President, ECRI – 15 years, CIO & CTO
Medical technology research, testing, and education; medical device nomenclature; standards directories; product evaluations; forensic/accident investigations

Vice President, MEDIQ/PRN – 10 Years, COO & CTO
Medical device & drug distribution, service, rental, and manufacturing

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Dr. Elliot B. Sloane is a clinical engineer, information scientist, a professor of Decision and Information Technologies at Villanova University, and he serves on the HIMSS IHE Strategic Planning Committee. He is a past president of the American College of Clinical Engineering (ACCE), heads the ACCE Task Patient Safety/Medical Errors, and co-chairs the joint ACCE/IHE Patient Care Device Domain Task Force. Dr. Sloane originally worked at the Emergency Care Research Institute (ECRI) for 15 years, where, as vice president of laboratory operations he was responsible for medical device evaluations, accident investigations, and all information systems design and development. He then spent 10 years as a vice president for MEDIQ/PRN Life Support Services, where he was responsible for nationwide medical equipment service, support, regulatory compliance, and quality assurance. Since 2000, he has been a faculty member Villanova University, teaching healthcare informatics, database management, eCommerce, and telecommunications, and his research and publication activities are in the medical informatics area, including medical decision support systems, wireless medical device networks simulation and validation, and healthcare information system security and reliability. He is the faculty advisor for Villanova's award-winning Business Ethics team, as well

Dr. Sloane has served as a consultant to the World Health Organization since 1984. He has been a frequent international guest clinical engineering and healthcare information technology faculty member for government agency training programs in regions including Australia, Latin America, the Caribbean, both Western and Eastern Europe, and Central Asia. Dr. Sloane is an invited presenter, session chair, and track chair at numerous international clinical engineering and information technology conferences. Dr. Sloane serves on an NIH SBIR grant review committee for elder-care technologies, and he advises the Ben Franklin Technology Partnership on Pennsylvania's regional business investments for biomedical technology companies. Dr. Sloane has twice served as President of the Association of Information Technology Professionals (AITP/DPMA - Montgomery County, PA Chapter), and is a director of their board as well as their regional Student Chapter Liaison. He has presented at the HIMSS annual conference in 2001 and 2002, 2003, and 2003, and published a medical decision support article in JHIM in 2002. Dr. Sloane is a Senior Member of IEEE, is on the Board of the Engineering in Medicine and Biology Society, and chairs the IEEE Membership Development Task Force for Healthcare. Dr. Sloane also provides professional and legal consulting services on medical information systems design, healthcare regulatory assurance, and clinical engineering projects to the medical and pharmaceutical industries.



BioBrief: Todd Cooper


25+ Years of Software Engineering & Medical Device Expertise

President, Breakthrough Solutions

- Medical device connectivity component software & consulting
- Chair, IEEE EMBS 1073 Medical Device Communication Standards
- Convenor, ISO TC215 WG7 Health Informatics - Devices
- Co-chair, HL7 Health Care Devices SIG
- Co-Chair, IHE Patient Care Devices Domain
- Board Member, ANSI/HIMSS Health I.T. Standards Panel
- Member, American College of Clinical Engineers

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Mr. Todd Cooper has over 25 years software engineering experience with over 15 years of that focused on acute care medical equipment, including infusion devices and ventilators. For the last 5 years he has served as President of Breakthrough Solutions, which provides consulting and component / middleware software for device connectivity. As chair of numerous medical device informatics and interoperability standards groups, Todd has worked diligently to advance the standardization and implementation of open real-time plug-and-play medical device interoperability, including serving as co-chair of the team drafting the IEEE 1073.0.1.1 *Health informatics – Point-of-care medical device communication - Technical report – Guidelines for the use of RF wireless technology*. Mr. Cooper worked at Kodak on high-speed motion analysis imaging systems before focusing on medical devices where his clients have included many of the major acute care equipment vendors.



Overview

- Critical safety feature needs
- Wireless technology review
- Applicable Standards
- Technical and legal requirements
- Critical success factors
 - Successful Specification, Procurement, Installation, and Management

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: When this session concludes, participants will:

1. Recognize the critical safety features that must be assured for any medical device network, including Quality of Service (QoS) and life-critical patient alarm integration

1. Identify the current and emerging wireless technologies that should be considered - and/or avoided - and list the critical limitations of each

3. Name and explain the appropriate AAMI, ANSI, IEEE, IEC, ISO, and HIMSS/IHE standards that must be considered for wireless medical device systems

4. List and define the key legal and technical requirements to ensure a secure wireless medical device network

5. Describe the critical success factors to ensure specification, procurement, installation, and management of safe, reliable, and affordable medical device sy



Why Patient Safety?

- **1999 Institute of Medicine (IOM) Report**
 - Up to 98,000 US patients die annually from medical errors.
- **Devices aren't blameless.**
 - ECRI has identified dangerous devices since 1968!
- **WDMS introduce new kinds of risks**
 - Life-critical alarms can be lost or delayed
 - Data errors introduce life-threatening artifacts
 - Data privacy can be difficult to assure
 - Ambulatory patients may be hard to locate

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: What do we mean by “Patient Safety,” and what risks do wireless medical devices create? Failures are easy to describe, e.g., Example 1: Wireless networks that are so busy that a life-critical alarm for a heart attack may be severely delayed or even lost. Example 2: Networks with sampling and data errors so high that heart waveform is distorted, filtering out clinical artifacts like Pre-Ventricular Contractions that would signal an impending heart attack. Example 3: Wireless networks allow unobtrusive detection – and tampering – creating novel patient, facility, HIPAA and JCAHO risks. Example 4: Wireless networks that successfully deliver such an alarm, but the ambulatory patient cannot be located until too late. In other words, wireless medical device networks can have problems like most of us experience with cell phones and wireless laptop computers. In healthcare, these problems can cause deaths and/or serious injuries, which adds to spiraling medical costs, too.




WMDS PATIENT SAFETY Critical Success Factors!

- *Timely and reliable alarms*
- *Reliable, accurate real-time vital signs data transfer*
- *Right devices associated with the right patient*
- *Continuity of critical services during mobility*
- *Improved clinician access from the point-of-care*
- *Secure information transfer*

“Success” is realizing these benefits!

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: How do you determine if your wireless network is “successful”, especially when measured in terms of safe care delivery? These factors provide insight into how wireless medical device connectivity can affect the delivery of care, but once systems are deployed (as they are to an increasing degree every day) the associated service constraints and risks must be well understood and mitigated in order to maintain and even enhance patient safety. For example, if you deploy vital signs monitoring devices and expect their wireless interface to communicate high priority alarm conditions, the risks associated with that service must be well understood. These include co-existence problems with other wireless technologies, intentional and unintentional interferers, loading limitations, etc. You might have a “smart pump” system that ensures a patient’s 5 Rights for infusion therapy, but if it depends on a wireless link (esp. during mobility) to interact with remote database systems, then a significant risk must be well understood and care delivery protocols adjusted appropriately. Safety also involves more than simply getting information exchanged in a timely fashion – it includes ensuring that the patient’s privacy is protected!



What is a Medical Device?

- According to the FDA, it is **ANY** product that affects the **diagnostic or therapeutic care** of a patient.
- Also, according to the FDA, if an IEEE 802.11g Wi-Fi access appliance is used to transfer life-critical data or alarms, **the Wi-Fi access point is treated as a medical device!**

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Legally, according to the Food and Drug Administration (FDA) “medical devices” include any device that affects the diagnostic or therapeutic care of a patient. [vital signs monitors, infusion pumps, vents, pulse-ox, glucometers, blood gas analyzers, ECG monitors, ...] Point-of-Care runs from OR to ICU to clinics to home to ... shopping malls and airplanes. Also according to the FDA, if a digital network appliance, like an IEEE 802.11g Wi-Fi access point, is used to transfer life-critical data such as heart alarms or drug ID data, the FDA considers that access point to be part of a medical device! That said, the risk management paradigm (and regulatory approaches) are shifting from a device oriented or single-vendor assessment approach to one that looks at the overall heterogeneous network where various device modalities from multiple manufacturers may be connected in an ad hoc manner and where residual risks (e.g., due to reductions in service availability) need to be mitigated by the end user (or some 3rd party service provider).

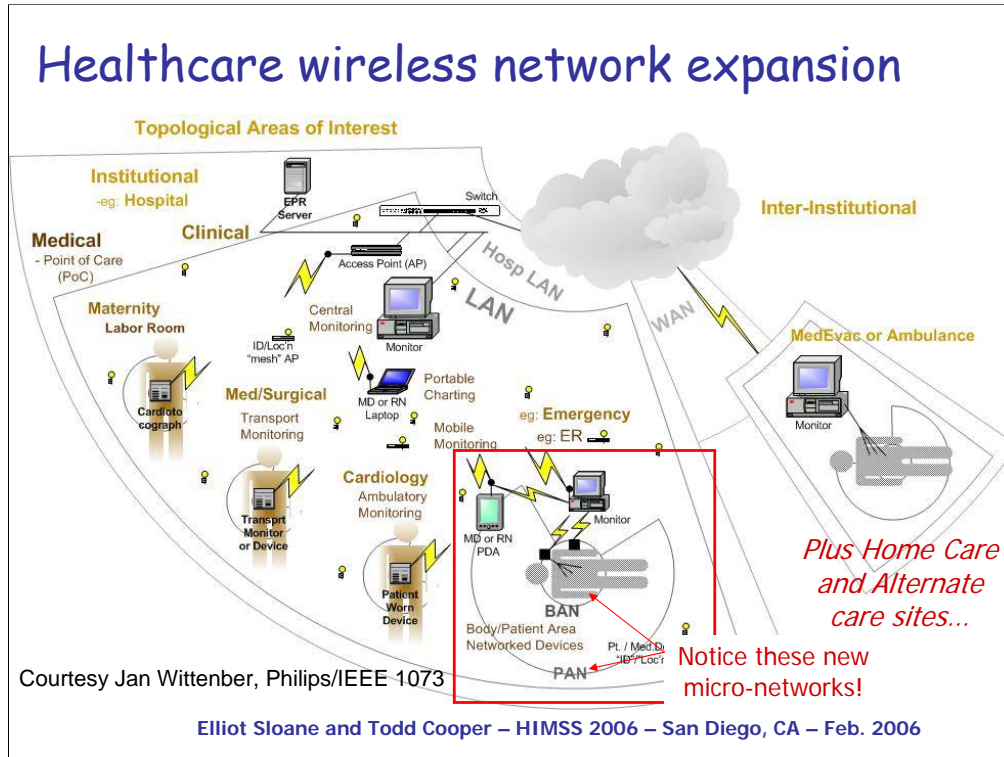
Potential FCC services utilized...

- ISM (Industrial, Scientific, Medical)
- WMTS (Wireless Medical Telemetry Service)
- PLMRS (Private Land Mobile Radio Service)
 - Public Safety
 - Bio-medical Telemetry
 - Industrial/Business
 - Private Land Mobile Paging
 - Radiolocation
- Paging
- MURS (Multi-Use Radio Service)
- FRS (Family Radio Service)
- GMRS (General Mobile Radio Service)
- MICS (Medical Implant Communications Service)
- Part 15
 - Medical Telemetry
 - RFID
 - Spread Spectrum
 - U-NII (Unlicensed National Information Infrastructure)
 - UWB (Ultra WideBand)
 - Medical Imaging
- Cellular Radio Service
- SMRS (Specialized Mobile Radio)
- AWS (3G) - Advanced Wireless Services Spectrum
- PCS (Personal Communications Service)
- *Amateur Radio*
- Private Operational Fixed Microwave

(Courtesy Rick Hampton / Partners, Boston)

Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: The range of technologies that may be utilized by healthcare providers is more than simple WiFi networks, WMTS or Bluetooth accessories, and requires very competent management - a Wireless Spectrum / Technology Czar who has the understanding and empowerment to manage use of these technologies so as to maintain patient safety and overall system performance, collaborating between all stakeholders. Some of the technologies listed on this slide may not have apparent uses, such as Amateur Radio, but when considering the crucial role of a healthcare facility especially during disasters when other communication technology is interrupted, the use of these alternative media become imperative!



Annotation: Illustrating The Wireless Problem – Each day more and more equipment is going “wireless” including many different device modalities from simple glucometers or pulse-oximeters to more complex patient vital signs monitors and ventilators. Both streaming real-time waveform and “batch” data uploads must be supported as well as multiple I.T. systems (bedside PCs, VOIP, RFID, streaming video, etc.), from multiple vendors and using many different wireless technologies (WiFi + BT + ZigBee + mobile phone + WMTS) as well as wired & wireless gateways. Environments must scale from a few clients to 100’s on a single subnet, and external factors such as nearby TV and radio stations can affect overall performance. And this must ALL WORK OVER A SHARED INFRASTRUCTURE! Many vendors are rushing off-the-shelf (COTS) technology into their systems; however, just because two systems use WiFi, doesn’t mean that they can interoperate without complication and configuration. Interoperability profiles and standards are required to ensure plug-and-play operation in heterogeneous environments.



GENERAL BENEFITS OF WIRELESS

- Ease of equipment placement (reducing wire & cable "nests")
- Options for real-time monitoring of ambulatory patients (mobile patients)
- Information easily accessed from anywhere within the coverage area (mobile staff)
- Information can be pushed immediately to clinician (e.g., lab results, alarms / alerts)
- Offers on- and off-campus alternatives to wired telephony and paging systems

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: When asked for the benefits of using wireless equipment, these are some of the quick responses from both vendors and clinical staff. It is important though to understand the stated and often assumed but not voiced benefits on the part of all stakeholders (clinical, engineering, biomedical, HIT, purchasing, etc.) to be able to ensure that (a) expectations are appropriately qualified (reality vs. hype) and (b) criteria established for evaluating proposed devices and networked systems and software to determine their efficacy for the target environment. Often, though, the residual patient safety and system operation risks are not recognized and understood, potentially resulting in unsuccessful technology deployment though both (a) and (b) above are met.

Universal wireless interfaces replace hard wires and proprietary data link communications

Untethered access to information

Mobility

Interoperability

Reduced cost and complexity

802.11b WiFi™

802.11g WiFi™

802.15.4 Zigbee™

802.15.1 BT™

802.3 Ethernet

Courtesy of NIST

Annotation: Partners Healthcare in Boston, the US Military and Veterans Administration, and many healthcare providers are collaborating to design the next-generation “Operating Room of the Future,” to ensure patient safety as well as reduce wasted time and labor. Wireless communication provides a major key to the emerging design. It enables constant contact with patient and staff regardless of location in the many areas within an OR environment the patient must move, and also eliminating confusing, dangerous, and unreliable jumbled tangles of wires on the floors and walls. Many classic “IT” digital network appliances are expected to allow inter-operability between infusion pumps, pulse oximeters, anesthesia ventilators, endoscope cameras, electrocautery units, etc. This will make the surgeons’ and anesthesiologists’ jobs more efficient, facilitates automated electronic health record capture, and helps ensure safety for the patient.



No Free Lunch: WIRELESS DRAWBACKS are REAL!

- Traditional Quality of Service (QoS) features associated with wired networks may not be fully supported
- QoS parameters such as throughput and latency may experience significant fluctuations due to coverage, traffic, and other emitters in the environment
- Cost may limit implementation of multiple / optimal technologies
- Appropriate prioritization protocols not always available, and overuse can quickly tax capacity and reduce compliance with QoS requirements

Annotation: Wireless networks provide a unique challenge to QoS management. Even with the advent of the IEEE 802.11e QoS standard, there are many ways that this service may be configured. In order to have devices (medical and non-medical) interoperate in a heterogeneous environment, the QoS management layer must be configured the same and must support authentication mechanisms that will ensure that devices that require different kinds of bandwidth will be granted that bandwidth (e.g., for priority alarm transmission regardless of network traffic) and other non-authenticated devices will either be given low priority or possibly no bandwidth at all. This area is the target of the new IEEE P1073.3.5.3 standard for wireless LANs.



A unique problem / challenge for medical devices...

To support safe and robust wireless
medical device systems...

<i>Device</i>	{	Semantics (alarms, RT waves, ID, ...)
<i>Interface</i>		Application Services (security, QoS)
<i>Profile</i>		Transport Technologies (WiFi ... ZigBee)

**Standards-based interoperability profiles are
required...from the transmitter to abstract
semantics!**

Annotation: As opposed to other device communication problems, the solution to the patient safety issues identified above require coordination between transport technologies, application services (e.g., QoS or security) and medical device informatics (e.g., unique device and patient ID, data classification (e.g., alarms vs. real-time waves vs. vital signs monitors)). Off-the-shelf (OTS) equipment + general IT solutions don't address critical patient safety needs. Interoperability profiles must coordinate between all three layers to be able to successfully deploy safe, effective and reliable systems that maximize patient safety. Focusing on individual technologies or single system / vendor solutions will not resolve the major issues. For example, a given medical device may need 2-3 different priority queues: one for alarms, one for real-time parameters or waves, and one for the rest of the stuff. That means, a given transport technology supporting QoS management, must support multiple priority queues, must allow authentication so that the device may be authenticated during connection establishment, and the appropriate semantics mapped to the allocated priority queues. And all of this must be done in a consistent and coordinated manner between different device modalities, and even non-medical device systems using the same infrastructure.



Key Problem: Patient Alarms

To support safe and robust wireless medical device systems...

- Alarm semantics must be standardized
- QoS must support semantic-sensitive priorities
- Priority access predicated on authentication
- Wireless technology: multiple priority queues

Alarm standards and profiles required!

Annotation: Chief among the challenging issues resulting from use of wireless technology is the detection and communication of patient and technical device alarms. Though alarm annunciation does not require a large amount of bandwidth, it does have a very low latency requirement: When an alarm condition is active, it needs to be communicated within seconds and cannot be delayed due to network traffic. This requires standardized device (alarm) events including priority, quality of service access / configuration that can ensure that high priority events and alarms are not delayed, network access and priority bandwidth allocation based on authenticated devices – “rogue” devices cannot get access to the net and launch denial of service type operations, and use of wireless technologies that ensure priority transfer of patient safety critical information, including support for multiple priority queues from a single transmitter. In other words, a medical device will have multiple types of information that it is trying to send, including alarms (highest priority / low bandwidth), real-time waves and parameters (high priority / potentially high bandwidth), and non-real-time information (e.g., periodic updates and control settings). Thus a single device wireless interface must be able to allocate appropriate amounts of bandwidth based on the communicated semantic information and associated QoS requirements. This demands standards, especially of alarm semantics and management.



Medical Device Alarms are REALLY complex!

- The “good news” is that standards are emerging from efforts driven by the Anesthesia Patient Safety Foundation over the past two decades.

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Understanding Medical Device Alarms is important, as they are much more complex than most technical or clinical users realize, even if they have significant expertise in their own domain. Few groups have invested as much effort as Anesthesiologists, and the Anesthesia Patient Safety Foundation, because of the unique complexity, risks and liabilities of medical device alarms in the operating room. Anesthesiology alarm design has been guided, too, by the aerospace and nuclear power industries, which have accumulated vast bodies of knowledge on human cognitive limits in dealing with multiple complex audible and visual alarm messages and formats.

	DRAFT INTERNATIONAL STANDARD IEC/DIS 60601-1-8
ISO/TC 121/SC 3	Secretariat: ANSI
Voting begins on 2002-06-07	Voting terminates on 2002-11-07
<small>INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE</small>	
 Medical electrical equipment — Part 1-8: General requirements for safety — Collateral standard: Alarm systems — Requirements, tests and guidelines — General requirements and guidelines for alarm systems in medical electrical equipment and in medical electrical systems	

Annotation: Medical device alarms have a precise definition. All diagnostic and therapeutic devices share these definitions. In addition, networks of devices – including the network itself – usually becomes part of the medical device in a real and legal fashion.

500

Table 201: ALARM CONDITION priorities

Potential result of failure to respond to the cause of ALARM CONDITION	Onset of Potential Harm ^a		
	Immediate ^b	Prompt ^c	Delayed ^d
Death or irreversible injury	HIGH PRIORITY ^e	HIGH PRIORITY	MEDIUM PRIORITY
Reversible injury	HIGH PRIORITY	MEDIUM PRIORITY	LOW PRIORITY
Minor injury or discomfort	MEDIUM PRIORITY	LOW PRIORITY	LOW PRIORITY OF NO ALARM SIGNAL

An INFORMATION SIGNAL, which conveys information without an injury connotation, may also be used for delayed minor injury or discomfort.

^a Onset of potential harm refers to when an injury occurs and not to when it is manifested.

^b Having the potential for the event to develop within a period of time not usually sufficient for manual corrective action.

^c Having the potential for the event to develop within a period of time usually sufficient for manual corrective action.

^d Having the potential for the event to develop within an unspecified time greater than that given under 'prompt'.

^e The design of MEDICAL ELECTRICAL EQUIPMENT with a therapeutic function usually prevents immediate death or irreversible injury by automatic safety mechanisms.

EN 1

Annotation: As formulated within the ISO Standard, medical device alarms are understood to have distinct priorities. “Immediate” alarms signify immediate danger, “Prompt” alarms signify impending problems, and “Delayed” alarms may signify low-risk situations. The diversity of alarms must be recognized and preserved when they move from place to place. Competent handling of critical alarms includes preserving all relevant clinical and technical data and time sequencing, as well as ensuring they are not delayed, distorted or lost in any operational situation. This standard actually defines the audible sounds and visible queues that should match the priority, in order to limit operator confusion and minimize stress.

580 Table 202: * Characteristics of the BURST of auditory ALARM SIGNALS

Characteristic	HIGH PRIORITY ALARM SIGNAL	MEDIUM PRIORITY ALARM SIGNAL	LOW PRIORITY ALARM SIGNAL ^d
Number of PULSES in BURST ^{a, b, c}	10	3	1 or 2
PULSE spacing (t_4) (see figure 201)			
between 1 st and 2 nd PULSE	x	y	y
between 2 nd and 3 rd PULSE	x	y	not applicable
between 3 rd and 4 th PULSE	$2x + t_4$	not applicable	not applicable
between 4 th and 5 th PULSE	x	not applicable	not applicable
between 5 th and 6 th PULSE	$2s \pm 0.2 s$	not applicable	not applicable
between 6 th and 7 th PULSE	x	not applicable	not applicable
between 7 th and 8 th PULSE	x	not applicable	not applicable
between 8 th and 9 th PULSE	$2x + t_4$	not applicable	not applicable
between 9 th and 10 th PULSE	x	not applicable	not applicable
INTERBURST INTERVAL ^{b, c, e} (t_b)	2,5 s to 15,0 s	2,5 s to 30,0 s	>15 s or no repeat
Difference in amplitude between any two PULSES	Maximum 10 dB	Maximum 10 dB	Maximum 10 dB
Where x shall be a value between 50 ms and 125 ms Where y shall be a value between 125 ms and 250 ms The variation of x and y within a BURST shall be $\pm 5\%$. MEDIUM PRIORITY $t_4 + y$ shall be greater than or equal to HIGH PRIORITY $t_4 + x$. It should be greater.			
^a See also Table 203 for characteristics of the PULSE ^b Unless otherwise specified in a particular standard for a particular MEDICAL ELECTRICAL EQUIPMENT ^c Manufacturers are encouraged to use the longest INTERBURST INTERVAL consistent with the risk analysis. Long INTERBURST INTERVALS can under certain conditions negatively affect the ability to correctly discern, in a timely manner, the source of the ALARM CONDITION. Writers of Particular Standards are encouraged to consider the longest appropriate INTERBURST INTERVAL of the auditory ALARM SIGNAL for the particular ALARM SYSTEM application. ^d The auditory component of a LOW PRIORITY ALARM CONDITION ANNUNCIATION is optional. ^e Unless inactivated by the OPERATOR, MEDIUM PRIORITY and LOW PRIORITY auditory ALARM SIGNALS shall complete at least one BURST, and HIGH PRIORITY auditory ALARM SIGNALS shall complete at least half of one BURST.			

Annotation: Alarm sounds are carefully defined, too, in order to avoid confusion and enhance prioritization. The audio tonal quality (i.e., pitch, or frequency), repetition rate, and other characteristics of all audible medical device alarms should be consistent with these ISO standards. Alarms that overshadow or mimic each other readily create dangerous situations in which uncertainty, confusion, or other cognitive overload has been shown to lead to tragic consequences.

NOTE: Ideally, these “intelligent sounds” one should be preserved as alarms pass from device to device!

Table 204—Characteristics of alarm indicator lights

Alarm category	Indicator color	Flashing frequency	Duty cycle
HIGH PRIORITY	Red	1,4 Hz to 2,8 Hz	20 % to 60 % on
MEDIUM PRIORITY	Yellow	0,4 Hz to 0,8 Hz	20 % to 60 % on
LOW PRIORITY	Cyan or Yellow	Constant (on)	100% on

Annotation: The color, blinking rate, and other characteristics of all visual medical device alarm should be consistent with these ISO standards. Alarms that overshadow or mimic each other readily create dangerous situations in which uncertainty, confusion, or other cognitive overload has been shown to lead to tragic consequences in the OR.

201.1.3 * INTELLIGENT ALARM SYSTEM

An explanation of any algorithm that can change the previously assigned priority or relative prioritization of a particular ALARM CONDITION or its effect on ANNUNCIATION shall be disclosed in the instructions for use.


If an ALARM SYSTEM can ANNUNCIATE more than one ALARM CONDITION of the same priority and it internally ranks the relative priority of the ALARM CONDITIONS within that priority, then an explanation of the effect this ranking has on ANNUNCIATION shall be disclosed in the instructions for use (see 201.2.5.2).

If an INTELLIGENT ALARM SYSTEM is provided, an overview of the logic decisions for ESCALATION and DE-ESCALATION and ALARM CONDITION DELAY(S) made by the ALARM SYSTEM shall be disclosed in the instructions for use. Alternatively, equivalent information concerning the function of the ALARM SYSTEM required for its safe use shall be disclosed in the instructions for use.

Compliance is checked by functional testing of the ALARM SYSTEM and review of the ACCOMPANYING DOCUMENTS.

Annotation: Integration of alarms from multiple devices is the final step for optimal alarm management. For example, in the 1980's, a number of patients have from crossed Oxygen and Nitrous Oxide gas lines. Although anesthesia machines of that day had multiple alarms, so did the pulse oximeters, the ECG and BP monitors, and other devices. In these mixed-gas-line incidents, the anesthesiologist could not rapidly determine which alarms were most important, leading to a patient death before effective steps could be taken.


Intelligent alarms are deployed in many industries, including aviation. This helps the pilots focus on the most urgent issues first, like an engine fire, before they tackle a myriad of other, less critical problems like a stuck landing gear or low fuel conditions.



As complex as this seems, there are many more Medical Device Alarm issues that we'll skip at this time...

- Alarm disable information (who, when, why...)
- Alarm settings information (too high/low, or off!)
- Patient-specific data that is needed in order to interpret alarm severity
- Systemic delay/synchronization issues
- Communication artifacts and failures
- Alarm symbol standardization
- etc...

Annotation: The participants must realize that this is the “tip” of the proverbial “iceberg.” There are many nuances in various facets of clinical care. One example: standards for clinical laboratory data – related to blood cell or chemistry analysis, for example – note that a single data point is useless unless it is supplied and preserved with its related calibration and/or methodology information. Different clinical laboratory devices and techniques yield similar, but not identical, values. Those disparate pieces of data must not be deleted, nor blindly grouped, trended, or charted, because inaccurate interpretation will likely result.



SUMMARY: Anesthesiologists
have wisely used these standards
to design safer “cockpits,,” and
we should to!

Intelligent alarm management will be
needed when medical device
interoperability is established...

These interoperable systems **MUST**
ensure that properly prioritized alarms
arrive intact and on time, and are
effectively displayed to the operator!

Annotation: The system must preserve the integrity and security every clinically-relevant piece of data and formatting of each alarm. Integrity – remains whole; Security – cannot be altered, lost, or stolen. Each device, and every component of the network, must be designed to accurately send, receive, interpret, and relay every facet of each possible alarm condition that any of the devices could generate.



Recap: Pressing issues of medical device inter-operability:

- Most manufacturers have not yet considered their device in the context of an integrated information system (as we're creating with IHE and EHRs)
- Life-critical alarms introduce life-critical data onto networks and systems of devices that may not be compatible or designed to the right level of quality.

Annotation: Historically, device manufacturers think of their devices as stand-alone instruments and when they provide a communication interface, they cannot foresee all the different ways in which it will be integrated into broader networks of devices and systems nor the myriad applications that will rely on timely and accurate information delivery. When life-critical alarms are added to the mix of information, the risk to patient safety resulting from communication issues becomes even greater. As standards-based device communication is realized, all stakeholders including both manufacturers and care providers (CEs and HIT personnel) must understand the broader issues that result from deploying applications that rely on networks of medical devices.




Bottom line: WMDS are riskier than wired medical devices!

- Poor management of RF spectrum
- QoS wireless standards in HIT not broadly discussed / understood / used
- Device alarms not designed for handling in the broader HIT environment
- Alarm nomenclature is only now being standardized

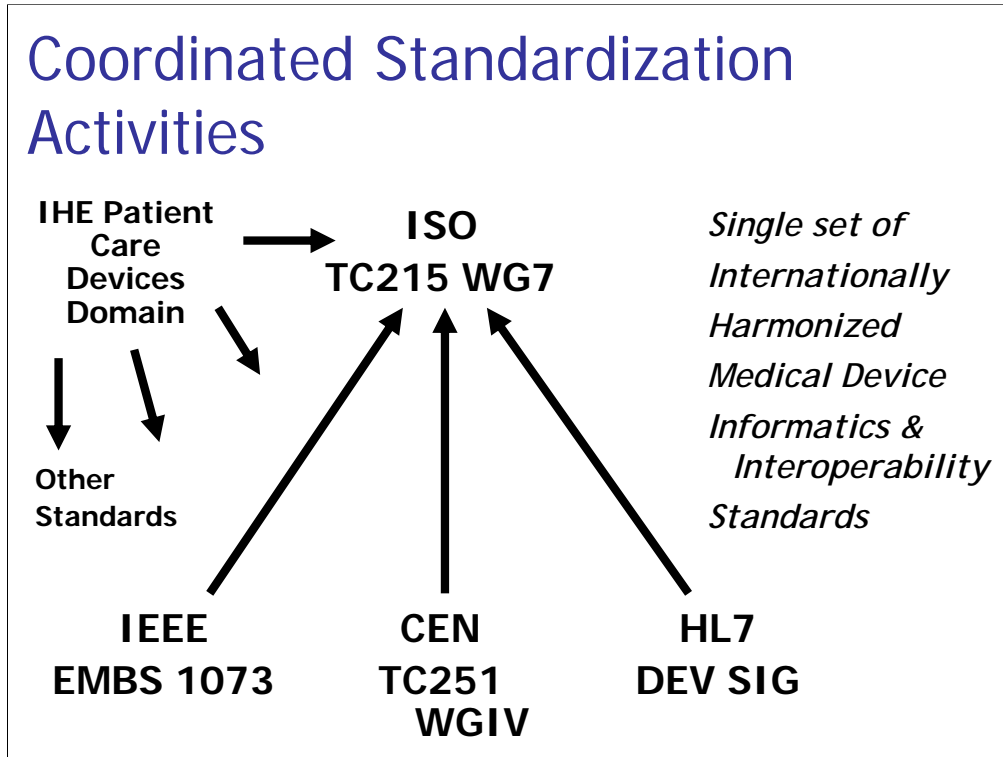
Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Prior systems were relatively fixed, i.e., the devices and any wired networks were limited to specific clinical areas, like the ER, ICU, OR, and Delivery Room. Modern medical devices are meant to be flexibly deployed throughout the hospital as generic assets, and they are increasingly use wireless communication to encourage mobilizing ever-more-sick patients to be as active as possible to speed recovery and discharge. Wireless medical devices also allow hospitals more elastic use of beds and space, to match varying patient needs. Furthermore, more and more patient care is occurring at home or free-standing clinics, and wireless medical devices encourage patient mobility, recuperation, and satisfaction while ensuring an “umbilical cord” to the hospital when or if needed.




Any questions so far?

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006



Annotation: These organizations are working in close coordination to establish a harmonized set of standards that provide for real-time plug-and-play interoperability of medical devices in heterogeneous environments, supporting connections from the physical layer (including wireless) to the abstract semantics, terminology, data model and data sets. This level of international coordination for medical device informatics standardization, addressing both point-of-care integration as well as enterprise integration, supports the international medical device marketplace. The IHE PCD domain group is developing integration frameworks, targeting specific clinical applications and frameworks that leverage standards from ISO/IEEE/CEN/HL7 as well as others. In the area of RF wireless technology, there is an international issue of spectrum allocation – available spectrum differs from country to country; however, management of the medical use of wireless technology is mostly the same.



RF (EMC/EMI) Wireless Guidance

- FDA Guidance:
www.fda.gov/cdrh/emc/emcresources.html
- AAMI TIR 18 & C63.18 (www.AAMI.org)
- ISO TR 21730
“Use of mobile wireless communication and computing technology in healthcare facilities — Recommendations for electromagnetic compatibility with medical devices”

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: For EMC and EMI management, there are a number of good resources available, both for vendors and provider organizations. The FDA CDRH EMC web page provides both guidance (<http://www.fda.gov/cdrh/emc/emc-in-hcf.html>) as well as a wealth of links to other documents and organizations. The AAMI Technical Information Report (TIR) #18 ***Guidance on EMC of Medical Devices for Clinical / Biomedical Engineers*** provides comprehensive EMC guidance for healthcare facilities. ANSI C63.18-1997 “***Recommended practice for an on-site, ad hoc test method for estimating radiated electromagnetic immunity of medical devices to specific radio-frequency transmitters***” provides guidance for how to conduct EMC assessments. The ISO document Technical Report 21730 provides more up-to-date (published 2004/2005) guidance for mobile wireless technologies. There are also many 3rd party companies and technology suppliers who provide testing and “site survey” services; however, the key issue of RF wireless technology coexistence – the ability of multiple wireless technologies to work without impacting the QoS of each other – is not well understood or managed, nor is the understanding of how well systems scale – at what point do things “break” as additional devices and I.T. systems are added which utilize the same shared infrastructure?

IEEE EMBS

1073 RF Wireless Group

IEEE P1073.0.1.1 Guidelines for the use of RF wireless technology...

- Beyond basic EMC/EMI testing...
- Provide general recommendations for how to design in, deploy, and manage medical devices with RF wireless interfaces
- Participants include leading device and technology vendors, care providers, and regulatory stakeholders

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: The IEEE 1073.0.1.1 “**Health informatics – Point-of-care medical device communication – Technical report – Guidelines for the use of RF wireless technology**” project seeks to provide guidance for how both vendors and end users can understand and manage the complex issues related to the use of RF wireless communication technologies. Though the guide is initially focused on the U.S., since spectrum allocation is independently regulated by each country, an international version is planned (ISO/IEEE 11073-00101). A group of leading vendors (both medical device and system vendors as well as wireless technology OEM’s), along with provider and regulatory stakeholders, has been meeting weekly to develop this set of guidelines, which looks at the broader issues of coexistence, QoS management, risk management, security, etc. Now that the guidelines are in the balloting stage, a number of follow-on standards projects have been initiated based on the needs identified in this document.

IEEE EMBS

1073 RF Wireless Group

Guidelines chapters include...

- Wireless medical device use cases
- Technology overview & analysis / constraints
- Device data characterization
- QoS Requirements
- Wireless service models
- Risk Management & Security
- Interference & Coexistence
- Conformance & Interoperability

Annotation: The IEEE 1073.0.1.1 RF wireless guidelines document contains chapters with the information identified above. As can be seen, the document goes far beyond EMC/EMI evaluation to include many of the issues that directly affect patient safety and system efficacy, providing the tools needed to evaluate prospective technologies, understand the risks involved, and manage the use of RF wireless technologies for medical device communication. The Use Cases chapter discusses various ways in which RF wireless technology is being used, providing numerous topological models that demonstrate the complexities that may be involved. Device data characterization and QoS Requirements provide general QoS characterizations for different classes of device data, supporting modeling of needed bandwidth, latency, priority, etc., as well as scaling networks from a few devices to 100's. The wireless service model chapter presents the different layers of standards and technologies that need to be integrated in order to implement and manage wireless medical device networks. A template risk management framework is provided to help both manufacturers and end users analyze and manage risks associated with these networks. Though conformance is discussed, the document provides guidelines and not normative standards – direction is provided for follow-on standards projects as discussed in subsequent slides.



Medical Device Data Classification

- Alarms
- Waves (real-time & near RT)
- Parameters (real-time and non-RT)
- Charting (params & wave snippet)
- Control and status
- History & archival / log
- Etc...

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: In order to understand QoS requirements, the class of device data must first be characterized. Each of the classes above represent different types of data each of which carries its own unique set of QoS requirements. Some of these data are communicated in continuous, periodic type streams, while others (such as “charting” oriented) are more intermittent, aperiodic transmissions. Before QoS requirements, system modeling and fault analysis can be performed, the data requirements from each device must first be understood and characterized.




Medical Device QoS Parameters

- Reliability (toleration of dropped bits)
- Latency (max allowable)
- Priority
- Bandwidth:
 - Bits per second
 - Continuous vs. intermittent / burst

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Each class of data is evaluated based on these QoS parameters. Especially in wireless environments, reliability becomes a major issue. When remotely viewing wireless waveform streams, how many bits may be dropped and at what periodicity before it affects its utility to make medical decisions? Latency typically ranges from a few hundred milliseconds or seconds (e.g., remote annunciation of critical patient alarms) to minutes (periodic updates of device control status). QoS requirements must address both clinical and regulatory concerns. Especially with regard to alarm annunciation, there are regulatory requirements stating the number of allowable seconds – and this typically does not take into account traffic in a wireless LAN!



QoS Characterization

Data Type	Bandwidth	Priority	Reliability	Latency
Alerts	Lo (64B/Al.), Intermittent	Highest	Hi	3 sec
RT-Waves	Hi (120 to 4KB/s/chan) Continuous	High	Hi	<RT> or CS=3 sec
RT-Param's	Lo-Med, Continuous	High	Hi	3 sec
Non-RT Param's	Lo (20B/p), Intermittent	High	Hi	---
Non-RT Events	Lo-Med, Intermittent	Medium	Hi	PoC: 3 sec CS: 5 sec
Controls	Low, Intermittent	Medium	Hi	PoC: 3 sec CS: 5 sec
History / Archive	Hi, Bursty, Intermittent	Low	Med->Hi	Push: >5 sec; Pull: < 5 sec
Web Browsing	Hi, Bursty, Intermittent	Low	Med->Hi	3-5 sec

Annotation: CS = Central Station; PoC = Point-of-Care This table indicates the mapping between device data classification and QoS requirements. With these, you can begin to analyze both the appropriateness of different wireless technologies, as well as assess the overall QoS requirements as you scale to large numbers of nodes and devices within an area.



Current IEEE RF Wireless Projects

- 20103 – *Application profile - Clinical context management (CCoM)*
- 30400 – *Inter-LAN (vLAN, IP, medical session, QoS, security, UDP, TCP, multicast discovery, addressing characters)*
- 30500 – *RF wireless – Framework & Overview*
- 30503 – *RF wireless – Local area network (wLAN)*
- 30505 – *RF wireless – Wide area (mobile phone) network (wWAN)*

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: This slide shows the most important and current IEEE medical device RF wireless related standardization projects. All hospitals and manufacturers will be affected, and should ensure qualified representation in the standards development and early adoption of approved standards as they are released. The CCoM project addresses maintaining a connection context while a patient is ambulatory, going throughout a facility where different wireless architectures from various vendors may be employed. The Inter-LAN standard addresses many of the basic LAN-oriented issues when networking medical devices and that need to be leveraged when working with wireless (as well as wired) networks.




Proposed IEEE Projects

- 20401 – Network directory service (find & bind)
- 20402 – QoS [transport independent]
- 20403 – Location services (patient, equipment, ...)
- 20404 – ID Services (RFID, patient, supply chain mgmt, ...)
- 20500 – Security F&O (PnP Security profile)
- 305xx – wPAN (Bluetooth / 802.15.1 based)
- 305xx – Mesh Networks (802.15.5?)
- 305xx – 802.15.3a (UWB)
- 305xx – 802.15.4 (Zigbee) addressed as it emerges in healthcare

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Though these projects have yet to be pursued, it indicates the state of where the industry is headed. Note that projects are initiated when there are a sufficient number of stakeholders willing to work on them. Some of these are very close to being activated; whereas, others are simply placeholders if / when they are needed. If your organization is looking at integrating systems using these technologies, then caution should be used to evaluate interoperability, conformance, risk management, etc. For example, though there are many different security technologies available in the market place today, there is no One technology that has been standardized for use in the medical device industry, and therefore, if one scheme is mandated for Vendor A's equipment, there is a very good chance that a different approach (and equally valid) will be required for Vendor B.




Quick Legal Perspective

- HIPAA Regulations require CIA!
 - Confidentiality
 - Integrity (of the patient data)
 - Availability (of the information)
- FDA requires that all medical devices comply with a large battery of safety, performance, and management processes.

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Providing a regulated medical device into the health care marketplace requires not only sound engineering and rigorous testing, but also navigation of many legal requirements, which can be summed up as ensuring safe, effective and secure devices and systems. The use of wireless equipment not only carries the legal / regulatory weight of its wired equivalents, but also has to address the unique challenges of wireless connections.




WMDS Threats for HIPAA - 1

- Confidentiality examples
 - Bluetooth (IEEE 802.15x) can be readily “hacked”
 - Emerging “Wi-Max” (IEEE 802.11n) devices can provide 30-mile access
 - Plus, all other lower-power wireless devices can be detected from miles away with simple antenna and receiver systems.

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: These security issues must be understood when evaluating the risk of their usage, and as can be seen in these examples, the problem isn't limited to the point of care. One of the “benefits” of wireless technology is patient mobility, and sometimes that includes metropolitan and wide area networks ... REALLY wide area!




Threats for HIPAA - 2

- Integrity
 - If a wireless link loses alarms or distorts a medical device display, data value, or clinician annotation, integrity has been lost.
- Availability
 - Most wireless links can “collide” with each other or with building structures. This can cause lost clinical data and/or block clinician access at a crucial time.

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation:

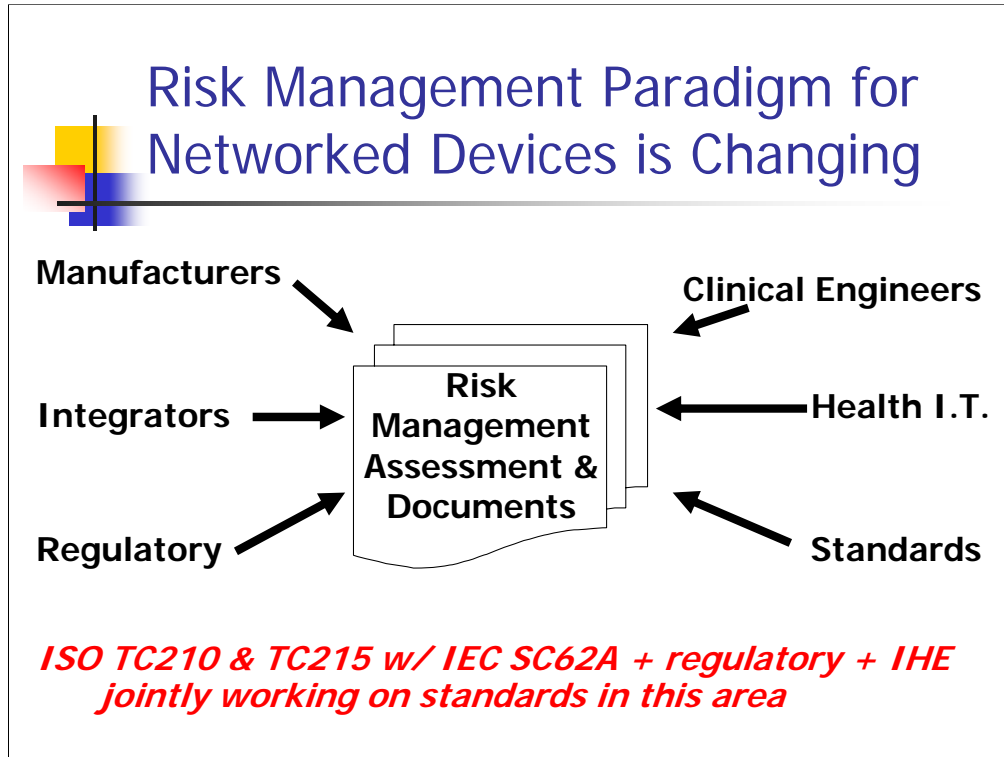


FDA Regulatory threats

- Medical devices are, by law, designed and manufactured “in compliance.”
- Integrated WMDS systems – and system components – may be considered as “adulterating” one or more products if they cause an injury or death.

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation:



Annotation: The traditional risk management approach put the vast majority of the responsibility on the shoulders of equipment manufacturers; however, with an ever increasing number of networkable medical devices, especially devices that employ RF technology, manufacturers can only mitigate the risks known at design time. Residual risks, though, must be understood and managed by other stakeholders. Thus the risk management paradigm is shifting away from manufacturer-focused to a broader stakeholder focus where all involved must work together to achieve safe and effective operation of medical equipment. These risks include both degradation of system operation due to changes in QoS, as well as security issues resulting from network configurations.



Medical Device Interoperability Status?

**State of open standards-based medical
device connectivity?**

Nonexistent!

*Proprietary / semi-standard Interfaces + Partnerships =
Security & lower risk for vendors
Limitations & expense for providers & patients*

A business issue – not a lack of technology

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Given all this talk about standards-based medical device interoperability, what is the state of the industry? In general, there is NO standardization within the medical device industry with respect to the protocols and technologies that are used. Even if the same basic technology is employed (e.g., TCP/IP or 802.11G), the lack of semantic standardization, shared security and QoS services, and under analyzed residual risks result in systems that do not provide the level of needed patient safety and overall system performance, as well as holding back innovations in advancing the state of the art in health care delivery. The key message here is that we don't have a technology problem, but rather a deployment problem. Vendors have consistently said that they have no interest in supporting open standards-based interoperability when it isn't being demanded by provider organizations and they can ostensibly do much better in the marketplace using proprietary technologies and strategic business alliances.



Interoperability Technology Deployment Logjam

What has blocked implementation of medical device interoperability?

Incomplete standards ... but no longer the case!

*Uncoordinated & inconsistent demand from
providers and other user stakeholders*

Under-defined stakeholder value propositions

Resources - esp. of standardization efforts

Organizational & Personnel Changes

(Dr. Brailer) Infrastructure is a hard sell:

"Diffuse benefit ... concentrated cost"

Annotation: If standards-based device interfaces are so important, why have we yet to realize them in the marketplace? There are many reasons, some of which are listed here. The main message though, as was stated in the previous slide, is that none of these problems are technical in origin – they are all business related. That means to realize standards based interoperability in the healthcare marketplace, especially medical device interoperability, the business issues must be resolved... <next slide>



What is breaking up this Chicken & Egg Problem?

*Executive Order #13335 - Formation of the Office
of the National (HIT) Coordinator + NHIN creation
w/"The Community", HITSP, Cert. Commission, etc.*

*Reimbursement Incentives ... based on level of
interoperability technology used*

*Expansion of the HIT marketplace (estimated at
4X over 4 years)*

Creation of the IHE Patient Care Devices domain...

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: The creation of the Office of the National Coordinator for HIT and the U.S. government's focus to establish a National Health Information Network has had a major impact already in moving toward standards-based medical device informatics and interoperability. To put teeth into adoption and implementation of a NHIN and the associated standards profiles, care reimbursement incentives will be used to reward those who provide care with advanced levels of HIT. All of this will lead to an unprecedented increase in spending on technology, representing new market opportunities, not just dividing up the same old pie. As a result of the 2005 HIMSS CIO survey regarding areas that should be targeted for IHE, where device integration came in at a high priority for 2/3 of the respondents, ACCE joined with HIMSS to create a Patient Care Devices domain.



What is breaking up this Chicken & Egg Problem?

IHE Patient Care Devices domain...

- *Planning Committee drives use case-based requirements*
- *Technical Committee develops interoperability profiles*
- *Coordinated closely with other IHE domains, incl. ITI*
- *Providers and vendors coordinate to their mutual benefit*
- *Profiles integrating RF wireless- a key area of interest!*

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: The IHE PCD will bring together users/providers and vendors to create the technical interoperability profiles needed to deploy safe and effective wireless medical device systems. The PCD planning committee will focus on the definition of high value use cases that will provide the ROI needed to drive purchasing decisions. The PCD technical committee will take the requirements identified in the PC's use cases to define technical interoperability profiles based on existing standards. Subsequent profiling and "connectathon" activities will ensure that the profiles and participating companies have met the stated needs, and in a way that provider organizations can call out the technical profiles in their RFPs. Profiles under consideration include those that leverage the use case work that was done in the IEEE 1073 RF Wireless group, providing us with a ready opportunity to validate and demonstrate wireless systems that implement the guidelines recommendations.



Future directions...


What advances will be occurring along with wireless system integration?

- *Intelligent integration of standardized alarm management and “smart alarm” detection*
- *Seamless integration of device data into EHRs, including for mobile and chronic patients*
- *Automated, real-time decision support systems*

...

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Just in the alarms area, there will be rapid movement towards much more intelligent integration of alarms. Also, ONC and many other agencies within other governments around the world are rapidly closing the gap on electronic health records (EHR) – The Community (AHIC) “breakthrough #3. Those EHR systems will depend on accurate and complete collection and retention of all medical device data, or the benefits of such a system will remain illusory. Finally, we are moving towards automated decision support systems that will advise clinicians of “best actions” based on available data, and, eventually, perhaps to automated/robotic/closed-loop interventional systems. Loss, distortion, or delay of critical data – including alarms – could be tragic.



Putting this all to work:

- Plan on using IHE-oriented procurement documentation (RFP's, et al.)
 - Those will be emerging in 2006
- Task CE and IT leadership to become fully aware of – and able to properly support – the appropriate technical standards.
- Develop and enforce installation WMDS verification testing BEFORE you pay!
- Develop and enforce ongoing verification testing after repairs, reconfiguration, and upgrades.

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation:




Critical Success Factors for Safe Wireless Medical Device Systems:

1. Know the clinical and device needs and constraints
2. Understand the applicable technologies and limitations
3. Apply the appropriate standards properly
4. Keep an eye on the legal implications
5. *Use IHE profiles and appropriate standards in your purchasing specifications, incoming inspections, and ongoing system testing and maintenance.*

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation:



Conclusion...

- WMDS and medical device inter-operability represents a huge opportunity for drastically improving the efficacy, efficiency, and safety of healthcare in the 21st Century, but there is no free lunch!
 - Assign ownership and responsibility
 - Know and apply standards
 - Document processes and outcomes

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

[Conclusions Slide]

SAFE AND SUCCESSFUL MEDICAL DEVICE SYSTEMS?

Understand the breadth of the issues ... don't focus on single system solutions

Designate and empower a wireless spectrum & technology tsar

Specify and demand **full** standards-based interoperability in purchasing decisions

Follow the guidelines provided by groups such as the FDA and IEEE 1073 RF

Actively participate in RF wireless standards and profiling groups – IHE PCD!

Annotation: [To successfully and safely support wireless medical device systems, you must (a) Understand the breadth of the issue; (b) providers must designate and empower a wireless spectrum & technology czar; (c) providers must demand interoperable systems in their purchasing decisions; (d) all should participate in the current standardization and profiling activities, including those of the ISO/IEEE EMBS 1073 RF Wireless group and the IHE Patient Care Devices domain.]




What we covered!

- Critical safety feature needs
- Wireless technology review
- Technical and legal requirements
- Applicable Standards
- Critical success factors
 - Successful Specification, Procurement, Installation, and Management

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: Because wireless medical device networks are rapidly approaching the "ubiquitous" stage, they will require appropriate system specification, procurement, installation, and management. To do so requires applying appropriate standards and best practices to ensure safe, reliable, and affordable systems. Recognize the critical safety features that must be assured for any medical device network, including Quality of Service (QoS) and life-critical patient alarm integration. Identify the current and emerging wireless technologies that should be considered - and/or avoided - and list the critical limitations of each. Name and explain the appropriate AAMI, ANSI, IEEE, IEC, ISO, and HIMSS/IHE standards that must be considered for wireless medical device systems. List and define the key legal and technical requirements to ensure a secure wireless medical device network. Describe the critical success factors to ensure specification, procurement, installation, and management of safe, reliable, and affordable medical device systems




Information Sources

- www.ACCEnet.org and www.ACCEnet.org/IHE
- www.HIMSS.org/IHE
- www.RSNA.org/IHE
- www.ACC.org/IHE
- www.IEEE1073.org

Safety First! Safe and Successful Wireless Medical Device Systems
Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006

Annotation: It is critical to become engaged in the standardization and standard implementation activities, especially for medical device networks that incorporate wireless technologies. These organizations and web sites provide a wealth of information about the activities that were mentioned in this presentation. The only way, as a vendor or provider, that your interests and concerns will be addressed by these groups is if you show up, provide input, and actively support their efforts! From this list, it is clear that the authors see the IHE Patient Care Devices activity as the best forum for the industry to address these wireless connectivity concerns.



**Thank you for your
attention and participation!**

Please join us in solving these challenges, too.

Elliot B. Sloane, Ph.D.

Villanova University
ebsloane@ieee.org

www.homepage.villanova.edu/ebsloane

Todd Cooper

Breakthrough Solutions
t.cooper@ieee.org

www.ACCEnet.org/IHE

Safety First! Safe and Successful Wireless Medical Device Systems

Elliot Sloane and Todd Cooper – HIMSS 2006 – San Diego, CA – Feb. 2006