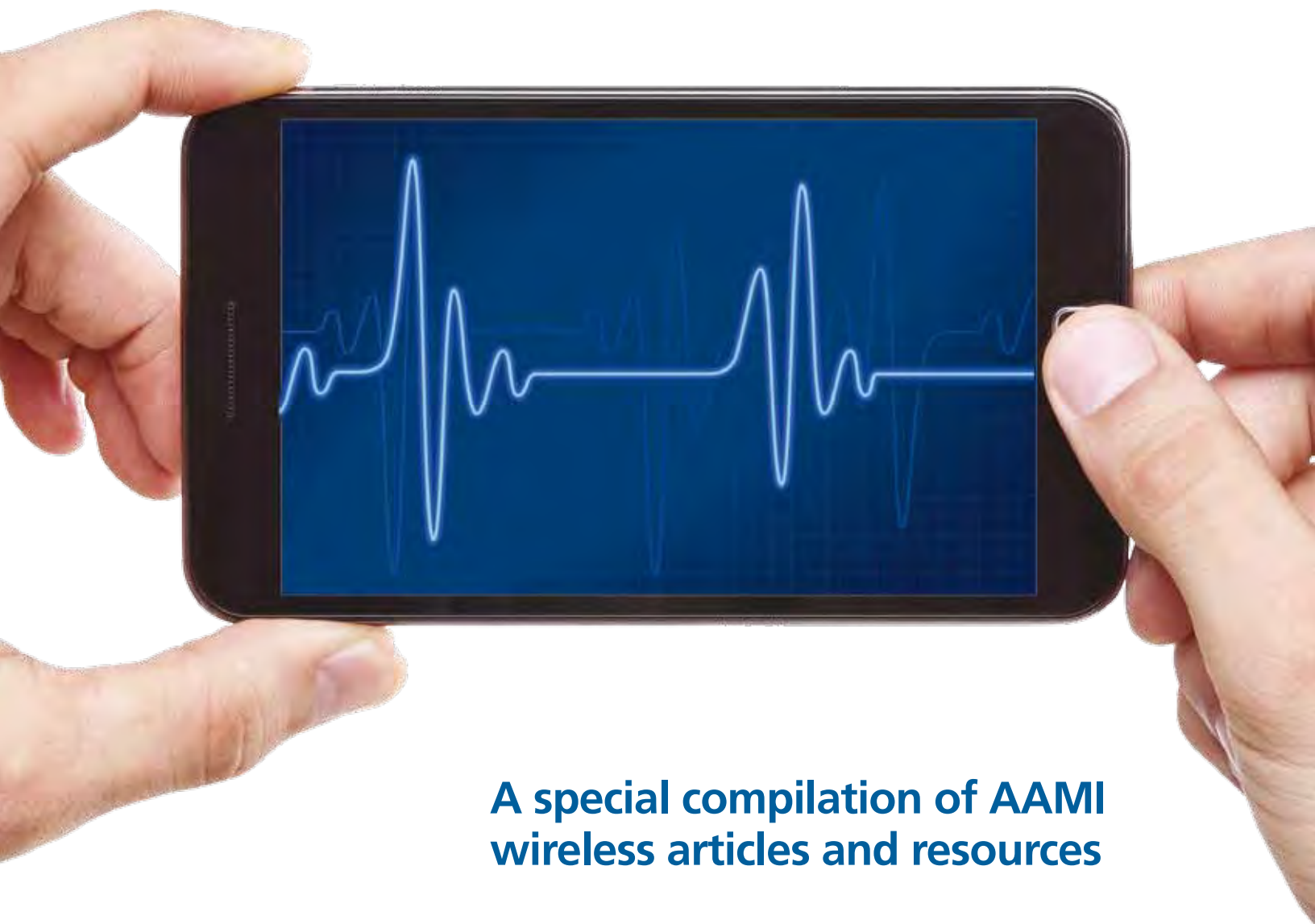


# Going Wireless



**A special compilation of AAMI  
wireless articles and resources**

## About This Compilation

AAMI has created this special compilation of wireless resources to provide insight and practical guidance to the healthcare technology community. These articles—originally published in AAMI’s journal, magazine, and summit publication—examine the major wireless challenges in healthcare. These peer-reviewed resources include case studies, a list of common mistakes, and additional resources and reading materials that you may wish to review. We encourage you to read the publication and apply lessons to improve patient safety, share this document with your colleagues, and nudge other organizations to help address these important issues.

## About 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.

## About AAMI’s Wireless Strategy Task Force

AAMI’s Wireless Strategy Task Force (WSTF) was formed to help implement the priorities identified during the AAMI Wireless Workshop held in the fall of 2012. Those priorities include clarifying roles and responsibilities in the wireless arena, managing spectrum to improve safety and security, designing wireless infrastructure for high reliability, learning from other industries, and managing risk and preventing failure. The WSTF—which is comprised of manufacturers, regulators, users of technology, and other interested parties—is developing educational resources and tools and sharing best practices to address wireless challenges in healthcare. Many of the resources included in this compilation were written by members of the WSTF. For more information about the WSTF, contact Steve Campbell at [scampbell@aami.org](mailto:scampbell@aami.org).

Mention of any commercial product, process, or service by trade name, trademark, manufacturer, or otherwise in this publication does not constitute or imply an endorsement or recommendation by AAMI. The views and opinions of the authors do not state or reflect the opinion of AAMI.

### *Published by*

Association for the Advancement of Medical Instrumentation  
4301 N. Fairfax Dr., Suite 301  
Arlington, VA 22203-1633  
[www.aami.org](http://www.aami.org)

© 2013 AAMI, All rights reserved

*Permission is granted to distribute or reproduce this publication in its entirety for noncommercial and educational purposes. For other uses, or to order reprints of this report, contact Joe Bremner at [jbremner@aami.org](mailto:jbremner@aami.org).*

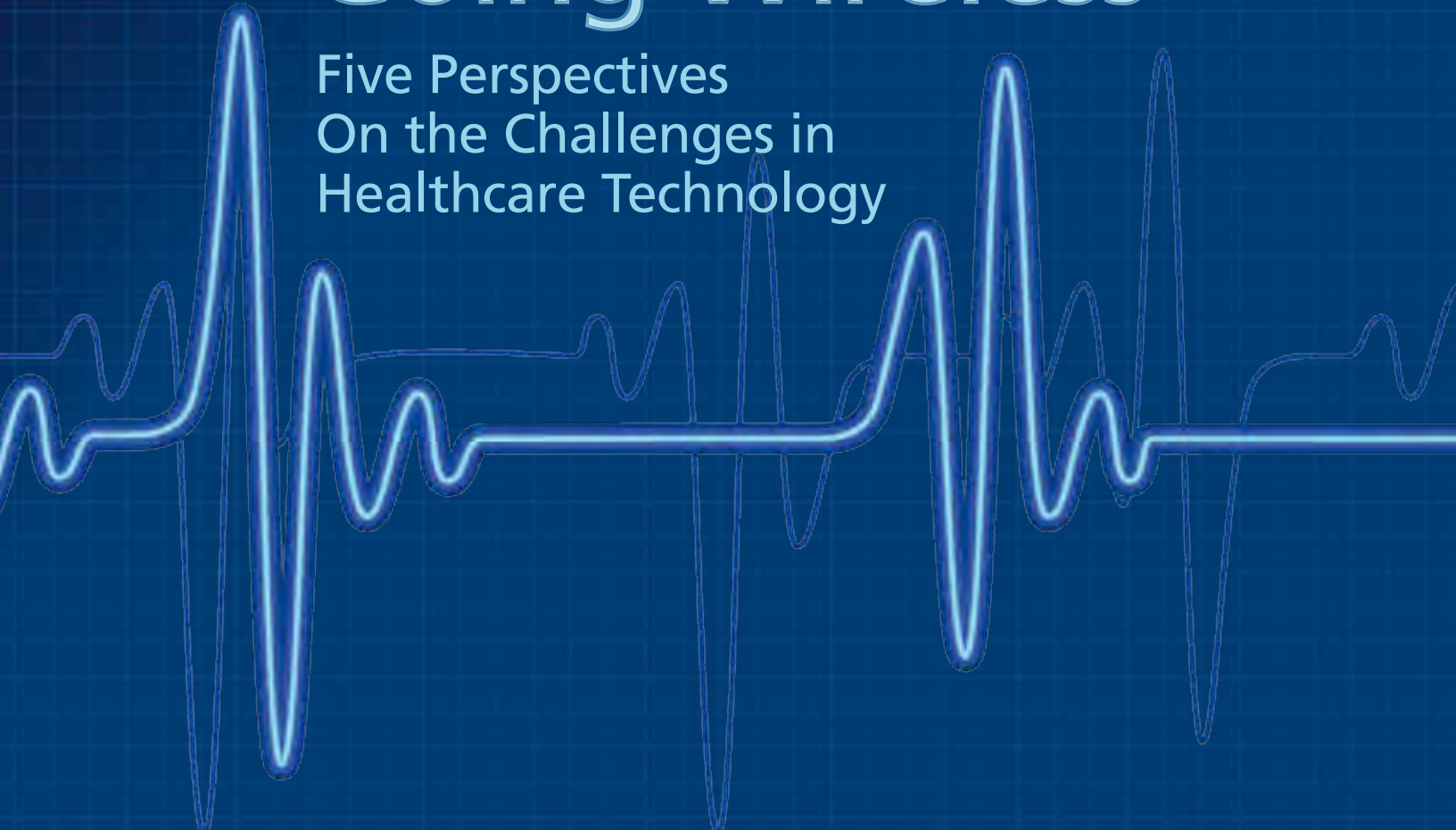
# Going Wireless

## Contents

- 2** Going Wireless: Five Perspectives on the Challenges in Healthcare Technology
- 3** Managing Your Hospital RF Spectrum
- 8** Achieving a Robust and Reliable Network
- 12** Technology Risk Assessment in Healthcare Facilities
- 18** Security and Safety for Medical Devices and Hospitals
- 22** Understanding the Wireless Spectrum in a Healthcare Facility
- 25** Top 10 Mistakes in Implementing Wireless Technology in Healthcare
- 26** Wireless Networking Risk Management Case Studies
- 30** Glossary
- 32** Wireless Resources and Additional Reading List

# Going Wireless

## Five Perspectives On the Challenges in Healthcare Technology



How can healthcare best harness wireless technology to help bring about safer, more efficient, and cost-effective patient care?

That broad and daunting challenge is the focus of the new AAMI Wireless Task Force, which is building on the momentum that began with last fall's Wireless Workshop. This past spring, the task force—a group of about two dozen representatives from medical device companies, hospitals, the U.S. Food and Drug Administration, and organizations that focus on wireless issues—met for two days to begin work on providing guidance to healthcare organizations.

As part of that effort, AAMI asked some members of the Wireless Task Force, which is led by Robert Stiefel of RHS Biomedical Engineering Consulting LLC, to contribute articles to this issue of *BI&T*, providing an overview of where things stand and a look at the road ahead. Even before the Wireless Task Force convened, Richard Swim of Baylor Health Care System, had contributed an article on the wireless spectrum. The five articles are the start of what AAMI hopes will be a comprehensive effort to help hospitals and other healthcare facilities navigate the world of wireless technology.

# The Wireless Challenge

## Managing Your Hospital RF Spectrum

H. Stephen Berger and H. Mark Gibson

*Editor's Note: Parts of this article first appeared in "Making Wireless Technology Work in Your Hospital" by H. Mark Gibson, published in the 2006 edition of IT Horizons.*

Wireless connectivity is increasingly the preferred method for communication in the healthcare delivery system. We talk over our cellphones, get information, send data over Wi-Fi networks, and use wireless sensors to monitor patients. With the rapid advances in wireless sensors and machine-to-machine communication, the use of wireless will only increase—and increase dramatically.

Wireless technologies in hospitals help doctors and nurses give patients better care, work more efficiently, and hold down costs. Patients, friends, and family bring their wireless devices so that they can continue to be connected and deal with other aspects of their lives while in the hospital.

However, every innovation brings its own challenges. Wireless communications can be interfered with or cause interference to other equipment. Radio frequency spectrum is the lifeblood of the wireless revolution, but it can become crowded or polluted by too many or the wrong type of emitters. As more and more wireless technologies and systems are introduced and rolled out in the hospital, proper management of this fundamental resource has never been more important.

### Use of Wireless in Healthcare

Because of their ability to provide mobility and instant access to data anywhere, wireless technologies have become widely used and accepted throughout healthcare. Some common wireless healthcare applications are:

- Monitoring patient vital signs
- Retrieving or updating health histories
- Receiving laboratory results remotely
- Clinician communication (patients and services)
- Computerized physician order entry (CPOE)
- Scheduling diagnostic tests while with the patient
- Tracking patients and equipment through the use of radio-frequency identification (RFID) technology
- Consulting the Physicians' Desk Reference
- Notifying patients to take medication

The addition of wireless to the already complex hospital environment has made the management challenge more difficult. Interference is a growing problem. In crowded conditions, the wireless links often become unreliable. A host of devices, intentionally and unintentionally, generate and radiate radio frequency (RF) energy. Add to this the com-

### About the Authors



*H. Stephen Berger is president of TEM Consulting in Georgetown, TX. E-mail: [stephen.berger.temconsulting@gmail.com](mailto:stephen.berger.temconsulting@gmail.com)*



*H. Mark Gibson is director of business development with Comsearch in Ashburn, VA. E-mail: [mgibson@comsearch.com](mailto:mgibson@comsearch.com)*

**As more and more wireless technologies and systems are introduced and rolled out in the hospital, proper management of this fundamental resource has never been more important.**



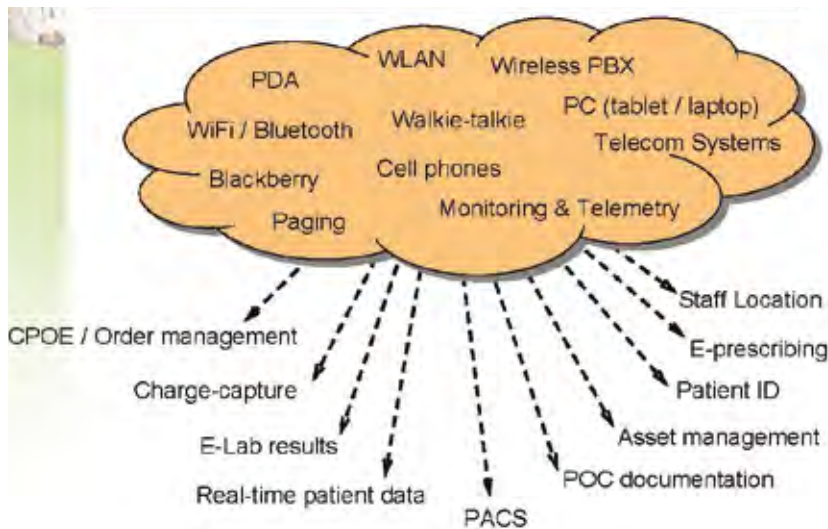


Figure 1. Functions Enabled by Wireless

plexities brought on by a wide variety of new wireless technologies and it is easy to see that proper planning is essential for the safe and efficient use of wireless in healthcare.

Connecting the management of spectrum in a hospital and the evaluation of medical devices that use wireless to the risk management processes used in the hospital is a new and necessary task for hospital administrators.

What can spectrum and technology experts do?

Frequency bands are already crowded. Especially in congested areas there can be more devices trying to communicate than the frequency band can support. Increasingly, these transmissions carry a mixture of entertainment and convenience information and important, time-sensitive medical data.

The Federal Communications Commission (FCC) regulates the use of spectrum in the United States, but the regulations were not written with the special needs of hospitals in mind, at least in some of the bands most commonly used by medical devices.

A large percentage of medical devices operate in the industrial, scientific, and medical (ISM) bands on an unlicensed basis. The choice comes at a cost. The FCC rules for unlicensed devices in these bands specify that:

1. The device may not cause harmful interference.
2. The device must accept any interference received, including interference that may cause undesired operation.

If unlicensed equipment has no guaran-

teed protection from interference, why would so many devices use these bands? There are a number of very compelling reasons:

1. The ISM bands are freely available.
2. These bands are internationally regulated, allowing products to be sold worldwide.
3. Because the bands are available to everyone, common chips, components and development support have been developed and are available to any company.

So while medical devices must operate in compliance with FCC rules, those rules only regulate what a device transmits. They do not regulate how sensitive the device is to the transmission of other devices in the same band or to unintentional sources of RF energy. This is the area in which a hospital can improve its situation. Devices vary greatly in their ability to operate in the presence of other emitters, whether intentional or unintentional. For this reason, careful device selection is very important.

What is required? The coexistence of the devices and systems being used need to be evaluated, and the use of spectrum should be managed to protect critical communications. However, a coexistence evaluation is a complex assignment involving multiple independent variables that interact in complex ways. The result of the evaluation is a set of probability distributions that identify the potential for interference.

While vendors may claim metaphysical perfection for their products, that is not the case. In fact, the ability of Wi-Fi devices to operate in the presence of other such devices varies by at least a factor of 100. Some Wi-Fi devices are many times more capable of operating in a crowded environment than other devices. Selecting the best devices on the market can reduce the amount of wireless interference in a hospital by a factor of 100 or more. However, information on the performance of devices is not easy to come by. Manufacturers of the more poorly performing devices are certainly not going to highlight that information. Often, the reality is that they haven't done the testing and don't know how well their own devices function in a crowded RF environment.

Another area of management is network configuration and updating. Wi-Fi and all of

**Some Wi-Fi devices are many times more capable of operating in a crowded environment than other devices.**

the commonly used wireless applications have improved their ability to operate in crowded spectrum. As more devices go wireless, RF designers have been adding a wide variety of innovative techniques to deal with the situation. However, many of these techniques are user selectable. They can be turned on or off. So a hospital can select more robust devices and then make sure they are configured to get the full benefit of the options available.

The 2.4 GHz band is by far the most heavily used band in hospitals. General uses that have also come into hospitals include:

- Wi-Fi, wireless local area network (WLAN), and other networking
- Bluetooth and ZigBee devices
- Microwave ovens
- Surveillance cameras and networks
- Building automation

Healthcare uses of the band include:

- Medical telemetry
- Nurse-call
- Patient data links

Because of its appeal, the band is becoming increasingly crowded. Managing interference is a common task for end users of equipment in the 2.4 GHz band.

### Managing the Wireless Environment

As a hospital's wireless environment becomes increasingly crowded and complex, it is good engineering practice to manage the RF spectrum proactively. A well-developed spectrum management program will mitigate the potential for problems before they cause critical equipment outage.

A first step is developing a frequency/device inventory of the devices under the hospital's control. This will not be a complete list of wireless devices in the hospital because patients, friends, and family bring in their own devices, as do contractors, police, emergency service personnel, and others who enter the facility. However, an inventory is critical for ensuring that a hospital has control of its own equipment and systems.

A wireless inventory is a key tool to be used in managing the wireless environment. The inventory should list as many known RF radiating devices in and around the hospital as possible, and should start with a rooftop-

to-basement assessment of operating and susceptible devices.

With this information, a spectrum plan can be developed to untangle the RF environment in the hospital. Spectrum sweeps provide an excellent snapshot of the existing RF environment. Armed with this baseline information and supplemented with an understanding of equipment susceptibilities and future growth plans, hospitals can develop strategies for coordinated wireless use throughout the facility.

The need to manage the spectrum falls into two priority areas. First, there will be some bands or situations in which interference is common and improvements are needed. An example might be lobby areas where there are many devices trying to operate at the same time.

A second priority area will be critical communications in which the consequences of interference are severe. Interference may not be frequent, but the chance of interference must be kept as low as possible.

Developing a successful wireless plan requires the involvement of all wireless stakeholders in the hospital—including representatives from biomedical engineering, risk management, facilities management, IT, nursing, and security.

Tips to follow in such an effort include:

- Know the RF environment in and around the hospital.
- Understand RF technologies being used

**A wireless inventory is a key tool to be used in managing the wireless environment.**

ISM (Industrial, Scientific, & Medical) Bands	
- 6.765 – 6.795 (6.78) MHz	- 2.400 – 2.4835 (2.450) GHz
- 13.553 – 13.567 (13.56) MHz	• Microwave Ovens
• RFID	• WLANs
- 26.957 – 27.283 (27.12) MHz	• Cordless Phones
• Cordless Phones	- 5.725 – 5.825 (5.8) GHz
• Garage Door Openers	• WLANs
• Wireless Auto Locks	• Microwave Systems
• Wireless Mouse	- 24.00 – 24.25 (24.125) GHz
- 40.66 – 40.70 (40.68) MHz	• Wireless Security Systems
• RC devices (e.g. model airplanes)	- 61.00 – 61.50 (61.25) GHz
- 902 – 928 (915) MHz	- 122 – 123 (122.50) GHz
• Cordless Phones	- 244 – 246 (245.00) GHz
• Paging	
• Nurse Call	
• RFID	

Those in RED are likely to be present in the hospital

**Table 1.** ISM Bands Used by Medical Devices

**It is unrealistic to expect every hospital to maintain a well-equipped RF diagnostic capability or have staff that is aware of the latest developments in this rapidly changing technology.**

and planned. Understand the impact of new technologies on existing ones, and vice versa.

- Know the weak spots in your hospital. If there is a heavy concentration of 2.4 GHz systems in a location, be aware what the introduction of additional devices might do to those already operating.
- Develop frequency coordination plans to separate priority communications from general use bands.
- Coordinate wireless deployment strategies throughout the hospital.
- Remember that you do not have to go it alone. While every hospital is unique, there are many common elements. Hospitals can work together through organizations such as AAMI to develop model plans and pool resources to accomplish the tasks required. The wireless environment is too dynamic to believe all problems can be avoided. New devices are constantly being introduced. Wireless technology is developing with amazing speed. Therefore, no matter how diligent you are, some interference is to be

expected. A hospital needs to be able to diagnose problems when they occur and deal with them.

The best diagnostic processes solve the common problems, but know when to seek additional help. It is unrealistic to expect every hospital to maintain a well-equipped RF diagnostic capability or have staff that is aware of the latest developments in this rapidly changing technology. A hospital can learn how to deal with the most common problems. Affordable instruments and tools are available to track down many problems. But there comes a time when more specialized equipment and wireless specialists will be needed.

The tools available to maintain a wireless network and eliminate interference sources are available, and an impressive number of new tools are being created. A hospital should learn about these tools. It is not difficult to equip yourself to deal with the most common kinds of interference. ■

FREQUENCY BAND	TYPICAL USE	HOSPITAL USE	NOTES
<b>Unlicensed Industrial, Scientific &amp; Medical (ISM) Bands</b>			
6.765 – 6.795 (6.78) MHz	Clock timing standard		
13.553 – 13.567 (13.56) MHz	RFID	RFID	Used for asset management
26.957 – 27.283 (27.12) MHz	Cordless Phones Garage Door Openers Wireless Auto Locks Wireless Mouse	Cordless Phones Wireless Auto Locks Wireless Mouse	
40.66 – 40.70 (40.68) MHz	Radio-controlled devices	None	
902 – 928 (915) MHz	Cordless Phones Paging Nurse Call RFID	Cordless Phones Paging Nurse Call RFID	
2.400 – 2.4835 (2.450) GHz	Microwave Ovens WLANS WiFi (802.11b) Bluetooth Cordless Phones Medical Telemetry	Microwave Ovens WLANS WiFi Bluetooth Cordless Phones Medical Telemetry	The FCC lists close to 8000 devices approved for use in this band
5.725 – 5.825 (5.8) GHz	WLANS (802.11a) Point-to-point microwave Systems	WLANS (802.11a) Point-to-point microwave Systems	
24.00 – 24.25 (24.125) GHz	Wireless Security Systems	Wireless Security Systems	
61.00 – 61.50 (61.25) GHz	Research		
122 – 123 (122.50) GHz	Research		
244 – 246 (245.00) GHz	Research		



OTHER UNLICENSED BANDS			
26.965 – 27.405 MHz	CB Radio	CB Radio	
72.0 – 73.0 & 75.4 – 76.0 MHz	Radio-controlled devices		
151.82, 151.88, 151.94, 154.57, & 154.60 MHz	Multi-Use Radio Service (MURS)		Like CB
402 – 405 MHz	Medical Implant Communications Service (MICS)	Medical implants	Primary allocation for meteorological aids at 400.15-406 MHz
406.0 – 406.1 MHz	Personal Locator Beacons (PLB)		
216.75 – 217.0 MHz	Low Power Radio Service (LPRS)		
462.5625 – 467.7125 MHz	Family Radio Service (FRS)	Family walkie talkies	
1920 – 1930 MHz	Unlicensed PCS Cordless Phones Wireless PBX	Unlicensed PCS Cordless Phones Wireless PBX	1910 – 1920 MHz reallocated to Nextel
5.150 – 5.250, 5.47 – 5.725, & 5.725 – 5.825 GHz	Point-to-point microwave Systems	Point-to-point microwave Systems	Unlicensed National Information Infrastructure (UNII)
OTHER SECONDARY USE SPECTRUM			
510 – 1705 KHz	Low power AM		Delivered through power lines
26.96 – 27.28 MHz	Radio controlled toys	Radio controlled toys	
40.66 – 40.7 MHz	Radio controlled toys & fireworks Remote entry Walkie talkies	Remote entry	
43.17 – 44.49, 46.6 – 46.98, 48.75 – 49.51, & 49.66 – 50.0 MHz	Cordless Phones	Cordless Phones	
49.82 – 49.9 MHz	Walkie talkies Wireless microphones Baby monitors	Walkie talkies Wireless microphones	
74.6 – 74.8, & 75.2 – 76.0 MHz	Walkie talkies Auditory assistance	Walkie talkies	
174 – 216 MHz	Broadcast TV (P) Medical telemetry Wireless intercom	Broadcast TV (P) Medical telemetry Wireless intercom	
300, 310, 315, 390 MHz	Government Land Mobile (P)* Remote control (keyless entry, garage door opener)	Government Land Mobile (P) Remote control (keyless entry, garage door opener)	There have been multiple reports of interference with garage door openers from people living close to military bases.
303.875 MHz	Government Land Mobile (P) Auto and home security alarms	Government Land Mobile (P)	Keyless entry devices
318.6 MHz	Government Land Mobile (P) Radio security alarms Smoke detectors	Government Land Mobile (P) Radio security alarms Smoke detectors	Keyless entry devices
418 MHz	Government Land Mobile & Research (P) Auto security Remote transmitters	Government Land Mobile & Research (P) Auto security Remote transmitters	Keyless entry devices
433.5 – 434.5 MHz	Amateur Radio (P) Auto security		
470 – 668 MHz	Broadcast TV (P) Medical telemetry	Broadcast TV (P) Medical telemetry	
554 – 590 MHz	Broadcast TV (P) Wireless microphones	Broadcast TV (P) Wireless microphones	

**Table 2.** Common shared and secondary-use frequencies found in and around the hospital\*

\* (P) indicates a primary allocation

# The Wireless Challenge

## Achieving a Robust And Reliable Network

Phil Raymond

### About the Author



*Phil Raymond is a wireless architect for Philips Healthcare. E-mail: philip.raymond@philips.com*

There is little argument that wireless connectivity in a hospital has many benefits in terms of clinical workflows, remote patient surveillance, mobility for clinicians and their patients, and even achieving meaningful use with data connectivity between clinical systems. There is also ample data showing that hospitals have chosen 802.11 wireless technology as the de facto standard for whole hospital data connectivity.

So are wireless medical devices, applications, and systems the perfect match for 802.11 wireless networks? Before answering, consider what we are trying to accomplish and how best to get there.

**A first step is to understand how your nurses and doctors are using their devices as part of their clinical workflows and daily operation. Do they rely on wireless network access to deliver safe and effective patient care?**

### **Why Do I Need a Robust and Reliable Network?**

Today's hospital clinical systems are now depending on the wireless network as an enabling technology, so the answer to this question may be as simple as, "Why wouldn't I"? But it is important to explore the ways in which the wireless network is used in your hospital. Each hospital will have different systems, different types of devices, different numbers of devices, and even different

policies, for example, those relating to BYOD or "bring your own device." And, of course, all this adds up to a radio frequency (RF) environment that is unique to that facility. From accurate departmental billing to using location technologies to provide patient family Internet access, there are many ways the wireless network is used, and each use may have different clinical implications or none at all.

A first step is to understand how your nurses and doctors are using their devices as part of their clinical workflows and daily operation. Do they rely on wireless network access to deliver safe and effective patient care? For example, if a doctor wants to pull up a radiology image while in a patient's room, is there a need for a robust and reliable wireless network? If a nurse is making a wireless "voice over Internet protocol" (VoIP) call at 2 a.m. to request assistance "stat," do you need a robust and reliable network?

If the answer to these questions is "yes," that is why a robust and reliable network is required. Obtaining an understanding of what types of devices are used and how they are used is important for more than just determining whether you need a robust and reliable network. It is also vital to designing and maintaining a robust and reliable network.

### **What Is a Robust and Reliable Network, and How Do I Get There?**

How do you put the cart before the horse? Design a wireless network(s) and then figure

out what number and types of devices and applications that the network must support. Understanding both the networking performance characteristics and clinical requirements of the devices prior to the design and deployment of the wireless network is crucial to creating a robust and reliable wireless ecosystem.

There are many ways to define a robust and reliable network, some of which are technical and others that are marketing focused (so-called “marketectures”). This paper focuses on a few of the technical attributes of a robust and reliable wireless network, and some design best practices to meet the connectivity needs of your hospital. Note that a network with a marketing branding of “medical grade” can be, but isn’t necessarily, robust and reliable. It needs to meet the requirements of the given hospital and the medical devices therein to be considered robust and reliable.

### **Coverage and Capacity**

It is one thing to cover an area with wireless access; it is another to make sure there is enough capacity in that wireless access to support all the devices. Consider how cellular coverage sometimes isn’t every place you want it to be and that during emergencies, the cellular networks are typically oversubscribed so calls cannot be completed. Providing coverage and capacity can be done in several ways. One way is to make use of available spectrum. If cellular coverage is sufficient in the hospital, then you may carry your voice calls over that network using regular cellular phones. You may also take advantage of the wireless medical telemetry system (WMTS) band for specific medical devices. You will most likely have an 802.11 network operating in unlicensed spectrum that is enabling data connectivity. You could even try and use the 802.11 network for converged services, such as voice, video, and data. It is the choice of each hospital as to how to effectively use the spectrum and available technologies, but there are options—all of which carry varying degrees of risk, technical competencies, and management. Within 802.11, channel reuse allows support of large numbers of 802.11 devices across the hospital.



A key step in achieving a robust and reliable wireless network is to determine how clinicians use mobile devices—including medical equipment and items such as tablets—in their daily jobs.

The bottom line is that you need coverage wherever devices are used, but you also need to account for the capacity needs, or bandwidth, to allow all of these devices to coexist peacefully in terms of networking performance. These decisions are made in the planning phase and always include risk management.

### **Mobility**

When a device is mobile, it will roam across the wireless network and in the case of a wireless local area network (WLAN), it will perform handovers between APs. The efficiency of this handover is crucial to maintaining a robust connection to the network. Clearly, it is critical that this handover occur very quickly, especially when the device requires a persistent connection to the network as in a VoIP call or a cardiac monitoring telemetry device. For example, 802.11 is a “break before make” technology, where the device must disassociate from an AP before it can connect to another AP. The time delta between the “break” and the “make” must be very short—in the order of milliseconds generally—because during this time the

**It is one thing to cover an area with wireless access; it is another to make sure that there is enough capacity in that wireless access to support all of the devices.**

device is not connected to the network. Good implementation of strong security, such as WPA2-Enterprise by both clients and the network, achieves this. Be sure that your network and devices support fast roaming.

### **Quality of Service**

Measuring quality of service (QoS) in networking terms is usually done with metrics such as packet latency (aka delay), packet loss, and jitter (time variation between packet-to-packet arrival times). When measuring the performance of a network, you may send a sequence of packets across the network with time stamps and receive them at the other end to determine the time it took to traverse the network. Network-monitoring tools use these metrics to evaluate the health of the network and are important to use in a network that needs to be robust and reliable.

Wireless QoS may be defined by additional metrics such as signal strengths, interference, signal-to-noise ratios (SNR), and packet error rate (PER). When you install a wireless network, there should be an RF site survey to measure signal strengths, co-channel interference, and SNR over the field of desired coverage. You generally want to design a WLAN RF environment to meet the

**Maintaining the RF environment takes diligence. One tool that is applicable is the periodic use of an RF site survey.**

needs of your most demanding application. That might be a VoIP application, video streaming, or patient surveillance. You also want to overprovision your network because the demand on the network will vary over the course of the day. It not only allows for high-usage scenarios, such as an emergency situation during which many users suddenly access the network, but also allows for scalability as more devices are connected to your network. A robust network supports the the QoS requirements of the most demanding devices while also providing network access to every device.

In the end, the goal is a positive and satisfying quality of experience (QoE) for users of the network, whether they are

nurses, other hospital staff, or a patient's family members. Properly designing and verifying the performance of the wireless network using the metrics of QoS will help to achieve that goal.

### **Now That I Am There, How Do I Stay There?**

Once your WLAN is operational and devices are successfully connecting and achieving their networking performance needs, implementing an effective maintenance program and change control process is important to staying robust and reliable.

### **RF Spectrum Management**

RF propagation in a hospital environment is a time-varying principle that can work for you one day and against you the next.

Maintaining the RF environment takes diligence. One tool that is applicable is the periodic use of an RF site survey. As mentioned, it is very important to perform an RF site survey during the design and deployment phase, but follow-up site surveys should be performed as part of the maintenance of the WLAN. They can be quarterly or every six months, but should be a key aspect of a quality maintenance program. Such surveys should also be done when there are changes to the WLAN, such as adding in access points, extending coverage into new areas of the hospital, or physical changes to the hospital.

### **Network Monitoring**

Many tools exist to monitor not only the performance of the network, but also the end devices. Network monitoring provides information for troubleshooting and management. It also can provide notification of degradation in performance of the network before the end devices experience poor connectivity. In the case of 802.11 WLANs, there are usually tools built into the controllers that measure bandwidth usage, number of clients, central processing unit (CPU) burden, PERs, and myriad other performance metrics. These tools should be used as part of the daily evaluation of the networking performance. This evaluation also can show the usage of the network to alert to higher capacity needs as the number of wireless

devices increases. One approach is to trend the worst-performing devices so you can be aware of when a piece of network gear starts to have issues. If the worst-loaded AP has typically 30 clients and a typical peak bandwidth of 15 Mbps, then increases over time to 40 clients and 20 Mbps, and finally 50 clients and 21 Mbps, there is a good chance this AP is oversubscribed. Watching to see if PERs trend up or SNRs trend down allows an information technology (IT) department to respond in time—rather than react to a network brownout.

### Change-Control Process

IT engineers are familiar with the concept of applying a change-control process to the management of the network. Adding medical devices and their associated clinical functionality adds another dimension. Taking down a network for a software upgrade without coordinating with the clinicians and healthcare technology management staff can lead to disasters. Checking with medical device vendors to see if their devices are validated for the updated infrastructure can help decrease testing and may lead to choosing a specific version of the network software that has been validated. Having a database of medical devices on the network and contact information for those devices allows an efficient way to do this.

Additional considerations for testing devices on either a lab setup or part of the actual network—but not on live patients—should also be part of the change-control process. Adding new devices to the network usually requires configuration changes on the infrastructure, so testing and managing the go-live process not only should ensure that the new devices can connect and perform as needed, but that existing devices are not negatively impacted. ■

### References

1. **AAMI.** ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT networks incorporating medical devices—Part 1: Roles, responsibilities and activities.* Association for the Advancement of Medical Instrumentation. Arlington, Va.

2. **AAMI.** ANSI/AAMI/IEC TIR80001-2-3:2012, *Application of risk management for IT networks incorporating medical devices—Part 2-3: Guidance for wireless networks.* Association for the Advancement of Medical Instrumentation. Arlington, Va.
3. **Wi-Fi Alliance.** *Wi-Fi in Healthcare: Security Solutions for Hospital Wi-Fi Networks.* 2012. Available at: [www.wi-fi.org/knowledge-center/white-papers/wi-fi%20AE-healthcare-security-solutions-hospital-wi-fi-networks-2012-0](http://www.wi-fi.org/knowledge-center/white-papers/wi-fi%20AE-healthcare-security-solutions-hospital-wi-fi-networks-2012-0). Accessed April 17, 2013.
4. **Wi-Fi Alliance.** *Wi-Fi in Healthcare: The Solution for Growing Hospital Communication Needs.* 2011. Available at [www.wi-fi.org/knowledge-center/white-papers/wi-fi%20AE-healthcare-solution-growing-hospital-communication-needs-2011](http://www.wi-fi.org/knowledge-center/white-papers/wi-fi%20AE-healthcare-solution-growing-hospital-communication-needs-2011). Accessed April 17, 2013.

**Taking down a network for a software upgrade without coordinating with the clinicians and healthcare technology management staff can lead to disasters.**

## ANSI/AAMI SW87:2012



Application of Quality Management System concepts to Medical Device Data Systems

**Order Code: SW87 or SW87-PDF**  
**List: \$100**  
**AAMI member: \$50**

SOURCE CODE: PB



**To order call +1-877-249-8226  
or visit <http://my.aami.org/store>**



# The Wireless Challenge

## Technology Risk Assessment In Healthcare Facilities

Todd Cooper and Ken Fuchs

### About the Authors



*Todd Cooper is a founding principal of 80001 Experts, LLC. E-mail: toddcooperafc@gmail.com*



*Ken Fuchs is senior principal architect for enterprise systems at Mindray North America. E-mail: K.Fuchs@mindray.com*

**More and more, vendors are installing systems in hospitals without a complete view of how they will be associated with other systems and how the infrastructure will evolve.**

The effects of an increasingly interconnected world are being felt in healthcare facilities everywhere. Vendor products—from the simplest medical devices to hospital-wide patient monitoring systems to complex electronic health record (EHR) systems—interconnect into systems of systems. More and more, vendors are installing systems in hospitals without a complete view of how they will be associated with other systems and how the infrastructure will evolve. As a result, the mission-critical burden of technology risk assessment and attending to unintended consequence avoidance falls increasingly on hospital staff.

To manage this evolving situation, hospitals need to adopt the tools that medical device vendors have learned to use over the past few decades, especially the concept of risk assessment. As designers quickly discovered, medical device design is all about risk management.

There is no such thing as a perfect medical device. Even the simplest medical device, such as a tongue depressor, can present risks—for example, slivers—to the patient. Aspirin has been hailed as a wonder drug, but when you read the label, there are numerous contraindications and risks associated with taking it. Similarly, the use of a blood pressure cuff has risks and benefits. The key point is that in all cases, the benefits associated with using the devices or drugs outweigh the foreseen risks to the patient or caregiver.

In order to assess the risk, you also have to understand the use context. Let's consider some scenarios concerning a patient being monitored on a wireless monitor. The risk to the patient varies depending on whether he or she is on a transport accompanied by a nurse, accompanied by an orderly, or is left unattended in a hallway, as can be the case in an emergency room (ER) overflow situation.

When a manufacturer submits a product to the U.S. Food and Drug Administration (FDA), one of the key statements is the “intended use,” which guides the regulatory review. Manufacturers can limit the intended use based on their risk analysis, which may signal that some scenarios present undue risk to the patient. They may decide, for example, that one of the above scenarios is too risky and may provide a warning. The hospital should pay attention to the manufacturer's statement of intended use, as well as all “instructions for use” (IFU) warnings to assure the medical device or system is not being used in a way the manufacturer did not intend or consider.

When a hospital integrates a medical device or system within its infrastructure, even if the hospital is adhering to the intended use, there is an additional burden on the hospital to assure that controls are in place to maintain an acceptable level of risk to the patient. We have arrived at this point as a result of technology changes occurring gradually over the past four decades.

## 40 Years of Networking

In the 1970s, patient monitors were “networked” together using analog signals. Cable harnesses were run from patient monitors to central stations with each signal requiring its own wire. In the 1980s, we started to see the adoption of serial communication, such as variations of synchronous data link control/high-level data link control (SDLC/HDLC) or proprietary protocols. In the 1990s, we saw the start of the transition to Ethernet, though at the time other competing technologies such as Token Ring needed to be considered. At the time, the bandwidth (10 mbit/second) which was shared among all devices and the nondeterministic nature of Ethernet kept many medical device engineers up at night. The installation of the first digital picture archiving and communication systems (PACS) required considerable bandwidth modeling and prestaging of images to get appropriate performance. This evolution mirrored changes in the general world of information technology (IT) as small stand-alone departmental systems were connected in unified enterprise infrastructures as the technology matured.

As we moved into the 21st century, wired infrastructure matured to the extent that hospitals started to think about merging patient monitoring and other medical device networks with their wired infrastructure. Networking technology had reached the point that each device could get a dedicated 10/100 Mbit/second connection, which was more than enough to meet the bandwidth requirements.

### What Does Wireless Have to Do with It?

Just when we thought we were safe, wireless technology such as Wi-Fi was introduced and has become wildly popular. Unfortunately, wireless brings back some of the technical challenges of the past with devices needing to share limited available bandwidth (typically ~20 mbit/sec). This may be fine for a stand-alone single use, such as a patient monitoring network, but since the radio frequency (RF) spectrum must be shared, there are many other uses and users clamoring for the same limited resource. Wireless also brings with it other issues, such as interference, security, and an inherent lower

**Wireless also brings with it other issues, such as interference, security, and an inherent lower level of reliability than wired networks.**

level of reliability than wired networks.

This situation has, at times, impacted the performance of wireless medical devices. In addition, the performance and capabilities of a wireless infrastructure differs considerably from one infrastructure vendor to the next. As a result, something that may work with Vendor A may not work with Vendor B or may not work as well, potentially negatively affecting the performance and resulting in unintended consequences.

### Genesis of ANSI/AAMI/IEC 80001

In 2008, The Joint Commission issued a Sentinel Event Alert, which stated, “As health information technology (HIT) and ‘converging technologies’—interrelationships between medical devices and HIT—are increasingly adopted by healthcare organizations, users must be mindful of the safety risks and preventable adverse events that these implementations can create or perpetuate.”<sup>1</sup>

In response, the FDA, manufacturers, and healthcare delivery organizations (HDOs) convened to work on this issue through a joint effort of ISO TC215 and IEC 62A, which created Joint Working Group 7 (JWG7). Over the course of five years, the group created the initial ANSI/AAMI/IEC 80001-1 standard as well as a number of technical reports that provide additional guidance on special topics, including wireless networking and security. The primary goal of the ISO/IEC 80001 series of standards is to assure that the safety, effectiveness, and data and system security of networked medical devices is not degraded in the context of the intended use of the device as determined by the “responsible organization” that is deploying the medical devices (e.g., hospital).

### Basics of Risk Assessment

Built on the same risk-management model<sup>2</sup> that medical device manufacturers use during

**What can go wrong?  
What are the possible unintended consequences that could result? And are they significant enough that risk controls need to be designed and implemented to ensure an acceptable level of safety?**

the development of their networked technologies,\* including entire vendor-specific medical networks,† 80001 begins with a risk assessment process that combines risk analysis—the identification of hazards, along with an estimation of the risk that they pose, given the context of their specific clinical use—with risk evaluation to determine acceptability of the technology being deployed. Per the IEC 80001-1 standard, hazards are defined as “potential sources of physical injury or damage to the health of people, or damage to property or the environment, or a reduction in effectiveness or degradation in data and system security.”<sup>3</sup>

In other words, think through the following: What can go wrong? What are the possible unintended consequences that could result? Are they significant enough that risk controls need to be designed and imple-

mented to ensure an acceptable level of safety? Again, note that the focus is not solely on patient safety, as is often assumed, but on all three “key properties” of the network: safety, effectiveness, and security (in that order of priority).<sup>4</sup>

In ANSI/AAMI/IEC TIR80001-2-1:2012, a 10-step process is detailed for basic risk management,<sup>5</sup> the first five of which are concerned with risk assessment:

1. Identify hazards.
2. Identify causes and resulting hazardous situations.
3. Estimate the potential severity of unintended consequence (or harm).
4. Estimate the probability of unintended consequence.
5. Evaluate risk.

In that document, a simple example is provided around the “loss of function”

Improbable	Very unlikely that use will result in any Unintended Consequence
Remote	Not likely to result in any Unintended Consequence
Occasional	Somewhat likely to result in any Unintended Consequence
Probable	Very likely to result in any Unintended Consequence
Frequent	Unintended Consequences occur frequently or occur every time

Scale	Safety	Effectiveness	Security
Catastrophic	Severe injury, death	Planned operation is no longer possible	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of information or services.
High	permanent impairment of body function or permanent damage of a body structure	Planned operation is disrupted or delayed	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of information or services.
Medium	Temporary and minor injury, medical intervention required	Inconveniencing to disrupted effect on operation	Will result in some tangible consequence, albeit negligible and perhaps only noted by a few individuals or agencies. May cause embarrassment. Will require some expenditure of resources to repair.
Low	Temporary discomfort, reversible without medical intervention	Very limited or inconveniencing effect on operation	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Negligible	Minor and short term discomfort	No or very limited impact on operation	Will have no impact if threat is realized and exploits vulnerability.

**Table 1.** Risk Probability and Severity Assessment Scales<sup>6</sup>

\*In the case of medical device manufacturers, the focus is on performing risk management during the development of a product in pursuit of regulatory approval to place it on the market; whereas, the risk management performed by hospitals is focused on what happens after the “sale” when networked technologies must operate safety, effectively, and securely as a convergent multi-vendor system-of-systems.

†For example, a patient monitoring network the entire network is considered a regulated medical device in and of its own right and is developed and managed by the manufacturer. See 80001-1:2010, Table C.1 - IT-NETWORK scenarios that can be encountered in a clinical environment.

hazard, during which a cable may be unintentionally disconnected in a patch panel that may result in a delay or non-provision of care. Depending on the specific patient condition, the therapy being provided along with related monitoring, the resulting harm could range from negligible to catastrophic. Depending on the processes and policies enacted around work involving patch panels, the probability may range from improbable to frequent.

Two tables provide examples<sup>§</sup> of tools that are often used to guide the risk analysis process (steps 1 – 4 above). In Table 1, two scales are provided to help determine the probability and severity of a given harm resulting from a hazardous situation.<sup>¶</sup> These are used in steps 3 and 4, respectively.

Once the severity and probability have been estimated, a table similar to Table 2 could help determine whether the identified harm

is severe enough to warrant the design and deployment of risk-control measures, whether additional analysis needs to be performed to determine more precisely the nature of the risk, or whether the hazardous situation represents a significant threat to patient safety, system effectiveness, or data and system security.

The relationship between the risk assessment concepts is summarized in Figure 1, along with the standardized definitions of each key term. Note that it all begins with a complete understanding of the potential hazards and hazardous situations that may occur. A “starter set” of these hazards is included in the 80001 guidance documents included in the reference list; however, as required in the IEC 80001-1:2010 standard, technology providers—both medical device manufacturers and information technology suppliers—are required to identify those

		Unintended Consequence for Security: Effectiveness and Data and System Security	Increasing Probability				
			Improbable	Remote	Occasional	Probable	Frequent
Increasing Severity ↑	Catastrophic						
	High						
	Medium						
	Low						
	Negligible						

<b>Low</b>	Risk is acceptable. Risk has little effect on goals, no additional control measures required.
<b>Moderate</b>	Risk acceptability needs further consideration. Risk has some effect on goals but can be accepted when balanced with benefit. RO must pre-define policies in Risk Management Plan for risks in this level. Policies can include special team reviews (IT, clinical) or review boards, rationales, top management signoff, showing risk has been reduced as low as practicable, etc.
<b>High</b>	Risk to goals is unacceptable, risk must be reduced before Medical IT network can be used, either by reducing likelihood or by reducing severity.

**Table 2.** Risk Acceptability Matrix<sup>7</sup>

<sup>§</sup>Note these are only examples; different variations of these may be created to address changes in care contexts, technologies being managed, etc., and may be updated as experience is gained performing risk assessment activities.

<sup>¶</sup>IEC 80001-2-1:2012, Section 2.1 provides a discussion of the differences between hazards and hazardous situations.



## 80001 Basics: *From Hazards to Harms*

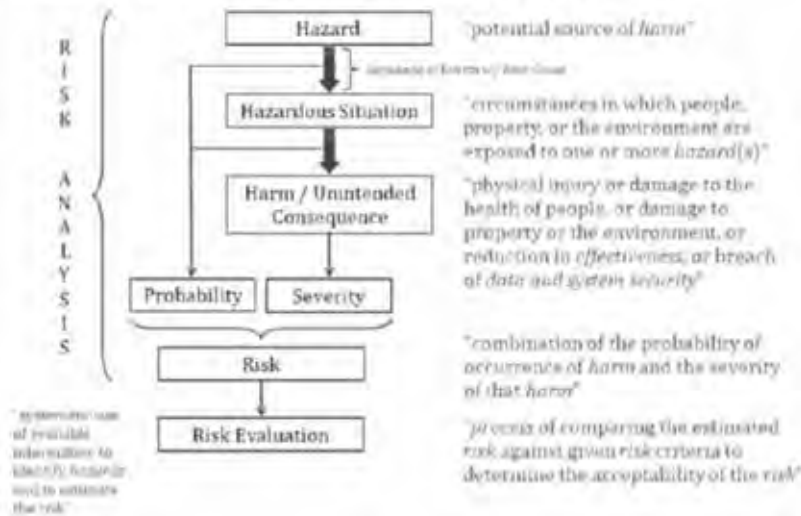


Figure 1. From Hazards to Harms (Taken from AAMI's Getting Started with IEC 80001.)

hazards that must be considered when performing these risk assessment activities.

Risk assessment is just the start. Once it is completed and there is a determination that use of a technology poses significant risks, the focus switches to risk control or mitigation and a final determination as to whether the technology is safe and clinically effective enough to outweigh the risks associated with its use. Details about risk-management activities subsequent to risk assessment are provided in the standards and articles identified in the reference list.

### Starting an 80001-based risk-management program—even the initial risk-assessment activities—has posed a significant challenge to healthcare providers.

#### Starting a Risk-Assessment Program

Starting an 80001-based risk-management program—even the initial risk-assessment activities—has posed a significant challenge to healthcare providers. Some have characterized it as an “unfunded mandate” and even suggested that until the FDA or accreditation organizations require it—or worse, until there is a high-profile catastrophe that could have been averted by risk management—there will be little interest in investing in such a program.

In the meantime, networked technology becomes increasingly interwoven with care delivery on a daily basis, and as a result, the potential for disastrous unintended consequences grows. Short of enacting a comprehensive enterprise-wide program, smaller more manageable projects should be selected to which risk management may be applied. Once these projects are completed, the results may be evaluated, improved, and applied to successive projects, incrementally building a core competency in risk management.

One approach for such a project is illustrated in Figure 2. Data is collected on present capabilities and technology needs of the organization, followed by a determination of readiness to begin the risk management process, both in terms of the needed information to drive the activities as well as competencies and capabilities (e.g., trained personnel, assessment models, and policies).

When the needed information is in place, a risk assessment may be performed to determine the organization's technology vulnerability. This will result in an action plan to both control the identified risks and determine how best to improve the organization's overall maturity in managing its networked technology—establishing benchmarks early on that may be used later to determine progress.

The important point is to get started and not wait until all the conditions are perfect.

In the meantime, the ISO/IEC JWG7 is not resting on its laurels, but is pushing ahead developing guidance on “responsibility agreements” (between technology suppliers and users to lay the foundation for multi-stakeholder collaboration for medical network risk management), risk management of distributed alarm systems, and an 80001 self-assessment model, providing detailed guidance on how to perform readiness assessments, with more in the pipeline.

In an increasingly connected healthcare environment, risk assessment as part of an overall technology management program is emerging as a mission-critical component for all hospitals. The resources and tools are in place today to get started in this important area. Do not let your patients and your ability to provide quality care fall victim to conse-

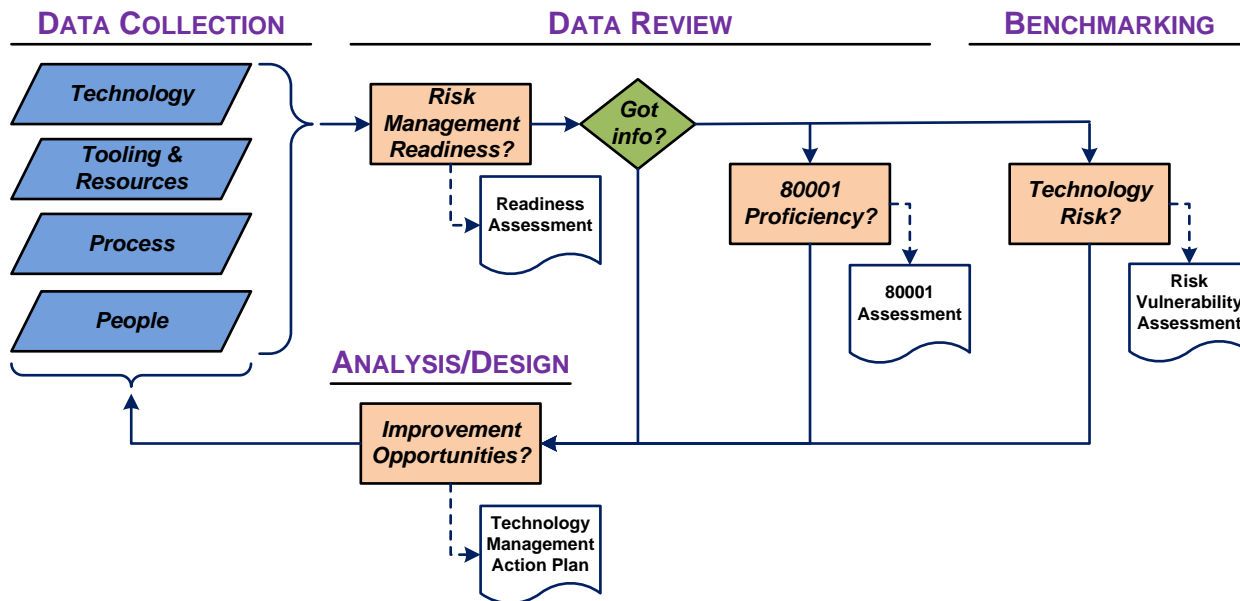


quences that could have been avoided if someone had made the effort to perform the analysis and take appropriate action. ■

## References

1. **The Joint Commission.** Sentinel Event Alert, Issue 42: Safely Implementing Health Information and Converging Technologies. Available at: [www.jointcommission.org/sentinel\\_event\\_alert\\_issue\\_42\\_safely\\_implementing\\_health\\_information\\_and\\_converging\\_technologies/](http://www.jointcommission.org/sentinel_event_alert_issue_42_safely_implementing_health_information_and_converging_technologies/) Posted Dec. 11, 2008. Accessed April 13, 2013.
2. **AAMI.** ANSI/AAMI/ISO 14971:2007/(R)2010, *Medical devices—Application of risk management to medical devices.* Association for the Advancement of Medical Instrumentation. 2007. Arlington, VA.
3. **AAMI.** ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT network incorporating medical devices—Part 1: Roles, responsibilities and activities. Sections 2.9 and 2.8 for definitions of hazard and harm.* Association for the Advancement of Medical Instrumentation. 2010. Arlington, VA.
4. **AAMI.** ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT network incorporating medical devices—Part 1: Roles, responsibilities and activities. Section 2.13 for definition of key properties.* Association for the Advancement of Medical Instrumentation. 2010. Arlington, VA.
5. **AAMI.** ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT network incorporating medical devices—Part 1: Roles, responsibilities and activities. Section 4.4, The 10 Step Process.* Association for the Advancement of Medical Instrumentation. 2010. Arlington, VA.
6. **AAMI.** Understanding & Benefitting from AAMI/IEC 80001-1 (webinar). Presented Jan. 19, 2011. Arlington VA.

## Networked Medical Technology Management Support



**Figure 2.** Technology Management Study Projects Process Model. (Copyright 80001 Experts, LLC. All rights reserved. Used with permission.)

# The Wireless Challenge

## Security and Safety For Medical Devices and Hospitals

Steven D. Baker, Jonathan Knudsen, and D. Mike Ahmadi

### About the Authors



*Steven D. Baker, PhD, is senior principal engineer at Welch Allyn. E-mail: steve.baker@welchallyn.com*



*Jonathan Knudsen is principal security engineer at Codenomicon Ltd. E-mail: jonathan@codenomicon.com*



*D. Mike Ahmadi, CISSP, is global director of business development and medical domain security expert for Codenomicon. E-mail: mike@codenomicon.com*

### Overview

In healthcare, security is often equated with compliance with the Health Insurance Portability and Accountability Act (HIPAA). Many believe that HIPAA compliance is all that is needed. This assumption is grossly inaccurate: Encryption of sensitive information is one part of a much larger picture.

Medical device companies want to be sure to manufacture products that allow a hospital to be HIPAA compliant, while often using the least expensive parts possible to remain price competitive. The minimum HIPAA requirement is, “A covered entity must, in accordance with §164.306... implement a mechanism to encrypt and decrypt electronic protected health information.”<sup>1</sup>

Unfortunately, the simple encryption available in the cheapest wireless solutions is not enough to safeguard medical devices, patient data, and the enterprise network. Wired Equivalent Privacy (WEP) and pre-shared keys (PSKs) used in Wi-Fi Protected Access (WPA/WPA2) can be compromised in a matter of seconds! Some medical devices use proprietary modulation schemes and protocols, but time and again we’ve seen that security through obscurity is never effective. It is far better to use solutions that are tried and tested by researchers (hackers on the good side of the law), such as the Advanced Encryption Standard (AES) algorithm in 802.11 that also meets the encryption requirements for the stringent Federal

Information Processing Standard (FIPS) 140-2 compliance.\*

The software that runs medical devices and the networks that support them impact quality of care and patient safety. Software quality and the process of hardening medical device systems is important for all devices, be they implantable pacemakers, surgical robots, large machines delivering precise doses of life-saving radiation, or the electronic health records systems that must safeguard protected health information (PHI) and the integrity of data that is used for clinical decision-making. Networks are required to support a myriad of wired and wireless, medical, and personal devices. This network support permits improvements in medical device capabilities and improves ease-of-use, but it adds complexity and risks.

Software, devices, and networks can fail accidentally or intentionally. Equipment that fails accidentally is not sufficiently robust, while equipment that fails when deliberately attacked is not sufficiently secure. The consequences attributed to equipment that is not robust and secure range from inconvenience to morbidity to mortality. The software on a medical device must be hardened to make it robust and secure. Software that is not specifically hardened during its development is far more likely to fail when exposed

\*More than just AES is required for FIPS 140-2 compliance.

to the vicissitudes of the real world or malicious attacks.

Recent events, such as the Chinese government's hacking of *The New York Times*<sup>2</sup> and other major U.S. newspapers, help us realize everyone can be a target. As Kevin Mitnick indicated, "I get hired ... to find security holes. Our success rate is 100%; we've always found a hole."<sup>3</sup> The goal of this paper is to help the reader understand some of the common security holes to support commonsense improvements in network security.

## General Concepts

### 1. Always use the strongest authentication and encryption available.

For Wi-Fi, this means WPA2-Enterprise. The WI-FI Alliance only supports WPA2 for new standards. That is, when a new radio goes up for 802.11n certification, it will fail if it supports WPA. It will also fail if it supports WEP,<sup>4</sup> which was quickly exploited and is a great example of failing to use security experts to vet an encryption solution. WPA was developed as an interim solution until hardware support for WPA2 and AES was available. It was never intended to be the long-term security solution and should be avoided as should WEP. (For more information on WEP, WPA, and WPA2, please see the reference list at the end of the article.<sup>5</sup>)

For remote access, including over cellular modems, use a secure tunnel, which can be accomplished through the use of a virtual private network

(VPN) that conforms to National Institute of Standards and Technology (NIST) and/or International Organization for Standardization (ISO) security guidelines.

Regardless of the secure mode of communication deployed, ensure that the system implementation is verified and validated to provide the expected level of security. To use an analogy, using the best ingredients for a gourmet meal doesn't guarantee gourmet taste. In the end, it comes down to the implementation.

**Regardless of the secure mode of communication deployed, ensure that the system implementation is verified and validated to provide the expected level of security.**

### 2. If it is easy to use, it is probably easy to hack.

Some medical offices use consumer-grade routers that ship with no security or in "open" mode to allow quick and easy connections. As a response to this obvious security hole—and primarily intended for consumer devices—Wi-Fi Protected Setup (WPS) was intended to make it easy to securely connect Wi-Fi devices to an access point. The "easy" part works, for both users and hackers, due a hard-coded PIN and poor implementation (it keeps allowing a device to try another PIN after multiple failures).<sup>6</sup> While enterprise-class hardware doesn't automatically solve all the issues, it at least doesn't support this vulnerability.

For some small sites, a hazard analysis may indicate that using WPA2-PSK may be acceptable when mitigations, such as those listed below, are implemented as using a pre-shared key introduces these hazards:

- Vulnerable to a brute-force dictionary attack, particularly when short passphrases are used. Rainbow tables exist for download that contain the pre-computed hash for every passphrase up to 16 characters.
- When an employee with knowledge of the PSK leaves or a device is lost, the key is compromised.

To minimize the risks associated with PSK, use a passphrase of at least 16 characters,

including upper and lower case letters, numbers, and symbols. Change the keys at pre-defined intervals not to exceed six months, when a device is lost or when an employee leaves.

In a large enterprise,

this process is difficult to sustain and is the reason 802.1x EAP-based authentication is preferred in large installations.

### 3. Don't purchase new medical equipment that compromises the network.

There are companies with state-of-the-art medical devices and obsolete security solutions. We ask, "How can one justify putting at risk the entire medical information

technology (IT) network to support equipment that makes the network vulnerable?” Healthcare delivery organizations can push manufacturers to provide secure solutions if requests for quotation (RFQs) have a line-item for WPA2-Enterprise support and only purchasing equipment that does. Even if your network doesn’t yet support WPA2-Enterprise, buy equipment that can support it when your network does.

A technique known as “fuzzing” is a powerful tool for evaluating medical devices as it provides an assessment of associated risk.<sup>†</sup> Reporting fuzzing vulnerabilities to the manufacturer and including a RFQ line item for “fuzzing tests” as part of the quotation process encourages manufacturers to use fuzzing as a part of the software development life cycle, which directly benefits patients and caregivers.

#### 4. Segment off devices that have poor security solutions.

Even if no new, low-security equipment is purchased, with a seven-plus year lifetime for medical devices, many hospitals have legacy equipment that must be on the network. Put these devices on their own virtual area local network (VLAN) separated from the rest of the network by a stateful firewall. Close down the ports to allow only the required traffic types, ports, and IP addresses.

#### 5. Use negative testing to harden software during development.

Typical software development includes a quality assurance (QA) team that finds bugs or coding errors by testing against functional requirements, a form of positive testing. The testers provide valid inputs to the software and

ensure the correct output is produced. For example, one test for an infusion pump might work like this: If I send a command to change the pump rate, is the pump rate set correctly?

Positive testing is important, but it does not prepare devices for exposure to the real world or to attack. Negative testing involves sending various types of nonfunctional inputs to software or hardware and observing the results. This can consist of something as simple as a storm, where a device is bombarded with traffic (which can cause the device to crash), or by fuzzing, which means applying a cleverly constructed input of malformed traffic. Examples of fuzz test cases for the infusion pump include:

- Setting the pump rate to a negative value
- Commanding a pump rate change without providing a value
- Sending an invalid command

Savvy QA teams use automated storm and fuzz tests, allowing detection of more software defects and vulnerabilities than relying on positive testing and resulting in a safer, more secure product.

Robustness testing is crucial to manufacturers who make devices that communicate on a network. Several organizations provide tools that can be used to quickly discover vulnerabilities through negative testing. Such tools, when used with a packet analyzer, allow device manufacturers to check for security flaws during the critical development cycle.

### Security Vulnerabilities

We describe two high-level vulnerability classes, known and unknown, and then provide examples.

Known security vulnerabilities can be exploited when assumptions about the vulnerability not occurring are overstated. Hackers can create security exploits from functional features, known interference, and component-level weaknesses. For example, if a certain interference frequency will disrupt a wireless device, a device manufacturer may reasonably consider that the environment (e.g., a hospital) does not have harmful levels of interference and/or may stipulate that the

**A technique known as “fuzzing” is a powerful tool for evaluating medical devices as it provides an assessment of associated risk.**

**Positive testing is important, but it does not prepare devices for exposure to the real world or to attack. Negative testing involves sending various types of nonfunctional inputs to software or hardware and observing the results.**

<sup>†</sup>Fuzzing should not be performed on equipment in use, or equipment that will be used for patient care.

device cannot be used in environments where the interference exists. An attacker can build a device to generate the known, interfering frequency and deploy it maliciously in a hospital, creating a safety risk or security vulnerability.

Unknown security vulnerabilities are the most challenging to device manufacturers as they generally do not have the engineering cycles to dedicate toward discovering the multitude of ways to misuse a device. In contrast, the security researcher and attacker mindset is focused on how such devices can be misused.

- **Interference-based attacks**—an attacker researches product literature from manufacturers, patent filings, and other sources to learn of an interference issue with a wireless device. A device may have a minor glitch when exposed to a certain type of interference, but an attacker bombarding the device with the known interference causes it to cease communicating. In some cases, the denial of service state allows an attacker to further compromise the system, or possibly use it as a gateway to penetrate further into the network.
- **Malformed traffic attacks**—the essence of how the fuzzing works. A device understands the “grammar” of a communication protocol and expects information that conforms to the protocol. However, if an input varies in minor ways from what is expected, the device may accept the input as fully valid, or may simply let down its guard long enough for malicious traffic to make its way through. This attack method is extremely effective, as most systems cannot be too rigid in what they allow as valid inputs due to the need to permit slight variations in the “rules” to allow for normal, malformed traffic caused by crosstalk on a communication, among other reasons. Allowing small glitches to pass through to permit constant communication of good traffic is essential for reliable service. Attackers attempt to insert malicious packets into this slightly malformed traffic, which may appear as glitches, but are actually known “kill packets.”
- **Misused functionality attacks**—a device has a feature for good purpose that can be exploited. Pacemakers that respond to a query with serial numbers provide an example. This feature can be used by a healthcare provider when the serial number of a device is unknown, but is required to send a command. Serial number protection ensures the command only goes to the intended device. However, an attacker may use the query feature to discover devices and then send malicious commands to the devices, or malformed traffic that causes the device to go into an unsafe or denial of service state.<sup>7</sup>

## Conclusions

Recent medical device hacking incidents illustrate that there is room for safety improvement that may come from negative testing. Every network is susceptible, in part due to networked device vulnerabilities. Following the guidance we’ve outlined

will help raise the security bar for networks and devices, but each healthcare delivery organization (and medical device manufacturer) should consider its risk profile and complete a risk analysis<sup>8,9</sup> to understand where vulnerabilities may exist. For larger hospitals, the decision may be made to retire obsolete devices that don’t support WPA2-Enterprise, install IDS/IPS gear that identifies network attacks, and hire a security research consultant for fuzzing-test analysis. On the other hand, a small clinic in a remote area with only a few devices may deem that using WPA2-PSK is acceptable. ■

## References

1. **Pham T.** Encrypting Data to Meet HIPAA Compliance. OT Blog. Available at: <http://resource.onlinetech.com/encrypting-data-to-meet-hipaa-compliance/>. Posted Dec. 7, 2011. Accessed April 10, 2013.
2. **Perloth N.** Hackers in China Attacked The Times for Last 4 Months. *The New York Times*. Available at: [www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all](http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all). Published Jan. 30, 2013. Accessed April 10, 2013.
3. **Mitnick K.** BrainyQuote. Available at: <http://www.brainyquote.com/quotes/quotes/k/kevinmitni469471.html>. Accessed April 10, 2013.
4. **The State of Wi-Fi Security.** The Wi-Fi Alliance. Available at: [www.wi-fi.org/knowledge-center/white-papers/state-wi-fi%20AE-security-wi-fi-certified%2084%A2-wpa2%2084%A2-delivers-advanced](http://www.wi-fi.org/knowledge-center/white-papers/state-wi-fi%20AE-security-wi-fi-certified%2084%A2-wpa2%2084%A2-delivers-advanced). Accessed April 10, 2013.
5. **Ibid.**
6. **Gallagher S.** Researchers Publish Open-Source Tool for Hacking Wi-Fi Protected Setup. *ARS Technica*. Available at: <http://arstechnica.com/business/2011/12/researchers-publish-open-source-tool-for-hacking-wifi-protected-setup/>. Posted Dec. 30, 2011. Accessed April 10, 2013.
7. **Kirk J.** Pacemaker Hack Can Deliver Deadly 830-Volt Jolt. *Computerworld*. Available at: [www.computerworld.com/s/article/9232477/Pacemaker\\_hack\\_can\\_deliver\\_deadly\\_830\\_volt\\_jolt](http://www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt). Posted Oct. 17, 2012. Accessed April 10, 2013.
8. **AAMI.** ANSI/AAMI/IEC 8001-1:2010, *Application of risk management for IT networks incorporating medical devices—Part 1: Roles, responsibilities and activities*. Association for the Advancement of Medical Instrumentation. 2010. Arlington, VA.
9. **AAMI.** ANSI/AAMI/ISO 14971:2007/(R)2010, *Medical devices—Application of risk management to medical devices*. Association for the Advancement of Medical Instrumentation. 2007. Arlington, VA.



# The Wireless Challenge

## Understanding the Wireless Spectrum in a Healthcare Facility

Richard Swim

### About the Author



*Richard Swim, CLES, MCSE, is a team leader of Clinical Technology at Baylor Health Care System in Dallas. E-mail:*

*Richards@BaylorHealth.edu*

Air. There's so much of it out there. There must be plenty of space for everything, especially those little wireless signals from medical devices. But that's not the case when physics dictates the amount of data and waveforms that can be transported via electromagnetic waves. There's only so much space for radio waves to coexist and not cause interference between devices. Management of this airspace in the healthcare environment is a requirement in order for medical devices to be used in a safe and effective manner.

Beginning in 1934, the Federal Communications Commission (FCC) was empowered with regulating interstate and international communications. Part of its responsibility is

managing the electromagnetic spectrum needed by wireless devices to communicate. The wireless spectrum is divided up in blocks of frequencies to support different purposes. The majority of medical equipment is communicating primarily in four of these blocks. Most wireless patient monitoring systems communicate on 608-614 MHz, the 1.4 GHz region, and some manufacturers use 2.4 and 5.8 GHz. There are clinical systems that may use

frequencies around 450 and 900 MHz for associated system devices. Examples of these nonmedical devices in hospital settings include pagers used with patient monitoring systems; pagers handed out to visitors and family; two-way portable radios used by hospital staff and law enforcement; and other systems that a visitor or patient might bring in.

### The Role of a Spectrum Manager

Our task in the healthcare technology management (HTM) arena is to help manage the use of the wireless spectrum in a manner in which one device does not unintentionally affect the performance of another. A challenging frequency block to manage is the 2.4 GHz range, in which many devices operate for medical, enterprise, and consumer use. The 802.11b and 802.11g wireless protocol operating on 2.4 GHz is in wide use by computers, in-house telephones, infusion pumps, electrocardiogram (EKG) carts, pulse oximeters, and some physiological monitoring systems. There are magnetic resonance imaging (MRI) patient monitoring and MRI infusion pump systems designed to communicate between the magnet field and the control room on stand-alone 2.4 GHz systems. These stand-alone wireless networks may compete with the hospital's enterprise wireless network.

Identifying a wireless spectrum manager for your healthcare system is important. Our organization manages a wireless frequency



inventory divided into worksheets for each of our geographic facilities. This inventory is intended to record every type of device that is using wireless communication on a campus. It provides a good starting point when there is a question around the purchase of a device to avoid possible conflicts with existing installations. In this inventory, we have rows documenting frequency, RF generator, power, comments, end user contact, device vendor, vendor contact, and other telephone and e-mail information for each existing RF device on campus. We even inventoried local television station frequencies back when the patient monitoring telemetry systems shared those same airwaves. We had to pick an unused frequency on which to operate our telemetry (television channels 7-13 174-216 MHz and 14-46 470-668 MHz).

### The ‘Baylor Event’

Many will remember the related “Baylor Event” in 1998 that ultimately led to the creation of the protected Wireless Medical Telemetry Service (WMTS) bands. Over a weekend of trying to figure out why several of our telemetry floors lost all monitoring, we finally determined that a local television station was testing their new digital television transmitter on the same frequency that we were operating telemetry. This event and similar situations around the nation led to the creation of dedicated medical device wireless frequencies, rather than relying on locally unused channels. A completely inoperable telemetry system is one example of devices conflicting with each other. There are many devices, such as cellphones, that can possibly interfere with each other at low power and close proximity. Maintaining an inventory of radio frequency (RF) generators for your facility and knowing about other frequencies in use near your facility can help avoid a problem.

When problems do arise, we just can’t throw our hands up in despair or point fingers at each other’s teams. There must be collaboration from the start. The HTM wireless spectrum manager should communicate with the hospital information technology (IT) network team during planning for equipment procurement. Such interaction will pay off—achieving the hospital’s objective for each

**Identifying a wireless spectrum manager for your healthcare system is important. Our organization manages a wireless frequency inventory divided into worksheets for each of our geographic facilities.**

system coexisting with effective wireless communications. In my organization, this communication is made easier since HTM reports through Information Services.

Rather than having to react to a situation in which a medical device or computing system is not working as desired, it is much better to plan for implementation prior to purchase. Creating a pre-purchase approval process that guides networked and wireless devices through appropriate staff in the HTM and IT groups will identify conflicts in design between systems. Even though most medical equipment designs have been in place much longer than today’s wireless computing, wireless patient monitoring is relatively new—other than traditional telemetry. Introducing a stand-alone medical device wireless network may conflict with the hospital’s enterprise network as there may not be enough available channels for the different wireless networks to coexist. When manufacturers suggest such setups, work with them to place their devices on the hospital network so that a stand-alone wireless access point is not discovered after the fact. If incorporating the vendor’s system into the enterprise network is not possible, facilitate interaction between the vendor and the network team to come to a possible solution for both wireless systems to coexist.

**When problems do arise, we just can’t throw our hands up in despair or point fingers at each other’s teams. There must be collaboration from the start.**

### New Developments

The WMTS bands were created in 2000 and protected medical telemetry lived happily ever after, or so the story goes. But there is an insatiable consumer demand for wireless devices independent of the healthcare setting. In February 2012, the FCC gave notice that the 608-614 band may be needed for broadband purposes. This reallocation would require healthcare facilities operating in the 608-614 band to replace their patient

## For More Information

A chart showing U.S. frequency allocations: [www.ntia.doc.gov/files/ntia/publications/spectrum\\_wall\\_chart\\_aug2011.pdf](http://www.ntia.doc.gov/files/ntia/publications/spectrum_wall_chart_aug2011.pdf)

FCC background about the Wireless Medical Telemetry Service (WMTS): [www.fcc.gov/encyclopedia/wireless-medical-telemetry-service-wmts](http://www.fcc.gov/encyclopedia/wireless-medical-telemetry-service-wmts)

The American Society for Healthcare Engineering and its WMTS registration process: [www.ashe.org/resources/WMTS](http://www.ashe.org/resources/WMTS)

**This situation is very dynamic, and HTM professionals are advised to stay informed in order to properly plan for long-term wireless equipment management.**

monitoring systems by 2020. But, based on compelling data from the WMTS database managed by the American Society for Healthcare Engineering (ASHE), the FCC tentatively concluded in November 2012 that systems operating in the 608-614 band may not have to relocate. ASHE estimated that it would cost up to \$1.4 billion for healthcare facilities to implement replacement systems. The \$300 million that was slated to help facilities migrate away from the channel 37 WMTS band would not meet the demand.

This regulatory back-and-forth demonstrates on a large scale the value of understanding the scope of wireless systems in operation. Healthcare facility wireless spectrum managers must understand what they have operating in the WMTS frequencies and register these through ASHE. Registration is a requirement of the FCC rules for systems installed utilizing WMTS bands. The FCC 608-614 MHz band reallocation proposal and the subsequent tentative reversal show another advantage of registering your WMTS systems. This situation is very dynamic, and HTM professionals should stay informed in order to properly plan for long-term wireless equipment management.

There have been other similar frequency reallocations over the years that have affected medical devices. Some telemetry systems operated in the same bands around 450MHz that public service and private radio operators transmitted. The FCC changed the rules in this band, allowing higher-powered devices to operate. Medical device owners and manufacturers had to change their systems to operate outside of the private land mobile radio system (PLMRS) bands. The FCC did not approve medical devices operating in this frequency after 2002.

Another PLMRS-related change may affect pagers associated with medical devices. Effective Jan. 1, 2013, devices operating in the 150-512 MHz radio bands were required to change their technology to operate in a more efficient 12.5 kHz range (originally 25 kHz). Some devices may be able to be reprogrammed to meet this new narrow banding specification, but others may have to be

replaced. A complication of this change is the potential reduction in power of paging systems after the narrow banding change. This issue may require redesign of local nursing floor paging systems associated with patient monitoring installations.

A new frequency “kid on the block” is the medical body area network (MBAN), which supports wearable sensors. MBANs will operate in the range of 2360 – 2400 MHz. Healthcare providers will have to register and coordinate the use of this equipment. This registration cannot be completed until the FCC appoints a frequency coordinator to manage the operations. Manufacturers are urging the FCC to have its MBAN coordination system in place by June 2013.

In summary, it's important to understand the radio frequencies within which your facility's medical devices operate, and the coordination that is required to avoid issues with their operation. Development of a wireless spectrum inventory and processes that encourage communication between all RF users in a facility will help systems operate effectively. ■

# 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**

## A Free Resource

This list comes from the AAMI publication, *Healthcare Technology in a Wireless World*. You can download a free copy of that publication at [www.aami.org/wireless/2012\\_Wireless\\_Workshop\\_publication.pdf](http://www.aami.org/wireless/2012_Wireless_Workshop_publication.pdf).

# Wireless Networking Risk Management Case Studies

## Case Study

### Managing Conflicting Requirements

**Project:** A hospital chooses to deploy 802.11-based active RF-ID tags to support equipment location and tracking

**Problem:** The clinical staff begins to complain about loss of data on 802.11-based patient monitoring systems.

**Cause:** The biomedical department contacts the manufacturer whose engineers prove that the APs are not acknowledging data even when a sniffer successfully receives the data. When asset tracking is disabled, the problem goes away. The AP vendor changes a configuration to “fix” the issue, but asset tracking doesn’t update regularly. The solution was to install separate APs for the sole function of asset tracking.

**Recommended Practice:** With 80001, the risk manager would have queried the AP manufacturer about side effects of asset tracking, learned it requires the APs to implement off-channel scanning, and determined this was unacceptable. Hospital would learn the true cost of the installation up front.

–Steven Baker and Ken Fuchs

## Case Study

### Managing Replacement of Potentially Interfering Equipment

**Project:** A hospital replaces one of two industrial microwave ovens

**Problem:** Several months later, the clinicians report issues with 802.11-based patient monitoring running in the 2.4 GHz band.

**Cause:** Investigation discovers the patient-monitoring issues began months before they were reported and traced to the time of the replacement of the microwave ovens. Before replacement, the ovens operated in phase. After the replacement, they did not run in phase. Solution was to add additional APs at larger distance from the interfering microwave ovens.

**Recommended Practice:** IEC 80001-1 wireless TR recommends cataloging all RF sources and periodic reviews. This database and timely reviews could be used to determine that the duty cycle of RFI increased and help determine root cause faster.

–Steven Baker and Ken Fuchs

## Case Study

### Security Hole

**Project:** Hospital installs some new wireless medical devices on its 802.11b/g network

**Problem:** War driver hacks into the wireless network and has access to the entire hospital network and compromises the security of servers which contain sensitive medical data.

**Cause:** After investigating the issue, IT realizes that the new devices only support WEP encryption which allowed the hacker to use a widely available tool that deciphered the WEP key after only a few minutes. Solution was to keep Wi-Fi devices with weak encryption on a separate ESSID/VLAN while using a firewall to quarantine this traffic.

**Recommended Practice:** An 80001 risk management analysis would have uncovered this risk to the network and the hospital would have considered different ways of managing this risk such as installing a firewall or installing a separate wireless network dedicated to the medical device (not always possible). Sometimes the best answer is to remain wired until security issues are resolved.

–Steven Baker and Ken Fuchs



# Wireless Networking Risk Management Case Studies

## Case Study

### Managing Infrastructure Firmware Updates

**Project:** IT department upgrades the firmware level on their wireless controllers and APs based on the recommendation of their wireless infrastructure manufacturer

**Problem:** Clinicians notice periodic loss of data

**Cause:** Investigation reveals the updated firmware has the APs changing channels as fast as every 10 seconds, forcing clients to roam unexpectedly. The wireless infrastructure manufacturer indicates that channel switch announcement should be enabled, but that makes things even worse. Further, investigation shows the APs send a de-auth packet when clients re-associate after the channel change. Solution was to increase the minimum channel dwell time.

**Recommended Practice:** Applying 80001, the risk manager would have included the clinical team in the risk analysis and preferably indicated the risk of upgrading was high and should only be done after clinical validation testing is complete. The AP vendor would have been asked and disclosed the changes in function and these would be presented to the medical device manufacturers for review.

—Steven Baker and Ken Fuchs

## Case Study

### Managing Wireless Infrastructure Firmware Upgrades

**Project:** IT receives a security advisory from the infrastructure manufacturer and immediately schedules an upgrade for the controller and AP firmware.

**Problem:** Nurses report that their devices are neither communicating with central stations nor IT applications.

**Cause:** During the upgrade time of 30 minutes, the Wi-Fi network and all wireless communication are unavailable. The nursing staff was not apprised of the change.

**Recommended Practice:** Systems supporting clinical systems are never taken offline without notice. The security risk of not upgrading would be compared against the clinical risk of a down network. Prior to the upgrade, confirmation of verification testing for compatibility with all critical systems should be made, or at least assess the risk of not having that testing. Part of the infrastructure purchase review would have included the risks associated with firmware upgrade. A 30-minute upgrade solution would likely require a staged upgrade and perhaps a different solution with faster upgrade would have been selected.

—Steven Baker and Ken Fuchs

## Case Study

### Managing Network Security Changes

**Project:** The IT department implements both an Intrusion Prevention System (IPS) and an Intrusion Detection System (IDS) as part of a plan to improve network security, but doesn't include clinical devices in the listing of known, approved devices.

**Problem:** Over time, clinical devices show difficulty roaming. Eventually, these devices will connect to only two APs on the entire floor.

**Cause:** The medical device manufacturer (MDM) is contacted to resolve the issue and discovers that the two APs to which the devices connect are the only APs that respond to authentication requests. The MDM eventually discovers IPS/IDS was implemented just prior to the roaming failures. Solution was to add the clinical devices to the approved devices list.

**Recommended Practice:** Following the guidance of 80001, the hospital would have a listing of all intentional RF radiators, which would have also included the clinical devices. Additionally, the clinical engineering department would have been apprised of the change.

—Steven Baker and Ken Fuchs

Originally Published in the Fall 2011 *Horizons*  
Association for the Advancement of Medical Instrumentation (AAMI)  
[www.aami.org](http://www.aami.org)

# Wireless Networking Risk Management Case Studies

## Case Study

### Managing Wireless Infrastructure Features

**Project:** Wireless infrastructure vendor convinces IT to start using the automated radio manager feature to manage the power levels and channel selection of their APs

**Problem:** Nurses start to notice that the waveforms from their 802.11 based wireless devices have gaps.

**Cause:** The MDM traces the gaps back to the radio manager feature as this puts the APs into an offline state to scan other channels for short periods of time, during which real-time data are not received. The MDM found this problem during verification testing and developed a solution with the AP manufacturer to hold off the scanning, but hold-off feature was not enabled.

**Recommended Practice:** The potential of features such as rogue AP detection or automatic channel and power allocation to create issues for medical devices is well known and covered in the IEC 80001 Wireless TR. A risk analysis should be performed to learn the side effects of using features before implementing those features.

–Steven Baker and Ken Fuchs

## Case Study

### Massager Breaks Telemetry System

**Project:** New foot massager is purchased

**Problem:** VHF telemetry system fails intermittently for patients near the nurse station.

**Cause:** Analysis found the failures correlated with use of the foot massager that was located at the nurse station and that the massager was not working properly. It was emitting considerable electro-magnetic interference in the WMTS (FCC allocated band for medical telemetry) band that the telemetry system was using. Solution was to replace the foot massager.

**Recommended Practice:** While it would be difficult to prevent this situation from occurring, the hospital should maintain a list of emitters and their baseline spectrums. If one of these devices fails in such a way that its emissions increase, the biomed department can more easily find the potential culprits.

–Steven Baker and Ken Fuchs

## Case Study

### Managing Changes in Network Configuration

**Project:** A hospital IT department changes network topology from a flat network to having different subnets in each building. They enable IP mobility to support roaming across subnets.

**Problem:** Clinicians notice data loss, particularly for ambulatory patients, and the MDM is asked to investigate.

**Cause:** The MDM network specialists discover a nonvalidated configuration. They and the infrastructure provider test and find that EAP-authenticated fast roaming does not work when IP mobility is enabled. Solution was to disable IP mobility until the infrastructure vendor fixes the bug and MDM validates the new build.

**Recommended Practice:** Under 80001-1, the network change would be documented and the clinical department apprised of the change. A risk analysis would indicate that the configuration isn't supported by the MDD. If the hospital chooses to go forward with the change, a recovery plan would be in place, and upon detection of degraded performance, would have been used.

–Steven Baker and Ken Fuchs

Originally Published in the Fall 2011 *Horizons*  
Association for the Advancement of Medical Instrumentation (AAMI)  
[www.aami.org](http://www.aami.org)

# Wireless Networking Risk Management Case Studies

## Case Study

### Managing Interference

**Project:** A hospital CIO mandates use of a distributed antenna system (DAS) to support enterprise-wide wireless VoIP (i.e., wireless telephony) that is used to relay clinical alarms

**Problem:** After installation, staff complains that the wireless phone system is not working well on one floor and alarms are not being reliably transmitted. Further, there was no escalation of alarms.

**Cause:** The IT department discovers that the biomedical department has a 2.4 GHz Frequency Hopping Spread Spectrum (FHSS) system installed. Moreover, the DAS runs adjacent to the FHSS Access Points (APs) and the DAS efficiently conveys all the FHSS transmissions to the 802.11b/g APs. Solution was to move the DAS to a distance of 3-m from the FHSS APs.

**Recommended Practice:** By following 80001, the CIO would consult with the risk manager before making such a mandate. The risk manager would have a list of all intentional radiators and alert the DAS installation team to work with the telemetry system manufacturer to mitigate interference risk. The DAS would have been installed with 3-meter separation from the FHSS APs and not presented issues. The patient risk due to no alarm escalation would have been noted and mitigated if the risk level was too high.

–Steven Baker and Ken Fuchs

## Case Study

### Too Much of a Good Thing

**Project:** Hospital installed a wireless network over multiple floors. Over time the number of access points increased and the power level on some APs was also increased to improve coverage.

**Problem:** After some time, users reported that the wireless network seemed “slow” and devices sometimes took a long time to connect. Investigation revealed that distribution of patient alarm conditions was unreliable.

**Cause:** IT investigated and found that it did not have current documentation of the wireless infrastructure. After updating the map of AP locations and configurations they found that the AP density was too high, especially given the power level settings. This resulted in a situation where the amount of beacon traffic was so high that normal communications were severely affected, despite all the APs having a Wi-Fi certification. Solution was to decrease transmit power and AP density.

**Recommended Practice:** According to the best practices outlined in IEC 80001, the wireless network is maintained under configuration control. Any changes are analyzed carefully and tested if possible to ensure that the integrity and performance of the network is not degraded.

–Steven Baker and Ken Fuchs

Originally Published in the Fall 2011 *Horizons*  
Association for the Advancement of Medical Instrumentation (AAMI)  
[www.aami.org](http://www.aami.org)

# 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.*



# Wireless Resources and Additional Reading List

## AAMI:

ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT Networks incorporating medical devices—Part 1: Roles, responsibilities and activities*: [www.aami.org/publications/standards/80001.html](http://www.aami.org/publications/standards/80001.html)

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 application and examples*: <http://my.aami.org/store/SearchResults.aspx?searchterm=80001-2-1%3a2012&searchoption=ALL>

ANSI/AAMI/IEC TIR 80001-2-2:2012, *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*: <http://my.aami.org/store/SearchResults.aspx?searchterm=80001-2-2%3a2012&searchoption=ALL>

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*: <http://my.aami.org/store/SearchResults.aspx?searchterm=80001-2-3%3a2012&searchoption=ALL>

ANSI/AAMI/IEC TIR 80001-2-4:2012, *Application of risk management for IT-networks incorporating medical devices—Part 2-4: General implementation guidance for healthcare delivery organizations*: <http://my.aami.org/store/SearchResults.aspx?searchterm=80001-2-4%3a2012&searchoption=ALL>

Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks: [www.aami.org/publications/Books/80001-GS.html](http://www.aami.org/publications/Books/80001-GS.html)

Healthcare Technology in a Wireless World: [www.aami.org/wireless/2012\\_Wireless\\_Workshop\\_publication.pdf](http://www.aami.org/wireless/2012_Wireless_Workshop_publication.pdf)

"Managing Medical Devices on the IT Network," *Horizons*, Fall 2011.

## FCC:

FCC Encyclopedia: Wireless Medical Telemetry: [www.fcc.gov/encyclopedia/wireless-medical-telemetry-service-wmts](http://www.fcc.gov/encyclopedia/wireless-medical-telemetry-service-wmts)

FCC Rule: Medical Area Body Network: [http://op.bna.com/mdw.nsf/id/plon-8xzshs/\\$File/FCCrule.pdf](http://op.bna.com/mdw.nsf/id/plon-8xzshs/$File/FCCrule.pdf)

Spectrum Dashboard: <http://reboot.fcc.gov/spectrumdashboard/searchSpectrum.seam>

## FDA:

"Draft Guidance for Industry and Food and Drug Administration Staff – Mobile Medical Applications," FDA: [www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf](http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf)

"Medical Device Use-Safety: Incorporating Human Factors Engineering into Risk Management": [www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm259748.htm](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm259748.htm) (draft guidance issued 2011; no final document as of summer 2013).

"Cybersecurity for Medical Devices and Hospital Networks," FDA Safety Communication, June 17, 2013: [www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm357090.htm](http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm357090.htm)

"Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff," June 14, 2013: [www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm)

## IEEE:

Baker, Steven D. and David D. Hoglund. "Medical Grade, Mission Critical Wireless Networks," *IEEE EMB Magazine*, March/April 2008.

IEEE 802.11 Wireless Local Area Networks: The Working Group for WLAN Standards. [www.ieee802.org/11/](http://www.ieee802.org/11/)

## NIST:

NIST Main Website: [www.nist.gov/index.html](http://www.nist.gov/index.html)

NIST Computer Security Division: <http://csrc.nist.gov/>

NIST Computer Security Publications: <http://csrc.nist.gov/publications/PubsSPs.html>

NIST Electronics & Telecommunications Portal – Overview: [www.nist.gov/electronics-and-telecommunications-portal.cfm](http://www.nist.gov/electronics-and-telecommunications-portal.cfm)

NIST Health Information Technology: [www.nist.gov/healthcare/](http://www.nist.gov/healthcare/)

NIST Information Technology Portal: [www.nist.gov/information-technology-portal.cfm](http://www.nist.gov/information-technology-portal.cfm)

NIST Information Technology Telecommunications/Wireless Portal: [www.nist.gov/telecommunications-wireless-portal.cfm](http://www.nist.gov/telecommunications-wireless-portal.cfm)

"Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," NIST: <http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf>

## NTIA:

United States Frequency Allocations: [www.ntia.doc.gov/files/ntia/publications/spectrum\\_wall\\_chart\\_aug2011.pdf](http://www.ntia.doc.gov/files/ntia/publications/spectrum_wall_chart_aug2011.pdf)

## Deeper Guides:

ARRL: [www.arrl.org/college-students-and-educators](http://www.arrl.org/college-students-and-educators)

*IEEC 802.11 Handbook: A Designer's Companion (IEEE Standards Wireless Networks)*. Available for purchase at: [www.amazon.com/The-IEEE-802-11-Handbook-Designers/dp/0738144495](http://www.amazon.com/The-IEEE-802-11-Handbook-Designers/dp/0738144495)

## WiFi Specific:

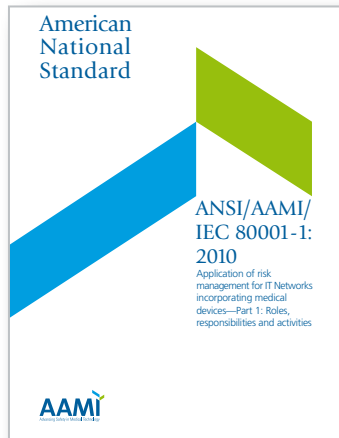
Certified Wireless Network Professional: [www.cwnp.com/](http://www.cwnp.com/)

"Wi-Fi in Healthcare: Improving the user experience for connected hospital applications and devices," WiFi Alliance: <https://www.wi-fi.org/knowledge-center/white-papers/wi-fi%C2%AE-healthcare-improving-user-experience-connected-hospital>

"Wi-Fi in Healthcare: Security Solutions for Hospital Wi-Fi Networks," WiFi Alliance: [www.wi-fi.org/sites/default/files/uploads/files/wp\\_201202\\_Wi-Fi\\_Security\\_for\\_Hospital\\_Networks-Final.pdf](http://www.wi-fi.org/sites/default/files/uploads/files/wp_201202_Wi-Fi_Security_for_Hospital_Networks-Final.pdf)

*If you are reading this list in a print version, you may wish to go to [INSERT LINK] for direct links to these electronic resources.*

# 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 \$120 / AAMI member \$60**

**TIR80001-2-1:2012**, *Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples*

**Order Code: 800010201 or 800010201-PDF**  
**List \$130 / AAMI member \$65**

**TIR80001-2-2:2012**, *Part 2-2: Guidance for the communication of medical device security needs, risks and controls*

**Order Code: 800010202 or 800010202-PDF**  
**List \$130 / AAMI member \$65**

**TIR80001-2-3:2012**, *Part 2-3: Guidance for wireless networks*

**Order Code: 800010203 or 800010203-PDF**  
**List \$120 / AAMI member \$60**

**TIR80001-2-4:2012**, *Part 2-4: General implementation guidance for healthcare delivery organizations*

**Order Code: 800010204 or 800010204-PDF**  
**List \$100 / AAMI member \$50**

**Order your Copy Today!**  
**Call +1-877-249-8226**  
**Visit <http://my.aami.org/store>**



# Move Your Healthcare Technology Career Forward

Education  
News  
Medical Device Standards

Career Growth  
Networking  
Leadership

## Join AAMI and receive:

- Subscriptions to AAMI publications;
- Opportunities to serve on AAMI committees;
- Access to listserves and members-only content on aami.org;
- Discounts on AAMI products and educational offerings;
- Free posting of your resume and 50% discount on online job postings;
- Networking events;
- and much more.

## Attention Students and New Professionals!

Receive discounted membership dues!  
Reference the Individual Membership Application for more information.

**Joining is Easy!  
Become a Member**

**[www.aami.org/membership](http://www.aami.org/membership)**