AAMI
Advancing Safety in Medical Technology

Healthcare Technology In a Wireless World

Priority Issues from the 2012 Wireless Workshop Convened by AAMI, ACCE, ASHE, and ECRI Institute

Wireless Workshop Conveners

AAMI

The Association for the Advancement of Medical Instrumentation (AAMI), a nonprofit organization founded in 1967, is a diverse alliance of nearly 7,000 members from around the world united by one critical mission—supporting the healthcare community in the development, management, and use of safe and effective medical technology.

AAMI serves as a convener of diverse groups of committed professionals with one common goal—improving patient outcomes. AAMI also produces expert and objective information on medical technology and related processes and issues. AAMI is not an advocacy organization and prides itself on the objectivity of its work.

American College of Clinical Engineering

ACCE is committed to enhancing the profession of clinical engineering. With members in the United States and abroad, the ACCE is the only internationally recognized professional society for clinical engineers. Visit **www.accenet.org.**

American Society for Healthcare Engineering

With more than 11,000 members, ASHE is the largest association devoted to optimizing the healthcare physical environment. As a trusted industry resource, ASHE is committed to its members, the facilities they build and maintain, and the patients they serve. Visit **www.ashe.org/.**

ECRI Institute

ECRI Institute is an independent nonprofit organization that researches the best approaches to improving the safety, quality, and cost-effectiveness of patient care. Visit **www.ecri.org.**

Published by

Association for the Advancement of Medical Instrumentation
4301 N. Fairfax Dr., Suite 301
Arlington, VA 22203-1633
www.aami.org

Healthcare Technology In a Wireless World

PRIORITY ISSUES FROM THE 2012 WORKSHOP CONVENED BY AAMI, ACCE, ASHE, AND ECRI INSTITUTE

Contents

A Call to Action

Dear Colleagues,

While we didn't start 2012 knowing we would be bringing together 75 experts to address wireless challenges in healthcare, we're glad we took the bait when three amazing AAMI members asked us to convene this invitation-only event. We all owe this dedicated, enthusiastic group a big thank you for their commitment to tackle the persistent and growing problem to improve the current state of healthcare technology in a wireless world.

Their gift to the entire healthcare community was to spend October 4–5 developing a list of the highest priority issues that need to be addressed to solve wireless problems, and to come up with solutions that a wider group of experts in the healthcare community can and hopefully will begin to address. In the process, they came up with a useful list of the top 10 most common wireless mistakes.

Our gift to the healthcare community was to capture their work in this post-workshop publication. We have also committed to convening a task force to refine and address some of the priority solutions.

What do we hope you will do with this publication?
1. Learn from it and apply its lessons to improve patient safety.
2. Share it with colleagues.
3. Nudge the "responsible organizations" that you know to pick up the tasks they can tackle.
4. Tell us your success stories and lessons learned.

Many thanks to the American College of Clinical Engineering (ACCE), American Society for Healthcare Engineering (ASHE), and ERCI Institute for co-convening this unique workshop with us. Many thanks as well to Don Witters at the FDA and Elliot Sloane of the Center for Healthcare Information Research and Policy for starting these conversations several years ago and for inspiring this expert community to keep at it. I would be remiss if I also didn't thank Rick Hampton (Partners HealthCare), Phil Raymond (Philips Healthcare), and Steve Baker (Welch Allyn) for the nudge.

As noted in a recent Institute of Medicine (IOM) report, learning is a continuous process. This workshop was a big step forward in capturing what and why we need to learn about wireless. The projects that we hope it inspires will result in even deeper and broader continuous learning. In five years, it will be fun to see the progress in our growth together.

Sincerely,

Mary Logan
AAMI President

Executive Summary

"Given the explosion of wireless devices, regulated and unregulated, no doubt we have a tsunami ahead of us. How do we manage the wireless infrastructure?"

— Elliot Sloane, president, Center for Healthcare Information Research and Policy

Seventy-five experts converged in Herndon, VA, in October 2012 for an invitation-only AAMI Wireless Workshop to lay out the risks, challenges, and opportunities of wireless technology in healthcare.

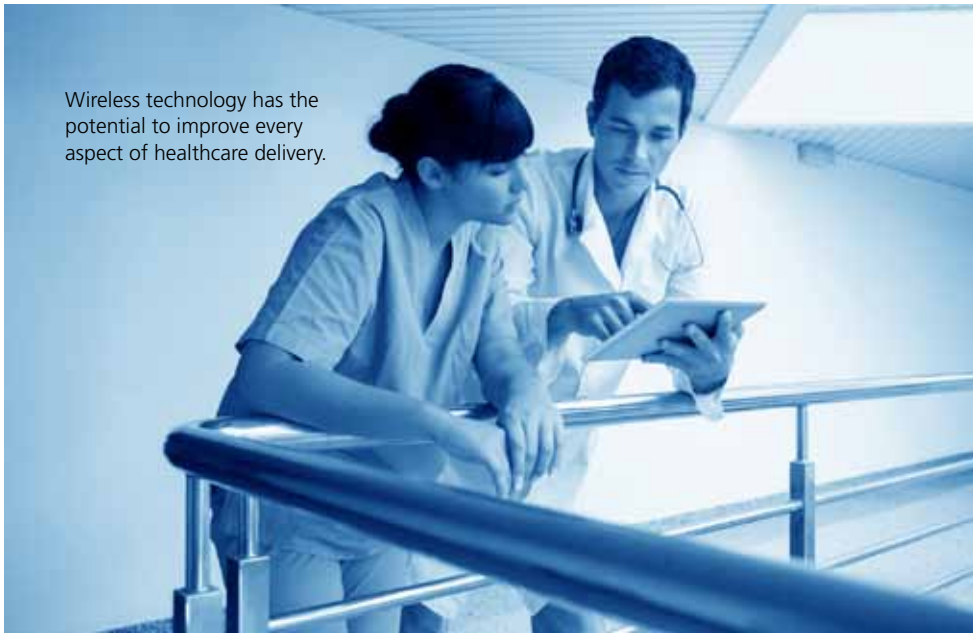
These experts are an elite, tight-knit group. Despite the rapid influx of wireless medical technology into hospitals, distributed care facilities, and home healthcare, expertise in this domain is still very much a niche specialty. The wireless experts of healthcare are limited in number. So they rely on one another to patch together solutions to the myriad challenges they are encountering as wireless connectivity goes mainstream.

At the workshop, however, the experts made clear that they have reached a tipping point when it comes to managing wireless technology on their own. The scope of the challenges goes beyond their organizations and authority. It spans the realms of patient safety, institutional leadership, regulations, standards, risk management, the security of technology and data, the reliability of the wireless infrastructure, and the capacity of the wireless spectrum.

Addressing the challenges requires engaging a broader group of stakeholders, including C-Suite executives and clinicians in healthcare delivery organizations; systems safety experts; manufacturers; standards-setting organizations; regulatory bodies; and professional groups. And the solutions must include home healthcare experts, since home use is a fast-growing segment of the wireless medical device market.

Workshop participants know the specific challenges they are facing. They spent two days prioritizing the challenges, which AAMI synthesized into five unifying themes:

1. Clarify roles and responsibilities.
2. Manage the spectrum to improve safety and security.
3. Design the wireless infrastructure for high reliability.
4. Learn from other industries.
5. Manage risk and prevent failure: Patient safety comes first.



Wireless technology has the potential to improve every aspect of healthcare delivery.

Participants in this workshop are among the biggest champions of the opportunities that wireless technology offers to healthcare. Clinicians and patients can benefit from wireless medical equipment that is used to monitor, diagnose, treat, and record patient conditions. Wireless technology can support every aspect of healthcare delivery and administration by providing easy, ubiquitous access, transmission, and use of information.

But the full potential of wireless technology will be realized only if it is managed safely and effectively. If not, workshop participants warn, it could cause patient harm—a growing possibility, given the increasing number of wireless devices, networks, systems, and critical applications that use wireless technology in healthcare.

There is a silver lining in this warning: The wireless experts at the workshop offered many specific, ready-to-go solutions to the challenges. By working together on the priority actions they identified, all stakeholders can help to ensure the safety, security, and effectiveness of wireless technology in healthcare.

About This Report

This publication reports on the unifying themes and priority actions developed by consensus at the workshop. It also highlights solutions identified for making progress, and recommends organizations that could take the lead on specific solutions. The report summarizes workshop presentations and provides additional perspectives from experts. The views expressed by these individuals do not necessarily represent the views of their organizations. They also have not been endorsed by AAMI or the workshop conveners.

More Workshop Information on AAMI Website

The workshop agenda, PowerPoint® presentations of speakers, reference materials, and updates are posted on the AAMI website.

www.aami.org/wireless

AAMI/FDA Interoperability Summit

In the two days preceding the workshop, AAMI and the FDA convened a summit on interoperability of medical devices. Some of the issues raised at the summit pertain to wireless challenges as well. The summit report, *Medical Device Interoperability: A Safer Path Forward,* and related information are posted on the AAMI website.

www.aami.org/interoperability

Top 10 Mistakes in Implementing Wireless Technology in Healthcare

Workshop participants identified these 10 common mistakes that healthcare delivery organizations make when they move to wireless technology:

1. **Underestimation of the potential risk to patient safety**

2. **Lack of planning**
   - **Inadequate testing**
   - **Too little time for verification**
   - **Unrealistic and/or incomplete budgeting and schedule**
   - **Lack of foresight about the pace of change and the need to plan for it**
   - **Failure to hire sufficiently trained professionals to support and maintain wireless technology**

3. **Decision making with false assumptions**
   - **"Shiny object syndrome"—assuming the desire for a new product trumps the need to design a system to support it**
   - **"Believing the hype"—assuming vendors have the healthcare organization's best interests in mind**
   - **Failure to consider electronic medical records (EMRs), personal health devices, and consumer mobile devices, such as smartphones and tablets, as "medical devices"**
   - **Failure to read manuals**

4. **Purchasing end-point wireless devices before realizing the limitations of the current infrastructure**

5. **Failure to design with a safety margin**

6. **Failure to properly manage changes made to the wireless network, such as failure to analyze and verify the impact of a firmware change to an access point on the medical devices on that network, or failure to properly analyze and test the impact of adding new applications to the network**

7. **Failure to embrace vendor site testing of the network**

8. **Failure to take into account different environments of care, intended uses, and intended use environments**

9. **Failure to perform routine maintenance**

10. **Failure to consider that construction projects, or physical changes to a facility, could impact wireless performance**

How We Got Here

"I do not think that the wireless waves I have discovered will have any practical application."
— Heinrich Hertz, German physicist

The Explosion of Wireless Technology in Healthcare

With all due respect to Heinrich Hertz, who in the 19th century proved the existence of the electromagnetic waves that now carry the signals that animate wireless devices, the healthcare community has put his discovery to amazing practical uses.

As in many industry sectors, wireless technology is pervasive and ubiquitous in healthcare, according to workshop presenter Elliot Sloane, president of the Center for Healthcare Information Research and Policy. Given the popularity of smartphones, tablets, e-readers, and other mobile devices among consumers, that shouldn't come as a surprise. "Look at it from a human perspective," Sloane said. "We're addicted to data and information. It has become like the oxygen we breathe."

To fully appreciate the unifying themes, priority actions, and solutions articulated at the wireless workshop, it's worth noting the many environments, applications, and types of wireless technology in healthcare. Workshop participants generated these lists:

Wireless Technology Environments

- Hospitals
- Physician practices
- Freestanding clinics, surgical centers, and emergency rooms
- Skilled nursing facilities
- Rehabilitation hospitals
- Long-term care facilities
- Assisted living facilities
- Homes and home-care services
- Emergency and first-responder services

Wireless Technology Applications

- Patient telemetry monitoring
- Infusion pumps
- Inter- and intra-enterprise clinical, security, and public safety communications, such as two-way paging systems, nurse call paging, and wireless waveforms
- Critical pharmaceutical and medical/surgical supply management
- Electronic patient records—electronic medical records (EMRs), electronic health records (EHRs), and personal health records (PHRs)
- Radio-frequency identification (RFID) for asset (patient, product, or device) location, tracking, data capture, or data transformation, inventory management, and more
- Voice over Internet Protocol (VoIP)
- Access to medical reference materials and to health, medical, and analytic applications
- 3G and 4G connectivity for staff, patient, and visitor mobile devices

- E-mailing and texting between care providers
- Social networking and Internet-based research about healthcare
- Patient/family entertainment and hospitality services
- Outpatient care and followup
- Home healthcare
- Self-managed personal medical care, fitness, and wellness activities in the home, at work, and "on the go"
- And many more

The penetration of wireless technology into healthcare is fairly astonishing, given that it has been widely available for only a decade or so. More wireless technology is arriving daily, Sloane said, with applications such as:

- Machine to Machine (M2M) communication, which includes wireless device-to-device, device-to-system, and system-to-system communications. M2M began as proprietary, single-vendor solutions and is now rapidly staged for open-source, multi-vendor solutions.
- Robotic food, pharmacy, and supply delivery
- iPhone, iPad, and Android medical applications for physicians, nurses, and patients—with some now approved by the U.S. Food and Drug Administration (FDA) as medical devices

In a connected world, the number of wireless devices is "rabbitly increasing," puns workshop presenter Shawn Jackman, principal, manager, wireless product management and engineering at Kaiser Permanente. Among those in widespread use now:

Wireless Technology Devices

- Phones
- Vocera badge
- Other wireless voice devices
- Pagers
- Tablets
- Laptops
- Barcode scanners
- Carts/workstations (mobile and stationary)
- Biomedical devices—too many to list
- RFID tags
- Digital signage
- Patient entertainment systems
- Home health devices

Expert Perspective

At the AAMI/FDA Interoperability Summit that preceded the wireless workshop, presenter Rick Hampton, wireless communications manager for Partners HealthCare, focused on the impact of wireless technology on a leading healthcare system:

"We have several tens of thousands of devices on our wireless network concurrently, at a minimum, at 3 a.m. on a Saturday. On Wednesday at noon, that number quadruples. We're getting slammed on the wireless side."

What's Driving the Rapid Adoption of Wireless Technology in Healthcare?

A number of factors are contributing to the keen interest in wireless technology, Sloane said. The lines between medical devices, information technology (IT), and information systems (IS) are blurring.

Federal investments in EHRs are accelerating the adoption of wireless medical systems as well. The Medicare and Medicaid EHR Incentive Programs provide a financial incentive to eligible providers and hospitals, as well as critical access hospitals for achieving "meaningful use" of certified EHR technology. Meaningful use requires physicians, other clinical providers, physician practices, and hospitals to use computerized physician order entry (CPOE) and ePrescribing, regardless of their location.

Wireless devices can help healthcare providers meet federal requirements—and deliver high-quality, cost-effective patient care. Accountable care organizations (ACOs)—groups of doctors, hospitals, and other healthcare providers who coordinate care for Medicare patients—are "transforming to new paradigms of care, almost exclusively based on mobile devices," Sloane said. ACOs can score high with the Centers for Medicare and Medicaid Services (CMS) by using inexpensive mobile devices. "More than 33 percent of ACO metrics can be supported with available and emerging medical and personal health devices," Sloane added.

For example, portable wireless devices can help clinicians and patients monitor falls and such conditions as diabetes, coronary artery disease, congestive heart failure, and chronic obstructive pulmonary disease. Soon, wearable or implantable micro-scale devices (or MEMS, for micro-electrical-mechanical systems), voice-activated devices, and nano-sensors with radio frequency (RF) capabilities will be broadly used to detect or track diseases, injuries, and treatments.

Moreover, "the home care market is huge," Sloane explained. Acute-care medical devices began moving into home care more than a decade ago. In home environments, a wireless cell phone may be a patient's only link to caregivers.

The technical capabilities of wireless devices are only part of the story, however. "The social part of this is huge," Sloane said. "Digital nurses and physicians are using these devices to make decisions 24 hours a day. We have to figure out how to manage all of this fusion of data on patient conditions, patient records, and clinical decision making to create a 'cockpit of care.'"

Increasingly, a Bring Your Own Device (BYOD) model applies, whether explicitly sanctioned by healthcare organizations or not. Caregivers are using their own personal devices to support healthcare services, including medical device-like applications. Already, healthcare organizations are struggling with how to manage and control clinicians' personal devices used for medical applications.

In the foreseeable future, healthcare organizations will have to contend with a "Bring Your Own Medical Device" environment, said workshop presenter Ken Fuchs, senior principal architect, Mindray of North America. The time will soon come when patients will bring a wide assortment of wireless medical devices or apps into healthcare settings.

Healthcare organizations should be thinking and planning ahead for this. Indeed, in a 2012 survey commissioned by AAMI, 42 percent of healthcare technology management professionals already believe that "medical devices brought in by patients" is a top challenge.

"Healthcare technology professionals must effectively design, assess risk, and deploy wireless solutions, meeting intended use cases with the entire infrastructure in mind, to face the increasing wireless demands," said Brian Long, director of field systems operations, at Masimo.

The rapid and unrelenting growth of wireless technology in healthcare instills a sense of urgency in addressing the unifying themes and priority actions that follow.

Data Points

- **Forty-five percent of clinicians say they are using mobile technology to collect data at the patient bedside in 2012, up from 30 percent in 2011.**
- **Half of clinicians say they will be using more mobile medical apps in the next year.**
- **Three-quarters of organizations say they will be using more mobile devices, especially tablets, in the future.**

  — 2nd Annual HIMSS Mobile Technology Survey, 2012

- **Sixty-nine percent of nurses interviewed say that nursing staff use their personal smartphones on the job, particularly to fill "critical communication gaps" with hospital IT.**
- **Twenty-five percent of nurses say they are dissatisfied with the quality and reliability of the wireless network in their facilities.**

  — Point of Care Computing for Nursing 2012, Spyglass Consulting Group

Unifying Theme 1: Clarify roles and responsibilities.

"I'm sorry, Dave. I'm afraid I can't do that."
— HAL, *2001: A Space Odyssey*

Challenge	Priority Actions	Accountability
A void in leadership and direction for implementing wireless technology in hospital settings	Engage and educate the C-Suite (e.g., chief executive officers, chief information officers, chief medical officers, chief nursing officers) on their role in leading and directing the management of the wireless technology infrastructure.	ONC, CMS, The Joint Commission and other accrediting organizations, AAMI, CHIME, ECRI, ACHE, ASHE, other professional societies
	Showcase wireless technology solutions and best practices in hospitals, in a similar format as the HIMSS Health Information Exchange or HIMSS Interoperability Showcase™ at the HIMSS Annual Conference and Exhibition. Use webinars and videos as additional channels of communication and education.	CHIME, AAMI, ACCE, ECRI, HIMSS Other organizations: Bluetooth SIG, DECT Forum, FCC, FDA, Wi-Fi Alliance, ZigBee® Alliance, West Health, and others
	Promote cross-functional and cross-industry collaboration. Offer a workshop to address common wireless guidelines and architecture, grounded in best practices, for healthcare delivery organizations, medical device manufacturers, wireless infrastructure vendors, and EHR vendors.	AAMI, ACCE, ECRI, ASHE, CHIME, HIMSS Other organizations: FCC, FDA
A lack of accountability for managing wireless technology in hospital settings	Clarify who is responsible for managing wireless technology in hospital settings.	Healthcare delivery organizations (HDOs)
Uncertainty about who is responsible for managing wireless medical technology in distributed care environments	Clarify who is responsible for managing wireless technology in distributed care settings, including patient transport and homes.	All stakeholders

The Role of Leadership

Because wireless consumer devices are so pervasive and easy to use, the perception persists that wireless medical technology is equally easy to implement in healthcare.

But wireless medical technology can be mission-critical—and even life-critical. Consider the potential organizational impact of a few very realistic scenarios:

- If a personal smartphone or tablet loses wireless connectivity for a moment or two, it's at most inconvenient or irritating. If a wireless telemetry monitoring or infusion system loses service, patient care could be compromised, and lives could be lost. These are quality of care, patient safety, risk, and liability issues.
- If a wireless service interruption in a hospital results in incomplete or inaccurate data transfers to EHRs, hospitals could lose money on Medicare, Medicaid, or other insurance reimbursements. Or if a wireless infrastructure or network is not well-planned and configured to meet current and future clinical and administrative needs, it's an expensive proposition to reconfigure it. These are financial, facilities, standards, and technical issues.
- If wireless devices, networks, and systems are not protected, sensitive organizational data or confidential patient or clinical data could be compromised. These are regulatory, privacy, and security issues.

These are the types of issues that keep wireless technology managers awake at night. Clearly, the takeaway point is that wireless technology management goes beyond technical expertise. "Organizations deploying wireless medical solutions must have the appropriate, qualified personnel in place to manage this complex environment," explained Brian Long of Masimo.

Right now, many senior leaders in hospitals are largely hands-off in their dealings with wireless technology management, workshop participants believe. And there is no clear line of accountability. Ultimately, however, hospitals and their leaders could be on the hook for any failures—whether they know it or not.

Wireless experts are worried about dangers that might not even be on the leadership radar screen. "Hospitals and companies are using wireless technology in ways you can't imagine," warns Rick Hampton of Partners HealthCare. "Where is there an understanding of how hospitals are using technology? There is a disconnect between what the hospital thinks it's using and what it's actually using."

Workshop participants made it a priority to engage and educate the C-Suite about both the risks and opportunities of wireless technology in healthcare. They recommended outreach at specific forums and identified specific organizations that could take the lead or support this effort.

Expert Perspective: "Wireless for Wireless' Sake" Is Not a Good Strategy

Ken Fuchs
Senior principal architect, Mindray of North America

"Sometimes wireless is just not reliable enough to assure adequate patient safety, and a wired approach should be used. In general, wired should be used whenever it will meet the clinical needs. It does not make sense to have a wireless patient monitor if it will always be sitting at the same bedside. If it needs to be used for transport from time to time, then it should be wired while at rest and wireless on transport (when someone will probably be with the patient). Wireless for wireless' sake is not a good strategy for critical medical applications. This is an education issue for the healthcare delivery organizations."

Where Does the Buck Stop?

Within hospitals, C-Suite leaders have a role to play in delineating who is responsible for wireless healthcare technology management—and getting actively involved in directing and supervising this work, workshop participants said. Senior leaders have a clear understanding of institutional goals, environments, and cultures, which should inform the planning and implementation of wireless technology.

Wireless technology management requires more than one point person or even department. In fact, medical technology vendors and wireless service providers share some accountability for the performance of their products or services. Healthcare professionals with expertise in medical devices, networks, and systems; patient safety and risk management; clinical practices; and facilities should work collaboratively on the design, testing, hazard analysis, installation, monitoring, and maintenance of equipment.

Workshop participants also believe that The Joint Commission and other accrediting organizations should address the safety, security, and reliability of wireless technology in their accreditation and certification programs for healthcare organizations.

Questions about accountability extend to healthcare settings outside of hospitals. As more wireless technology is deployed outside of hospitals—in hospital-affiliated facilities and physician practices, by contracted service providers and independent care facilities, in patients' homes, and by patients on the go—who is responsible for ensuring robust wireless connectivity and wireless technology performance?

The answers to these questions are as yet unknown. The entire healthcare community will need to come together to address them. "We need a concerted effort to bring all parties together to understand the issues, create a road map for all parties, and arrive at a full range of solutions amicably," Hampton said.

The unifying themes that follow examine the most important issues for cross-functional, cross-industry collaboration in more detail.

Unifying Theme 2: Manage the spectrum to improve safety and security.

"Spectrum is the oxygen that your devices breathe. You need to manage it."
— Mark Gibson, senior director, Comsearch

Challenge	Priority Actions	Accountability
Balancing the finite radio spectrum with unlimited demand for wireless connectivity	Maximize spectrum allocation and efficiency for healthcare uses. Reserve some bands of the spectrum for healthcare. Minimize the potential for spectrum interference. Prioritize healthcare requirements for spectrum use from most to least critical. Manage the spectrum in collaboration with the healthcare community.	FCC NTIA FDA ONC HDOs
Lack of security of wireless devices, networks, and software	More actively enforce security of wireless technology as part of accreditation of healthcare organizations.	The Joint Commission and other accrediting organizations
	Develop reasonable approaches for dealing with security risks. Survey the healthcare industry and other industries to discover the guidance on cybersecurity that is already available. Create a flowchart or software tool to identify and enumerate all the questions and issues relevant to covering security risks. Hold off on security regulations until there is consensus on reasonable approaches.	HDOs Industry FDA NIST SDOs

The Limits of the Spectrum for Wireless Technology in Healthcare

Any efforts to manage wireless medical technology must be informed by an understanding that the radio frequency bands on the electromagnetic spectrum—the wireless waves that Heinrich Hertz discovered—are in high demand and limited supply.

The full frequency of the radio spectrum that can be used for wireless communication ranges from 3kHz to 300 GHz, as shown in Figure 1.

Within that frequency range, the radio spectrum is allocated for many uses and technologies, as shown in Figure 2. "You can see how complicated this has become," said workshop presenter Mark Gibson, senior director, Comsearch. "There is no place where the spectrum is not being used, except in the kilobyte range." In other words, the spectrum is crowded with users.

The wireless traffic jam comes into sharper relief in view of the even more precious spectrum resources that are allocated to

healthcare, as shown in Figure 3. The MedRadio (Medical Device Radiocommunications Service) band is allocated to implanted medical devices and devices worn on the body, which are used for diagnostic and therapeutic purposes. The WMTS (Wireless Medical Telemetry Service) band is used for remote patient monitoring.

In 2012, the Federal Communications Commission (FCC) set aside part of the spectrum for MBANs (Medical Body Area Networks), which will be used for wireless networks made of body-worn medical sensors that collect and transmit data from patients to telemetry systems and other systems, such as EMRs. MBANs will allow patients to be monitored whether they are stationary or ambulatory, without being tethered to wires and cables.

The FCC and the National Telecommunications and Information Administration (NTIA) regulate and coordinate spectrum allocation. "Regulation of the radio spectrum is becoming more and more important in the medical community," said workshop presenter Ira Keltz, deputy chief, Office of Engineering and Technology, at the FCC.

Spectrum management at the national level is a mix of engineering, law, economics, diplomacy (including international agreements), and public policy, Keltz said. Engineering expertise, for example, helps the FCC understand how much power devices need to operate and, thus, where on the spectrum they need to be. On the diplomacy side, the FCC works with international regulators to harmonize spectrum allocation. For medical uses of the spectrum, this ensures that people with implantable or wearable medical devices can travel with the assurance that their devices will work safely.

It's in the policy arena that hospitals, manufacturers, medical practitioners, other federal agencies (such as the FDA), and the general public can collaborate and advocate for spectrum management practices that benefit healthcare. Indeed, GE Healthcare and Philips Healthcare petitioned the FCC for the MBANs' spectrum allocation.

Keltz shared the FCC's spectrum management goals:

- Maximize the use of a limited resource for non-federal users by adopting rules

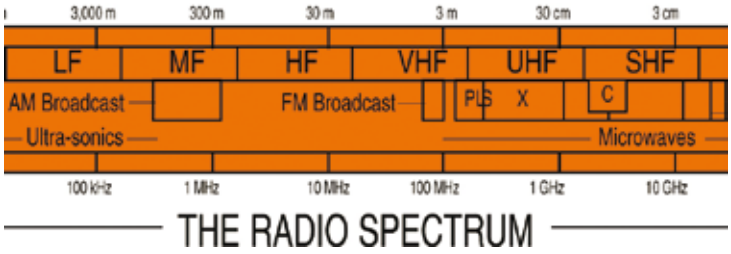
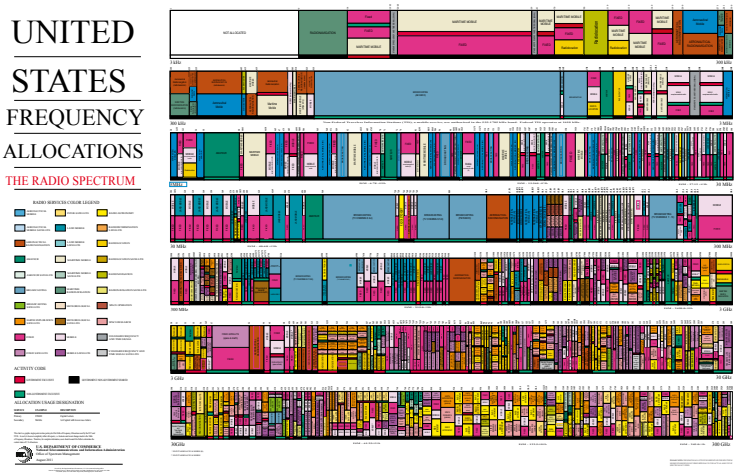


Figure 1. The Radio Spectrum

Source: http://ptolemy.eecs.berkeley.edu/eecs20/sidebars/radio/spectrum.gif



For a more detailed view of the image, click here.

Figure 2. How the Spectrum Is Allocated

Source: U.S. Department of Commerce, National Telecommunications and Information Administration, Office of Spectrum Management, August 2011. http://www.ntia.doc.gov/files/ntia/publications/spectrum_wall_chart_aug2011.pdf

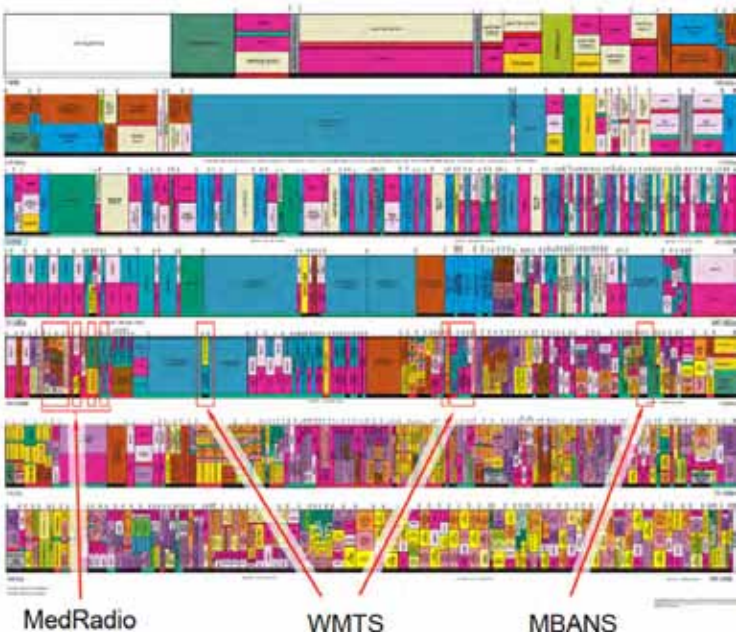


Figure 3. Spectrum Allocations for Healthcare

Source: U.S. Department of Commerce, National Telecommunications and Information Administration, Office of Spectrum Management, August 2011, and Comsearch. Source: Mark Gibson: Radio-Frequency Terminology and Challenges: Understanding the Concepts and Applicable Challenges to Wireless Connectivity," presentation at the AAMI Wireless Workshop, Oct. 4–5, 2012. http://www.ntia.doc.gov/files/ntia/publications/spectrum_wall_chart_aug2011.pdf

designed to allow radio users to operate with minimal interference from other users.
- Meet a mandate to manage spectrum in the "public interest, convenience, and necessity"—by finding the "highest" and "best" uses of radio spectrum for society, in terms of economic value, societal value (such as public safety), and research and development, among other considerations.
- Maximize spectrum to:
  – Maximize spectrum efficiency
  – Minimize potential for interference

An important implication for the healthcare community with spectrum management at the national level is that all not spectrum allocations are created equal. Spectrum allocation is licensed—but wireless devices using the spectrum for healthcare purposes typically are not:

- **Licensed spectrum** allows for exclusive, and sometimes non-exclusive, use of particular channels in particular locations and conveys interference rights—the right to commandeer use of the limited spectrum in case of emergency. Licensed spectrum for public safety conveys exclusive use for law enforcement agencies or first responders. Licensed spectrum is also allocated to commercial users, such as the cellular, broadcasting, satellite, aviation, and maritime industries.

"Ninety-three percent of the spectrum is shared among federal and non-federal uses."
— Ira Keltz, deputy chief, Office of Engineering and Technology, FCC

- **Unlicensed devices** can use the spectrum—with no rights to exclusive use and no interference rights. Devices must not cause harmful interference to the spectrum, and must accept interference from authorized services. In healthcare, many medical devices operate under these rules, such as assistive listening devices; implantable pacemakers, cardioverter defibrillators, and cardiac resynchronization therapy devices that use inductive coupling; enteromedics, or implantable devices to treat gastrointestinal disorders; and retinal prosthesis systems.
- **License by rule** is similar to unlicensed use of the spectrum, but it conveys some interference rights. In healthcare, MedRadio and WMTS are licensed by rule; MBANs will operate under this license as well. For WMTS and MBANs, there are some obligations that healthcare organizations register their use of the spectrum with a frequency coordination agency.

Notably, the FCC is considering offering experimental licenses to promote research and development of new radio technologies, devices, and applications. One type of proposed experimental license would provide "test beds" for medical institutions and manufacturers to test new devices over a wide variety of frequencies and other operating parameters under real-world conditions.

On this front, Elliot Sloane of the Center for Healthcare Information Research and Policy said, "We need testing and development 'sandboxes' so that everyone can learn together quickly."

Access to the Spectrum Does Not Convey Safety or Security

The crux of the spectrum limitations for healthcare is this: The FCC is not a medical safety agency. The agency regulates spectrum allocation through technical rules on transmitters. It tries to resolve interference issues—but "tracing interference can be very difficult," Keltz said. And its enforcement jurisdiction extends to illegal RF jamming devices, which intentionally cause interference.

The FCC does not regulate wireless medical technology or medical apps used on wireless devices. "The federal Communications Act gives us the authority to regulate transmitters, not receivers," Keltz said. "We don't set receiver standards. We rely on industry groups to come up with receiver standards and requirements for power, emissions, and bandwidth. This is becoming a bigger issue."

This issue surfaced with the MBANs spectrum allocation petition. "Experts ... worry that because the FCC didn't specify rules requiring interoperability in the bands set aside for MBANs, companies will not make their products compatible with one another—

a problem already apparent in the WMTS" (Hartford, 2012).* Wireless expert Rick Hampton of Partners HealthCare already sees that happening with incompatible wireless medical systems from different manufacturers that, when placed too close together in a hospital, interfere with one another.

"The challenge is that with more wireless devices, and a lot of congestion, how do we make everything compatible?" Keltz said. "You have to think about these things as you implement systems within facilities. You need people to understand the equipment they're buying, especially on the receiver side. Ask manufacturers, 'How well do the receivers filter out and discriminate for interference?'"

Managing the Wireless Spectrum

For these reasons, for healthcare delivery organizations and manufacturers, the spectrum is a critical asset that must be managed accordingly, Gibson noted.

"I've noticed over the years that hospitals have really embraced the concept of the FCC and spectrum management a lot more," Gibson said. "The key point about all of this is that, in most cases, the spectrum must be shared with other users. You should know who those other users are. You may have exclusive rights, but you'll be sharing the spectrum with someone. There is no spectrum that is allocated to a single source that you don't have to worry about."

The worry is interference—disruption of the operation of wireless device when it is in the vicinity of an electromagnetic field in the spectrum that is caused by another wireless device. "Interference will be a limiting factor in the success of wireless technologies," Gibson said.

Interference can compromise a wireless device, network, and software security and reliability. Healthcare organizations will have to deal with this interference through effective wireless planning, including taking stock of all of the wireless medical devices in their inventories and in personal use. An emerging technology, device databases, can help healthcare organizations manage all of these devices by dynamically locating vacant spectrum and switching them to available segments of the spectrum.

In the future, the FCC may unlock underutilized slivers of the broadcast TV spectrum, known as "white space," which could change the wireless mobile landscape with more secure technology. For example, one promising technology to watch is TD-LTE (Time Division-Long Term Evolution), according to Gibson. LTE is the fast, efficient technology that powers 4G networks; TD makes LTE even more efficient. Telecommunications companies around the world are experimenting with this technology.

Other ways of securing and managing wireless technology are addressed in the unifying themes that follow.

*__Hartford J.__ MBANs Could Advance Patient Care, But Interoperability Is a Concern. *Medical Device and Diagnostic Industry News*. Sept. 11, 2012.

Unifying Theme 3: Design the wireless infrastructure for high reliability.

"Design for performance more than anything. The faster and the healthier a device can get on and off the network, the better."
— Shawn Jackman, principal and manager, wireless product management and engineering, Kaiser Permanente

Challenge	Priority Action	Accountability
Lack of a robust wireless infrastructure compromises the reliability of wireless technology	Understand, define, and document the purpose, business requirements, and intended uses of wireless technology. Design, build, and test the infrastructure against these requirements and uses. Involve all critical stakeholders, including, at a minimum, senior leaders, clinicians, biomedical and IT professionals, and vendors.	HDOs Industry
Uneven use of best practices in designing, building, and testing wireless infrastructures	Identify best practices on wireless deployments and the effective co-existence of hardware and software.	Wi-Fi Alliance Industry All stakeholders
	Develop consensus around a reference wireless architecture, with consistent and explicit use of standards, for healthcare organizations and industry.	Industry SDOs
	Build test cases of the wireless infrastructure around intended uses focused on clinical workflows.	HDOs Industry SDOs
Different challenges to building a robust wireless infrastructure in different care settings	Consider the wireless infrastructure requirements and intended uses of wireless technology in distributed care settings, including patient transport and home healthcare. Include these environments in the exploration of best practices and development of test cases.	HDOs Industry SDOs

Overcoming "Shiny Object Syndrome"

Healthcare organizations can be blindsided when the allure of shiny (wireless) objects meets the reality of inadequately designed, built, and tested wireless infrastructures.

Workshop participants offered a veritable litany of common, infrastructure-related shortcomings in "Top 10 Mistakes in Implementing Wireless Technology in Healthcare" (page 5). The mistakes include lack of planning, poor decision making, premature purchases, inadequate testing, and failure to consider the patient safety risks, business requirements, infrastructure capacity, and intended uses by real people. Compromised reliability can result.

Workshop presenter Peter Thornycroft, engineer, office of the CTO at Aruba Networks, a Wi-Fi service provider, describes reliability as "delivering bits as fast as we can and as uninterrupted as we can" to enable mission-critical medical mobility.

The advice of personal finance guru Suze Orman—"People first, then money, then things"—is an apt analogy for designing a wireless infrastructure for high reliability. Aruba Networks frames its infrastructure focus in its registered trademark: "People move. Networks must follow."

The wired and wireless infrastructure is the foundation on which security, devices, applications, and users operate, as shown in Figure 4. The infrastructure enables people, processes, and technology to work more effectively. "All of them are constantly changing," Thornycroft said. "We have to give them the best possible performance within the parameters we're given. You want to get all the devices, users, and services to play well together at a predictable level—particularly at the high-priority level."

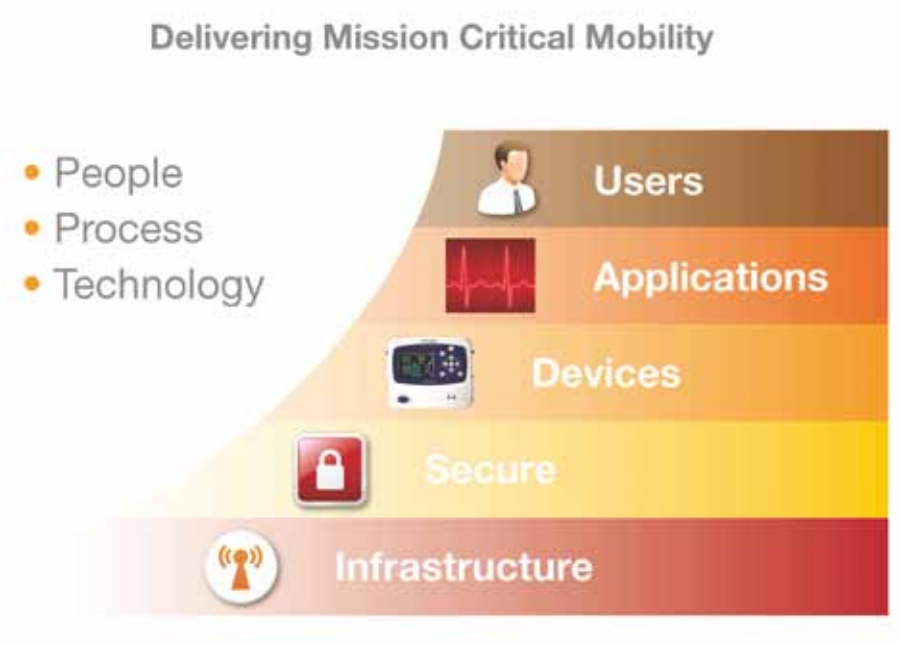


Figure 4. Delivering Mission Critical Mobility

© 2012 Aruba Networks. Source: Peter Thornycroft. "Enabling Mission Critical Medical Mobility," presented at the AAMI Wireless Workshop, Oct. 4–5, 2012.

Characteristics of a High-Reliability Infrastructure in a Healthcare Organization

- Strong leadership and accountability
  - Coordination among users and stakeholders
  - Use of 80001 to guide change management
- Clearly established business requirements
- Sufficient for intended use—tailored to each facility
- Managed and supervised by skilled personnel with knowledge of all wireless services
- Resourced adequately
- Built-in safety, using risk mitigation and risk avoidance strategies
- Secure, with protections from unauthorized access and for data
- Self-aware, self-monitoring, and self-protecting against intrusion
- Fully tested and verified
- Designed for quality of service—speed, availability, adequate coverage, and minimal latency (delays in processing data)
- Built-in redundancy to compensate for assumed failure and overload
- Support for legacy technology
- Easy to repair

Top Obstacles to Building a High-Reliability Infrastructure

- **Failure to catalogue all the requirements and intended uses of wireless devices that currently use, or will use, the infrastructure**
- **Failure to assess the existing infrastructure and its capabilities**
- **Failure to plan for BYOD (Bring Your Own Device) and BYOI (Bring Your Own Infrastructure) realities**
- **Lack of agility in anticipating and planning for change**
- **Failure to account for the true cost of implementation**
- **Lack of agreement on standards for safety**

To achieve this result, healthcare organizations must first define their current and anticipated expectations for wireless technology, with patient safety, effectiveness, and reliability as top-of-mind concerns. They need to develop a plan that supports all of the people, processes, and technology that will rely on the infrastructure. This is more than a technical exercise; it requires multidisciplinary expertise and leadership involvement.

To support organizational planning, workshop participants generated a list of the key characteristics of a high-reliability infrastructure—and the top obstacles to building such an infrastructure, detailed in the sidebar.

Given the enormous amount of mission-critical wireless technology, healthcare has unique infrastructure requirements, Thornycroft said. "We're talking about access points in every third room, every 15 meters—we're already getting into something fairly unique in hospitals." In addition, workshop participants believe this uniqueness extends to the wireless infrastructure for distributed care environments, which at this point are even less well planned than hospital infrastructures.

A robust wireless infrastructure builds in checks and balances for reliability. For example, Thornycroft said, it monitors who is on the network and which devices they are using, with different authentication and encryption levels to access data and applications for different authorized uses. The infrastructure also monitors traffic on the network, analyzes how the spectrum allocation is being used, and prioritizes mission-critical access.

Lead User Profile

Kaiser Permanente

The Goldilocks Challenge

Kaiser Permanente offers Wi-Fi connectivity for guest access at nearly 150 sites, with plans to provide this connectivity to 800 sites. Guest access is important to Kaiser in providing patients and families with positive healthcare experiences. Right now, some 25,000 users are on the network at any one time, at an aggregate bandwidth usage of 150 Mbps.

Future plans include offering a "digital health strategy," with member-facing services that allow auto sign-on for Kaiser Permanente members; mapping and "wayfinding" on member smartphones with a Kaiser Permanente app; and notifying personnel about prescriptions, lab results, and more. These plans may be augmented and leveraged as a Bring Your Own Device/Network Access Control (BYOD/NAC) remediation VLAN (virtual local area network). This solution has the potential to serve as an onboarding mechanism for new devices, such as employee devices, using a downloaded, automated configuration package.

Managing this infrastructure requires choosing just the right infrastructure technology, vendor, and design methodology to support current and future plans. It's what Kaiser's Shawn Jackman calls "the Goldilocks challenge." To get the mix just right, Kaiser attends to these Wi-Fi design considerations:

Wi-Fi Design Considerations

- Plan for voice and video
- Use a real-time locating system (RTLS) to identify and track the location, status, and movement of devices and people for general positioning, with an infrastructure of location sensors (overlay) needed
- High availability
- Consider 3D RF propagation
- Don't rely on automated RF configuration features
- Plan for heavy guest access use
- Client power/capability imbalance
- Outdoor uses
- Remote, offsite events

Jackman characterized the Goldilocks challenge as follows:

- Physical layer (PHY) rates—the speeds at which devices communicate via an access point or AP—are directly proportional to signal quality.
- The number of transmitters on the same channel is inversely proportional to performance.

According to Jackman, two aspects of the infrastructure are underemphasized in healthcare today: the importance of managing client devices (wireless devices and accessories that use the wireless infrastructure) and radio firmware that controls network connectivity. To address these issues, he recommended these considerations:

"Hospitals are now Internet service providers. Get used to the idea."
— Shawn Jackman, principal, manager, wireless product management and engineering at Kaiser Permanente

Client Device Considerations

- Precisely manage client radio firmware versions that control network connectivity.
- Understand client settings are equally as important as infrastructure.
- Consider radio characteristics: frequency(s) of operation, antenna(e), Tx/Rx power.
- Assess device density; plan for a high amount of device growth.
- As devices are not created equal, baseline them against each other to guide design standards and support efforts.

It is also important to provide fast, secure roaming (FSR) as an optimized way of quickly moving devices between APs to maximize performance.

Unifying Theme 4: Learn from other industries.

"Even the best safety standards are useless unless they are actually implemented."

— Yukiya Amano, director general of the International Atomic Energy Agency, urging a worldwide safety review after Japan's Fukishima nuclear disaster

Challenge	Priority Action	Accountability
Lack of agreement on standards and other guidance for wireless safety, security, testing, and reliability	Empanel a team to survey existing standards, policies, guidance documents, and best practices in healthcare and other industries (e.g., guidance on cybersecurity for manufacturing). Find and address gaps and vague language. Develop consensus on which standards and guidance should be used consistently by medical device developers. Share findings in a white paper and bibliography. Commission case studies of both successes and failures.	AAMI, IEEE, NIST, FDA, other SDOs
	Establish minimum, baseline security standards for specific environments that healthcare delivery organizations can use in requests for proposals.	All stakeholders
	Consider "medical grade" wireless standards.	SDOs Industry

The Role of Standards, Guidance, and Best Practices

Workshop participants are charting new territory in their efforts to develop and implement wireless technology in healthcare. Standards, guidance, and sharing of best practices are not keeping up with the demand for roadmaps for this work.

Standards do exist—but gaps and vague language inhibit their usefulness and, hence, their actual use, workshop participants said. Likewise, guidance and best practices are lagging behind wireless implementations. "Add to this the lack of qualified wireless personnel in healthcare organizations and it creates a situation where wireless applications do not meet their intended use cases," said Brian Long of Masimo.

But many other high-risk industries are tackling similar challenges with standards, policies, guidance, and best practices. Workshop participants are eager to learn from these industries, and from best practitioners in healthcare. Participants also called

EXISTING STANDARDS AND GUIDANCE FOR WIRELESS TECHNOLOGY

- ANSI/AAMI/IEC TIR 80001-2-1:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples
- ANSI/AAMI/IEC TIR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- ANSI/AAMI ISO 14971:2007, Medical devices - Application of risk management to medical devices
- ANSI/AAMI/IEC 80001-1:2010: Application of risk management for IT Networks incorporating medical devices - Part 1: Roles, responsibilities and activities
- ANSI/AAMI/IEC TIR 80001-2-3:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for wireless networks
- AAMI TIR18:2010 -- Guidance on electromagnetic compatibility of medical devices in healthcare facilities
- ANSI C63.18, Recommended Practice for an On-Site, Ad Hoc Test Method for Estimating Radiated Electromagnetic Immunity of Medical Devices to Specific Radio-Frequency Transmitters
- FDA Draft Guidance: Radio-Frequency Wireless Technology in Medical Devices
- IEC 60601-1-2: Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral standard: Electromagnetic compatibility - Requirements and tests
- IEEE 802®: Overview & Architecture
- IEEE 802.1™: Bridging & Management
- IEEE 802.2™: Logical Link Control
- IEEE 802.3™: Ethernet (Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications
- IEEE 802.11™: Wireless LANs
- IEEE 802.15™: Wireless Personal Area Networks (PANs)
- IEEE 802.16™: Broadband Wireless Metropolitan Area Networks (MANs—"Wi-Max")
- IEEE 802.17™: Resilient Packet Rings
- IEEE 802.20™: Mobile Broadband Wireless Access
- IEEE 802.21™: Media Independent Handover Services
- IEEE 802.22™: Wireless Regional Area Networks
- IEEE 473-1985, IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 GHz)
- IEEE 11073-00101:2008, Healthcare informatics – PoC medical device communication: Part 00101: Guide – Guidelines for the use of RF wireless technology
- ISO/IEC 15408-2:2008, Information technology – Security techniques –- Evaluation criteria for IT security – Part 2: Security functional components
- ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management

for a concerted effort to examine the state of the art in wireless technology and to disseminate findings broadly. Where there are gaps in standards, or where standards are lacking, they support efforts to develop additional standards.

In healthcare, as in other industries, it's important to express security requirements in a common way—and to design security to allow for the adoption of new technology and adaptation for security threats that are constantly changing. Developing standard approaches to testing, and usability standards, are important security steps as well.

"Medical Grade" Wireless Standards

An emerging concern of workshop participants is the increasing use of consumer devices and medical applications that run on them—without medical equipment standards.

Smartphones and tablets are communicating with medical devices using applications, thus putting these consumer devices "in charge" of the communication, according to workshop presenter Bill Saltzstein, president, connectBlue, Inc. Effectively, there are a whole new set of medical devices, developers, and designers, raising a number of issues and challenges, including:

- Inexperience with medical device development
  - Insufficient understanding by app developers on why regulatory agencies need to be involved.
  - Lack of distinction between a fitness vs. a medical device
  - Different mindset of quality
  - No understanding of hazard/risk analysis
  - Disbelief that apps can kill
- Off-the-shelf hardware and software
  - A challenge that predates wireless technology, and one for which the FDA has issued guidance, but the challenge now is consumers installing apps on platforms that cannot be configured or managed by healthcare technology managers. So, if a vendor verifies with a certain operating system (OS) release, it is likely that by the time the user installs the app, it will be on a newer version of that OS
- Multiple wireless interfaces
- Interference/coexistence
- Security

This will require educating the new medical device development community on the hows and whys of device development processes and hazard analysis, Saltzstein said.

Elliot Sloane of the Center for Healthcare Information Research and Policy suggested that there could be value in "medical grade" wireless standards, akin to existing Medical Grade Oxygen and Hospital Grade Electrical Outlets standards.

Wireless devices and applications have a direct role in patient care.

"Discussion, collaboration, standardization, and coordination of safe and orderly coexistence among many wireless healthcare devices and applications would help immensely, and probably cannot be ignored for much longer," Sloane said. Issues that need to be addressed include:

- Frequency allocations
- Quality of service
- Priority management
- Bandwidth management
- Security and access management

At this point, cautioned workshop presenter Steve Baker, senior principal engineer, Welch Allyn, "No one may declare that a network meets the requirements of a medical device except the manufacturer of that device. Simply being marketed as 'medical grade' does not mean that it is approved by the device manufacturer or the FDA. A cellular provider cannot say its products are medical grade. The definition of medical grade depends on the intended use."

Regulatory Perspective: Key Considerations for Wireless Medical Devices

Workshop presenter Don Witters, regulatory review scientist, Center for Devices and Radiological Health, FDA, said that safe, effective, reliable, and secure medical devices should be designed and deployed with the following considerations, which will ensure their performance now in the future.

- **Selection and performance of wireless technology.** "My approach is to be frequency agnostic," Witters said. "Whatever you choose, test and manage it."
- **Wireless quality of service (QoS).** "I am heartened by the conversation I've heard [at this workshop], with the discussion of quality of service and medical devices together," he said.
- **Wireless coexistence.** "It's important to associate wireless with components that are going to use it," he said. "What does the quality of service need to be for it to work properly? If you need certain reliability, this is where you start to describe that." Witters added that the American National Standards Institute (ANSI) has started a group working to develop a coexistence test method and standard.
- **Impact on other devices.** As a part of wireless infrastructure preparation for a medical grade environment, it's important to check to ensure that one device doesn't make it impossible for a second device to operate. Some wireless experts contend that this is easy to do, but medical device experts who have done installations and see the vast differences between hospitals know something very different. It's extremely difficult to codify this type of check-in requirements.
- **Wireless security.** Assessing the appropriate wireless security requirements must be accounted for with all medical applications.
- **Electromagnetic compatibility (EMC).** The collateral standards that accompany IEC 60601-1 cover requirements for EMC including emissions, electrostatic discharge (ESD), and susceptibility. A medical grade wireless infrastructure should be tested to these standards and provide some way of assuring that the wireless infrastructure: a) does not cause performance issues with the medical devices it supports, and b) provides a reliable data connection.
- **Information for set-up and operation.** Wireless infrastructure manufacturers need to provide best practices for the design and implementation of the variety of devices that may exist in healthcare environments.
- **Maintenance.** As new software, features and capabilities become available, healthcare organizations must assess the impact on already-deployed applications before deploying new solutions—and have a backup plan if things go south.

Unifying Theme 5: Manage risk and prevent failure—*Patient safety comes first.*

"Hold on! There's safety involved here."
— Bill Saltzstein, president, connectBlue, Inc.

Challenge	Priority Actions	Accountability
Inadequate recognition that wireless technology could jeopardize patient safety	Make patient safety the top priority of wireless medical technology in hospitals, distributed care settings, and for patient transport and mobility. Design wireless devices, networks, and system components for failure, using engineering principles and strategies.	HDOs Wireless infrastructure and component providers Industry
Inadequate attention to risk management	Use ANSI/AAMI/IEC 80001-1:2010: *Application of risk management for IT Networks incorporating medical devices* to manage risk, and the AAMI Technical Information Report (TIR) on risk management.	HDOs TJC and other accrediting organizations
	Prioritize wireless technology by risk level to patient safety and clinical applications. Conduct hazard analyses.	Industry HDOs
	Develop a standard approach to performance testing. Plan for the cost of testing and maintenance during design. View testing as a system that requires ongoing monitoring. Define testing responsibilities and staff testing appropriately. Allow adequate time for testing and verification.	Industry HDOs
Inattention to clinical needs, patient care settings, and workflow	Define clinical users and characterize use environments. Design wireless devices, networks, and systems to meet user needs in environments of care.	Industry HDOs
	Develop usability standards (e.g., a wireless icon, understanding of who the user is, a link between applications and wireless issues). Simplify the user interface.	SDOs Industry
	Improve the efficiency of the clinical workflow.	HDOs

Manage Risk

As with all medical technology, patient safety is too often an afterthought in wireless technology design, development, and implementation—a challenge that pertains to both industry and healthcare delivery organizations. Workshop participants advocated for making patient safety the top priority, the driver of wireless technology design, usability, testing, and risk management.

For healthcare delivery organizations, the focus must be on risk management.

The place to start is with the ANSI/AAMI/IEC standard 80001-1:2010: *Application of Risk Management for IT-Networks Incorporating Medical Devices—Part 1: Roles, Responsibilities, and Activities*. Just what is 80001? It's a standard that "introduces a new framework for managing safety and security when medical devices are included on a convergent, heterogeneous IT-network," according to AAMI.

The standard identifies the activities necessary to maintain key properties of the network—safety, effectiveness, and security. This standard, and guidance and tools associated with it, helps healthcare delivery organizations prioritize high-risk technology to focus on; discover emergent, or unexpected, properties in IT networks; and assign roles and responsibilities to risk management.

Workshop presenter Todd Cooper, co-chair of the ISO/IEC 80001 Joint Working Group 7, outlined current approaches to manage risk arising from the increasing deployment of devices in multi-vendor/multi-modality networking environments.

In one example, he highlighted a situation in which a hospital aimed to virtualize its infusion pump server. However, the hospital allowed oversubscription to increase average utilization. For 18 months, hospital and technology providers chased intermittent system malfunctions.

By implementing the network risk management standard IEC 80001, first published in 2010, Cooper revealed, the hospital was able to define critical operational requirements, identify hazards and risks (severity and probability), and deploy risk controls (e.g., bandwidth alerts).

In another example, a hospital acquired a new radiology system, which it was in the process of integrating and testing. However, management wanted to meet annual goals and pushed to have the system "go live" even though the deployment processes had not been completed.

Using 80001, the hospital was able to define organizational roles and responsibilities and a risk management policy and process, identify violation of the policy and process, leading to an executive "signoff" and assumption of responsibility.

According to the IOM's 2011 report, *Health IT and Patient Safety: Building Safer Systems for Better Care,* health IT may lead to safer care and/or introduce new risks. Because system-level failures almost always occur from unforeseen combinations of component failures, the report recommends that healthcare accrediting organizations adopt criteria relating to EHR safety; that all health IT vendors be required to publicly register and list their products, as well as adopt quality and risk management processes; and that reporting of health IT-related adverse events should be mandatory for vendors and voluntary and confidential for users.

> **"At Partners HealthCare, we are uniquely paranoid and proud of it."**
> — Rick Hampton, wireless manager, Partners HealthCare

These recommendations align, Cooper said, with the main elements of 80001. According to the standard, a hospital medical-IT network's "key properties" include:

- **Safety—**freedom from unacceptable risk of physical injury or damage to the health of people or damage to property or the environment.
- **Effectiveness—**the ability to produce the intended result for the patient and the responsible organization.
- **Data and system security—**an operational state in which information (data and systems) is reasonably protected from degradation of confidentiality, integrity, and availability. Accountability is key.

As Cooper noted, 80001-1 is only the first of a series of standards in this growing area. Several other related technical reports (TIRs)

in process include 80001-2-1 on step-by-step risk management; 80001-2-2 on communication of medical device security needs, risks and controls; and 80001-2-3 on wireless networking.

Bottom Line Up Front (BLUF)

Partners HealthCare's Rick Hampton delivered a presentation prepared by Andrew McGraw, medical device Information Assurance project manager, U.S. Air Force, with risk perspectives from the military. McGraw's BLUF (Bottom Line Up Front) message about risk:

- Operational risk is a *reality*.
- Zero risk is *impossible*.
- Some risk is *needed*.
- Ignoring risk is *foolish*.
- Allowing or avoiding too much risk results in *mission failure*.

Like the healthcare industry, defense has a difficult time meeting every requirement on devices themselves, according to McGraw. But risk is a reality. So risk management at the wireless operating system, network, and system levels must be business as usual as well. Strategies for risk management at these levels include encrypting information, authenticating users and uses, installing a wireless intrusion prevention system (WIPS) on the network, embedding firewalls, filtering wireless traffic with access control lists (ACLs), and isolating sensitive data.

"No single-fault failure should result in a high-risk event."
— Steven Baker, senior principal engineer, Welch Allyn

Prevent Failures

In industry, patient safety considerations should begin in the design phase, with "design for failure" as the guiding principle. "No single-fault failure should result in a high-risk event," said Steve Baker, senior principal engineer, Welch Allyn. In other words, if some part of a wireless system, network, device, or component fails, other parts of the system should continue to operate, even at reduced level, without putting patients at risk. "Seek and destroy single-fault failures," he said.

"Consider cascading failure events," he added. In other words, how likely is it for that initial failure to precipitate additional failures or disruptions in service? "It is amazing the many ways that things can be broken."

Reliability must be designed into the system. Just bolting reliable equipment together can result in an unreliable system. Instead, Baker offered this sequence of activities for systems design, which is relevant both to industry providers designing wireless products and connectivity services and to healthcare delivery organizations integrating wireless technology into their enterprises:

- Define the requirements
  - Conduct a failure modes and effects analysis (FEMA)
  - Conduct a hazards analysis
- Implement
- Test each component and subsystem
- Test the system
- Go live
- Test the live system

Baker and other workshop participants emphasized that adequate budget, time, and professional skills are required for testing and verification.

(The AAMI/FDA Interoperability Summit that preceded the Wireless Workshop explored systems design in detail. To learn more about systems design, see that report at www.aami.org/interoperability/Interoperability_Summit_publication.pdf).

Baker offered some specific solutions to guard against and mitigate Wi-Fi failure:

- Make use of fail-over redundancy supported by servers and infrastructure
- Ensure redundant RF coverage with interleaved backhaul (every other AP's Ethernet backhaul is to a different Power over Ethernet, or PoE, switch)
- Ensure uninterruptible power supply (UPS) backup
- Establish robust connections, drivers, and middleware
- Support 6Mbps data rate for maximum coverage and to minimize loss
- Follow wireless infrastructure design guide best practices to maximize coverage and minimize loss
- Consider disabling 802.11b support
- Use best-in-class security
  - WPA2 Enterprise and PSK
  - FIPS 140-2

Even with rigorous safety measures, "all medical device manufacturers still have 'problem' sites that exhibit worse RF performance than the rest," Baker said. In some cases, the physical facility impedes wireless performance. Failure to take facility constraints into account, and plan for them during design, can compromise wireless service and performance.

Another worrisome reality is that healthcare delivery organizations make changes to wireless devices, networks, or systems without notifying others within their organizations, let alone the manufacturer, Baker said. For safety's sake, it's important to collaborate with internal and external stakeholders when changes are made—and it's important to document changes as well.

Workshop participants recommended using additional tools and strategies to ensure the safety and security of wireless technology, including fault tolerance and software assurance. Fault tolerance is the ability of a system to respond gracefully to unexpected hardware or software failures, or power outages, with duplication built in so if one system fails, another can take over. Software assurance is a rigorous regimen of tools and processes to test and validate software to ensure safe and secure operations and reduce vulnerabilities to breaches and other threats.

The needs of clinical users tend to take a back seat in wireless technology design, development, and implementation as well, workshop participants said. Wireless technology is not always easy to use—and clinicians do not always have the skill set to troubleshoot problems. Designing wireless devices, networks, and systems to meet clinical needs in patient care settings, including hospitals, distributed care environments, and for patient transport and mobility, is paramount.

Participants also called for the development of usability standards to express users' needs, and attention to the clinical workflow to enable clinicians to make better use of wireless technology. Streamlined clinical processes would facilitate industry design of wireless products and services that are easier to integrate into healthcare.

Workshop participants also recommended the use of onboard diagnostics and remote diagnostic capability, which would help healthcare technology managers identify and correct any issues or failures with wireless technology, take the burden of handling wireless issues away from clinicians, and avert patient harm. In addition, they recommended proactive battery management to keep wireless technology powered without unanticipated interruption.

Testing, Testing: What Medical Device Manufacturers and Hospitals Can Do

Just who is responsible for testing wireless medical technology? Workshop presenters Phil Raymond, wireless architect, Philips Healthcare, and Welch Allyn's Steve Baker offered the following advice to medical device manufacturers (MDMs) and hospitals, as well as specific advice on when, where, and how to test:

What an MDM Can Do

- Define system-level performance specification (e.g., latency, traffic types)
- Characterize device and radio performance specification (e.g., QoS, security)
- Establish RF environment requirements (e.g., received signal strength indication or RSSI; signal-to-noise ratio, or SNR)
- Provide device-specific intended use(s)
- Test to some specific wireless local area network (WLAN) vendor configurations
- Test to ensure there is minimal to no negative impact on clinicians from the network

What an MDM Cannot Do

- Test to a specific hospital RF environment
- Test every network topology
- Create a replica environment of hospital devices (coexistence)
- Test every variation of WLAN vendor configuration (standard and proprietary)

What Hospitals Should Do

- Apply a risk management umbrella within the design, deployment, and management of a medical IT network
- Understand clinical use, networking performance, and characteristics of end devices
- Know your WLAN vendor (read the manual)
- Test according to hospital RF environment, network topologies, configurations, device coexistence

When to Test

- Changes to the network & devices
  - WLAN configuration
  - New device(s) introduction
  - WLAN physical layout
  - New construction (RF environment changes)
- Consider risk management as a tool to identify the "when"
  - If the risk level is high and testing decreases the probability or severity of unintended consequences, then test
- Compare the difficulty in testing vs. the difficulty in recovering from network failure
- Example:
  - Test failover recovery on a redundant controller

What to Test

- Depends on what has changed (risk review)
- Include regression testing
  - Existing devices included for interoperability
- Both medical and non-medical devices
  - New VoIP devices added to hospital WLAN
  - WLAN vendor software upgrade
  - WLAN configuration changes (vendor recommended, QoS implementation, security upgrade to RADIUS)
  - APs added or AP location changed
- Interoperability between WLAN and device configurations

- Basic connectivity of all devices
  - Example: IT security certificates SNAFU
  - From device to server, not just "on" the network
  - Test procedures are not just a set of check boxes!
- Long-term operation
  - 24 to 96 hours
- Roaming or device handover
  - AP to AP, ward-to-ward
- WLAN Load
  - Particularly with new devices, test on single AP if not actual network

Where to Test

- Small clinic or IT network in a non-patient area of the hospital
  - Pros:
    - Isolated physically and logically: Eliminate direct risk of connected patients
    - Uses IT network configurations
    - Includes both medical and non-medical traffic
  - Cons:
    - Requires changes (additions, modifications) to IT network configuration (consider a permanent test subnet/VLAN to mitigate this)
    - May need to coordinate scheduling with IT and hospital administration
    - Test traffic pathways require definition: routing, etc.
- A stand-alone lab
  - Pros:
    - Test when needed with full control over network configurations
    - Physically isolated from hospital IT network
  - Cons:
    - Smaller network footprint (fewer network devices, less complex)
    - Device numbers not representative of IT network loading
- Use a phased approach from isolated testing IT to network testing live-patient, high-confidence testing

How to Test

- Not on patients! Most devices have demo modes.
- Collaborative effort
  - In hospital—clinical engineering CE and IT
  - External to hospital—MDM and network manufacturer
- Understand device-level networking requirements
- Understand and duplicate current production configuration
  - Device configuration
  - WLAN configuration—duplicate hospital network configuration
- Proper tools
  - Site survey tool (RSSI, SNR, Interference)
  - Wireless and wired packet capture
  - WLAN and device manufacturer built-in performance monitoring tools
- Test device, WLAN, configurations prior to going live

Conclusion and Next Steps

The AAMI Wireless Workshop had a "roll up our sleeves, get to work, and get something done" flavor to it. In two days, 75 wireless experts in healthcare, developed specific priority actions, offered smart solutions, and recommended organizations that could take the lead on solving the most urgent challenges.

After struggling for some time to address these issues on their own, these experts are eager to engage a broader group of stakeholders to improve patient safety in an increasingly wireless world.

AAMI is not a "wireless" organization, nor does it inherently possess wireless expertise. AAMI does, however, know how to convene experts, and that is exactly what it has done and will continue to do to "do our part."

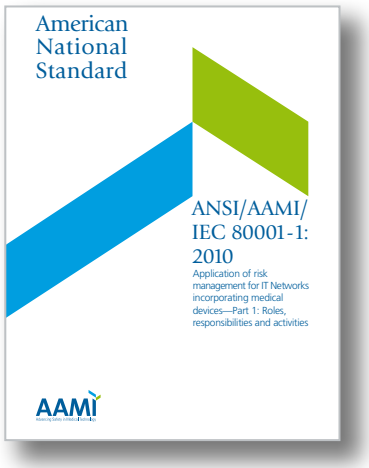
The follow-up work has already begun. After the workshop, AAMI formed a wireless task force, a small group of experts who have graciously agreed to keep this moving forward. The group will meet in March 2013 to clarify and refine the work and determine what is best suited for standards-setting organizations, healthcare delivery organizations, the medical technology industry, wireless infrastructure providers, and so on. Some challenges will require collaboration among different stakeholders, which is exactly the spirit in which all of this work should proceed.

Bob Stiefel (robsti@verizon.net) will coordinate and manage the task force for AAMI. When the task force has completed its work, it will disband or morph into something else, yet to be determined. In the meantime, here's a heads-up: AAMI or the wireless task force might be nudging other organizations to take on projects that are clearly needed.

If you have made it through this publication and are pondering what your organization can do to help, thank you. Real progress will take many organizations and committed individuals doing their part. Together, we can create a wireless world in which patient safety comes first, wireless medical technology is more secure and reliable, and the healthcare community harnesses the wireless waves for maximum effectiveness.

3 NEW TIRS!

AAMI Guidance For Healthcare Providers Managing Medical IT-Networks



ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT Networks incorporating medical devices— Part 1: Roles, responsibilities and activities*

Order Code: 8000101 or 8000101-PDF
List $100 / AAMI member $50

ANSI/AAMI/IEC TIR80001-2-1:2012, *Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples*

Order Code: 800010201 or 800010201-PDF
List $120 / AAMI member $60

ANSI/AAMI/IEC TIR80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the communication of medical device security needs, risks and controls*

Order Code: 800010202 or 800010202-PDF
List $120 / AAMI member $60

ANSI/AAMI/IEC TIR80001-2-3:2012, *Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for wireless networks*

Order Code: 800010203 or 800010203-PDF
List $110 / AAMI member $55

Order your Copy Today!
Call +1-877-249-8226 or visit www.aami.org

SOURCE CODE: PB

AAMI
Advancing Safety in Medical Technology

GLOSSARY

Editor's Note: *This glossary of wireless networking terms and definitions is based on one from the wireless guidance technical report, ANSI/AAMI/IEC TIR80001-2-3:2012; Application of risk management for IT-networks incorporating medical devices—Part 2-3: Guidance for wireless networks. Reprinted from AAMI Horizons "Managing Medical Devices on the IT Network."*

802.11: a series of IEEE standards that relate to wireless local area networks typically in the 2.4GHz ISM and 5GHz ISM and unlicensed national information infrastructure (UNII) bands

802.11A: an IEEE standard that relates to wireless local area networks in the 5GHz ISM and UNII bands

802.11B/G: an IEEE standard that relates to wireless local area networks in the 2.4GHz ISM band

Access Point (AP): a bridge from a wireless medium to a wired medium

Advanced Encryption Standard (AES): a symmetric-key encryption standard. One of its uses is for the WPA2 wireless encryption standard.

Body Area Network (BAN): a network of wireless sensors placed on the human body that communicate with each other

Basic Service Set Identifier (BSSID): an 802.11 term for the MAC address of an AP

Bootstrap Protocol (BOOTP): a network protocol used by a network client to obtain an IP address from a configuration server

Encoder/Decoder (CODEC): a module that can encode data and decode data

Chief Information Officer (CIO): person in the organization who is responsible for IT strategy and deployment

Data Integrity: assurance that transmitted files are not deleted, modified, duplicated, or forged without detection

Digital Enhanced Cordless Telecommunications (DECT): a digital communication standard, which is primarily used for creating cordless phone systems

Distributed Antenna System (DAS): an antenna system that collects wireless signals and routes them to centralized locations

Dynamic Frequency Selection (DFS): a mechanism for dynamically selecting frequencies to avoid interference sources – usually used in conjunction with the mechanism 802.11A-based systems use to avoid frequencies used by radar systems

Dynamic Host Configuration Protocol (DHCP): a method to allocate IP addresses to client devices upon request by the client

Extensible Authentication Protocol (EAP): an authentication framework frequently used in wireless networks and Point-to-Point connections. It is defined in Request for Comments (RFC) 3748 and was updated by RFC 5247

Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): a specific authentication method using the EAP authentication framework (RFC 5216)

Electromagnetic Interference (EMI): degradation of the performance of a piece of equipment, transmission channel, or system (such as medical devices) caused by an electromagnetic disturbance

Electronic Medical Record (EMR): a computerized medical record created in an HDO

Electronic Protected Health Information (EPHI): any protected health information (PHI) which is stored, accessed, transmitted or received electronically

Extended Service Set Identifier (ESSID): a term that describes a logical grouping of multiple BSSIDs

NOTE: This term is sometimes used in place of SSID.

Frequency Hopping Spread Spectrum (FHSS): A method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver

Hazardous Situation: circumstance in which people, property, or the environment are exposed to one or more hazard(s)
[ISO 14971:2007, definition 2.4]

Healthcare Delivery Organization (HDO): a facility or enterprise such as a clinic or hospital that provides healthcare services

Health Insurance Portability And Accountability Act (HIPAA): legislation enacted in the United States that among its provisions requires the protection of Protected Health Information (PHI)

Go-Live: the point at which a system transitions from the installation phase to the active use phase

Immunity: the ability of an electrical or electronic product to operate as intended without performance degradation in the presence of an electromagnetic disturbance.

Intensive Care Unit (ICU): a defined area or department in the hospital allocated for critically ill patients, sometimes also referred to as an Intensive Therapy Unit (ITU)

Internet Group Multicast Protocol (IGMP): a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships

Intrusion Detection System (IDS): a system that monitors the wireless environment and detects unauthorized uses such as "rogue" access points, viruses, worms, etc.

Internet Group Multicast Group (IGMP): a communications protocol used to manage the membership of Internet Protocol multicast groups

Intrusion Protection System (IPS): a system that includes an IDS and actively attempts to block system intrusions

Information Technology (IT): synonymous with Information Systems, as used in many HDOs

Industrial, Scientific, and Medical (ISM) Band: certain radio bands that were originally reserved internationally for the use of radio frequency (RF) energy for industrial, scientific and medical purposes

Latency: the time it takes for a unit of information to cross a wireless link or network connection, from sender to receiver, also known as transfer delay

Local Area Network (LAN): a computer network covering a small physical area

NOTE: In 802.3 parlance, a LAN is a set of devices that share a broadcast domain.

Media Access Control (MAC): part of the Link Layer in the Open System Interconnection Reference Model

Medical Device Manufacturer (MDM): a manufacturer of medical devices

Multiple-In Multiple-Out (MIMO): the use of multiple antennas at both the transmitter and receiver to improve communication performance

Multicast Addressing: a technology for delivering a message to a group of destinations on a network simultaneously

Personal Area Network (PAN): a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body

Personal Communication Services (PCS): term used for the 1900 MHz band that is used for digital mobile phone services in North America

Physical Interface (PHY): the layer of a communication controller that interfaces to the physical world

Portable Digital Assistant (PDA): a small computing device used for applications such as maintaining a personal diary or schedule

Pre-Shared Key (PSK): a shared secret that was previously shared between the two parties to be used for the encryption of data to be communicated between them

Quality of Service (QoS): A level of performance in a data communications system or other service, typically encompassing multiple performance parameters, such as reliability of data transmission, transfer rate, error rate, and mechanisms and priority levels for time-critical signals

Radio Frequency (RF): a rate of oscillation in the range of about 30 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals

Radio Frequency Identification (RFID): identification of objects or persons using special tags that contain information (such as demographics, serial number, etc.) that can be read using RF based readers

Received Signal Strength Indicator (RSSI): a measure, typically in dBm, of the RF power detected by a receiver

Security: a collection of services, policies, and mechanisms that provides some level of assurance that unauthorized parties are meaningfully restricted from accessing, manipulating, or leveraging particular system resources
NOTE: Some security services might include data encryption, data integrity-checking, user and device authentication, and non-repudiation.

Service Level Agreement (SLA): the necessary level of performance in a data communications system or other service, typically encompassing multiple performance parameters, such as reliability of data transmission, transfer rate, error rate, and mechanisms and priority levels for time-critical signals
NOTE: A typical network services SLA covers metrics such as availability, latency and throughput. It can also include specifications for mean time to respond, mean time to repair and problem notification/escalation guarantees. In wireless systems, examples include data rate, signal strength, jitter, and latency.

Simple Network Management Protocol (SNMP): an Internet-standard protocol for managing devices on IP networks

Signal to Noise Ratio (SNR): a comparison of signal power to noise power

Susceptibility: the potential for equipment (including medical devices) to respond to an electromagnetic disturbance. The inability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance. *Note: Susceptibility is a lack of immunity.*

TCP: one of the core protocols within the Internet protocol suite
NOTE: Differs from UDP in that TCP is acknowledged and connection oriented

Temporal Key Integrity Protocol (TKIP): this was an interim security solution that legacy hardware could support when WEP was found vulnerable
NOTE: Also known under the 802.11 branding as WPA

User Datagram Protocol (UDP): one of the core protocols within the Internet protocol suite
NOTE: Differs from TCP in that UDP is not acknowledged and connectionless oriented.

Validation: a process or test to determine if the device, under actual or simulated use conditions, conforms to defined user needs and intended uses

Verification: a process or test to determine if the device performs according to design and development input specifications

Virtual Lan (VLAN): a group of hosts that communicate as if they were attached to the same broadcast domain, regardless of their physical location or physical attachment to the same network switch

Voice over Internet Protocol (VoIP): a technology that allows telephone calls to be made over computer networks
NOTE: A typical CODEC, the G.711 consumes a network bandwidth of 64 kbps comprised in 50 packets per second.

Vulnerability: See latency, security and susceptibility.

Wide Area Network (WAN): A network that covers a very broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries)

Wired Equivalent Privacy (WEP): the original security mechanism of 802.11 has been superseded by TKIP (aka WPA) for legacy devices and AES (aka WPA2) for all 802.11 certified devices since 2006

Wireless Coexistence: the ability of one wireless system to perform a task in a given shared environment where other systems (in that environment) have an ability to perform their tasks and might or might not be using the same set of rules

Wireless Fidelity (WI-FI™): a trademark of the Wi-Fi Alliance

Wireless Local Area Network (WLAN): a Local Area Network (LAN) in which devices communicate using wireless means (such as 802.11 based technology)

Wireless Medical Telemetry Service (WMTS): a wireless service (set of RF bands) specifically defined in the United States by the Federal Communications Commission (FCC) for transmission of data related to a patient's health (biotelemetry)

Wi-Fi Multi-Media (WMM): a subset of the 802.11e standard that provides a higher Quality of Service for delivery of messages for some traffic classes

Wi-Fi Protected Access (WPA): an interim security solution that fixed many of the weaknesses in WEP and could be implemented on legacy hardware designed to implement WEP

Wi-Fi Protected Access 2 (WPA2): The long-term security solution put in place to replace WEP and WPA
NOTE: WPA2 uses the Advanced Encryption Standard and adds security features such as a message integrity check.

ACKNOWLEDGMENTS

Workshop Presenters

Steve Baker
Welch Allyn

Todd Cooper
80001 Experts

Ken Fuchs
Mindray

Mark Gibson
Comsearch

Rick Hampton
Partners HealthCare

Shawn Jackman
Kaiser Permanente

Ira Keltz
Federal Communications Commission (FCC)

Phil Raymond
Philips

Bill Saltzstein
connectBlue, Inc.

Elliot Sloane
Center for Healthcare Information Research and Policy

Peter Thornycroft
Aruba Networks

Donald Witters
U.S Food and Drug Administration

Writing

Martha Vockley
Vockley•Lang

Erika Hatva
AAMI

Kristin Blair, Design
AAMI

A special thank you to West Health for supporting both the workshop and the publication.

West Health
www.westhealth.org

Aaron Goldmuntz
amgoldmuntz@westhealth.org
202-729-8568

Move Your Medical Technology Career Forward

Join Your Peers...

Nearly 7,000 medical technology professionals are members of AAMI— a community dedicated to advancing the safety of medical technology.

Join AAMI to receive:

- Complimentary subscriptions to AAMI's journal, newsletter, and other publications featuring important news
- Access to up-to-date activities about AAMI's Sterilization committee
- Deep discounts on standards, guidance documents, webinars, and other educational programs
- Direct access to manufacturing experts, clinicians, and users of technology; as well as FDA and Joint Commission officials
- New information about patient safety initiatives, leading practices, cost-saving tips, and troubleshooting techniques
- Networking opportunities, career tools, other online resources, and much more

Join AAMI today—visit www.aami.org/membership or call +1-800-332-2264, ext. 1214.

AAMI
Advancing Safety in Medical Technology

Thank You Sponsors

This publication was made possible by the financial support provided by these organizations.

B. Braun Medical
www.bbraunusa.com

Jack Hoffman
jack.hoffman@bbraun.com
405-657-4916

ConnectBlue
www.connectblue.com/AAMI

Bill Saltzstein
bill.saltzstein@connectblue.com
425-442-5854

Philips Healthcare
www.philips.com/clinicalit

Olivia Hecht
olivia.hecht@philips.com
978-659-3000

CareFusion
www.carefusion.com

Krishna Uppugonduri
krishna.uppugonduri@CareFusion.com
858-617-5648

Intel Corp.
www.intel.com

Michael P. Taborn
michael.p.taborn@intel.com
480-554-1064

University of Michigan
http://secure-medicine.org

Kevin Fu
kevinfu@umich.edu
616-594-0385

Comsearch
www.comsearch.com

Laura Fontaine
lfontain@comsearch.com
703-726-5885

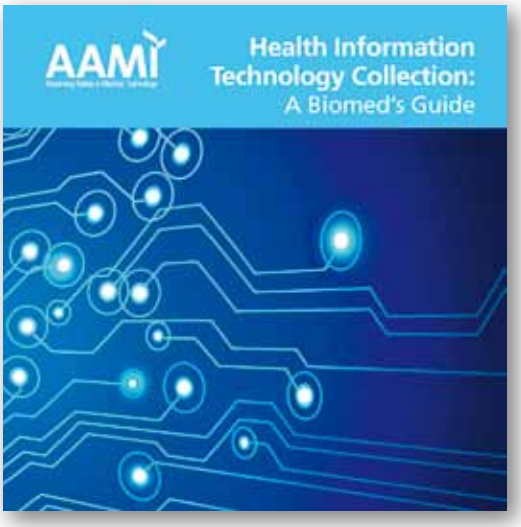
Masimo
www.masimo.com

Charlie Schmidt
cschmidt@masimo.com
949-297-7369

The sponsors listed on these pages helped to pay for the production costs for this publication. The sponsorships do not constitute any type of endorsement of the sponsors by AAMI or its co-conveners. AAMI expresses its gratitude to these companies for sponsoring this publication.

Health Information Technology Collection: A Biomed's Guide

This comprehensive CD includes more than 200 articles from AAMI publications, specifically on major IT issues in the medical profession.



It examines:

- Device connectivity
- IT Security, bots, malware, and spyware
- Integrating patient data
- Network management and applying 80001
- Picture archiving and communications systems (PACS)
- Radio frequency identification technology (RFID)
- Networked medical devices
- Bluetooth wireless technology

The CD features a detailed glossary of terms, and a convenient search function.

Order Code: ITCD

List / AAMI member: $150 / $80

Order your Copy Today!
Call +1-877-249-8226 or visit
www.aami.org

SOURCE CODE: PB

AAMI
Advancing Safety in Medical Technology

AAMI
Advancing Safety in Medical Technology

4301 N. Fairfax Drive, Suite 301 Arlington, VA 22203-1633 Phone: +1-703-525-4890 Web: www.aami.org