The Medical Connectivity FAQs

AAMI

Advancing Safety in Health Technology

About AAMI

AAMI is a is a diverse community of more than 9,000 professionals united by one important mission—the development, management, and use of safe and effective health technology. AAMI is the primary source of consensus standards, both national and international, for the medical device industry, as well as practical information, support, and guidance for healthcare technology and sterilization professionals.

Published by
AAMI
901 N. Glebe Road, Suite 300
Arlington, VA 22203
www.aami.org

The Medical Connectivity FAQs

Table of Contents

Introduction

AAMI's Wireless Strategy Task Force (WSTF) created the initial Wireless FAQs in 2014 to address the answers to frequently asked questions (FAQs) regarding wireless issues in the healthcare environment. As technology has advanced and more devices are being placed on the wireless infrastructure, new challenges have emerged. We have developed an updated version, and this document is intended to help healthcare technology management (HTM), information technology (IT), and facilities management professionals understand the state of wireless tools and technologies, their use in healthcare, and how they can best be managed given the disparate roles and responsibilities. A goal of this document is to help HTM and IT professionals improve mutual understanding of their roles and responsibilities and how to best collaborate to ensure effective management of the environment. We hope this compilation of FAQs leads to enhanced cooperation through information sharing about tools and techniques, problem solving strategies, and understanding what the differences are between these critical roles in healthcare.

We give firm answers to purely informational questions. However, for guidance questions, there is no one right or wrong answer. The goal is to provide information and pointers for the reader to make an informed decision.

AAMI would like to acknowledge the efforts of the Wireless Strategy Task Force for the work in updating the FAQs document, including: Steve Baker, PhD, who served as editor, and William Salzstein, Travis Ruthig, Ali Youssef, Rick Hampton, Paul Sherman, Matt Pekarske, Peter Thornycroft, Shawn Jackman, Calvin Sproul, Phil Raymond, Maggie Berkey, and Mark Heston.

In 2019, the Wireless Strategy Task Force was integrated into the Health Technology Alliance (HTA), a partnership between the Association for the Advancement of Medical Instrumentation (AAMI), the Healthcare Information and Management Systems Society (HIMSS), and the American College of Clinical Engineering (ACCE). HTA provides a forum for collaboration among HTM, healthcare IT, and healthcare informatics professionals, as well as others in the broader healthcare community who are dedicated to the promotion of healthcare quality, safety, efficacy, and efficiency through better uses of technology.

To learn more, visit www.healthtechnologyalliance.org.

Disclaimer: Mention of specific products and materials is based on experience of the team of authors and reviews and does not constitute any endorsement by AAMI.

General Questions

1. Wireless support has been added to my responsibilities, and I don't know anything about it. Where can I go to learn?

Hospitals typically use multiple wireless solutions for communication, such as Wi-Fi, Wireless Medical Telemetry Service (WMTS), cellular, Bluetooth® wireless technology, and also for location and asset tracking. In this document, "wireless" includes any communication that doesn't depend on a physical wire between devices. Wireless expertise is gained over time and the topic is sufficiently broad to require a focused team approach.

To start learning about Wi-Fi networking, read *Wireless Networks for Dummies*[1], followed by the *CWNA Certified Wireless Networks Administrator Official Study Guide*[2], and then take the training class. Many wireless vendors have good online seminars, training, white papers, configuration guides, and documentation that can help you get started. "Learning Wireless LAN Technologies," available from wlanpros.com, has some good methods for learning.[3]

Work with your IT group to learn and understand your hospital's wireless architecture via a readable network drawing. A network diagram really is worth 1,000 words, or more! Doing this will help you understand how controllers and access points (APs) are connected physically and their current locations.

For general understanding of how RF (wireless communication) works, consider some of the products available from the Amateur Radio Relay League (ARRL), which has an immense catalogue[4], in addition to the specific items in the list below:

- ARRL's *Antenna Physics: An Introduction*[5]
- ARRL's *Propagation and Radio Science*[6]
- AAMI's "HTM Resources Page"[7]
- AAMI's *Going Wireless* publication[8]
- *Basic Radio: Understanding the Key Building Blocks* by Joel Hallas[9]
- *Basic Communications Electronics* by Jack Hudson and Jerry Luecke[10]
- National Instruments web page "RF and Communications Fundamentals"[11]
- Maxim Integrated's *RF Basics*[12]
- "Bluetooth Technology: Topology Options" web page[13]
- Prominent wireless blogs including *Revolution Wi-Fi*[14], *wirednot*[15], and *Wireless LAN Professionals*[16]

More advanced understanding of wireless local area networks (WLANs), including architecture, is covered in *A Guide to the Wireless Engineering Body of Knowledge*, edited by Andrzej Jajszczyk.[17]

2. What wireless systems and technologies are typically found in a hospital?

The list of wireless technologies below includes those either already established in the healthcare environment or currently making inroads. You should be aware of, if not familiar with, each of these. Note that this list is *not* exhaustive.

- Bluetooth
- Cellular
- Long-Term Evolution (LTE)
- Long Range (LoRa)
- Medical Device Radiocommunications Service (MedRadio), including Medical Body Area Networks (MBANs)
- Medical Implant Communication Service (MICS)
- Near-field communication (NFC; 13.56 MHz)
- Radio frequency identification (RFID)
  - 125 KHz, 134 KHz
  - 13.56 MHz
  - 433 MHz
  - 900–915 MHz (RAIN RFID [RAdio frequency IdentificatioN] for medical unique device identification)
- "TV white space"
- Two-way radios
- Wi-Fi
- Wireless Medical Telemetry Service (WMTS)
- Ultra-wideband (UWB)
- Zigbee

3. Are personal wireless devices (e.g., phones, iPads, etc.) in a hospital a problem?

Medical device manufacturers (MDMs) test to several standards and are held accountable for ensuring that their products are safe and effective, while personal consumer devices are not. Personal wireless devices can present various issues and prudent institutions should have a strategic plan and a security policy and framework allowing for their use that protects patient data and the clinical networks.

We will consider three areas: *guest* (patient, family) personal devices, *clinician* personal devices, and *clinician* bring your own devices (BYODs), where the clinician's personal device is used in a clinical role. For each of these areas, the risk topics include security and interference.

Risk mitigation plans and policies should consider how a device might allow breaching of network security, result in a HIPAA (Health Insurance Portability and Accountability Act) violation, and/or compromise operation for medical devices.

For guest personal devices, there is little control other than providing a Wi-Fi connection, such as captive portal, to provide an Internet connection with no access to the hospital network. The terms and conditions of use might include requests to respect privacy of other patients in the hospital.

Assuming the clinicians carry personal devices that are not allowed for clinical use, these policies should define whether those devices are allowed on the hospital network. The policies should also define whether employee devices are allowed on the guest network, where they compete with patients for bandwidth. As with patients' personal devices, there is little control over their use, except as part of an employment agreement.

Most hospitals mandate some form of mobile device management software to be installed on clinician BYODs that includes restricted/limited network access, an endpoint integrity scan to ensure the device is not infected with a virus, restricted ability to save patient data locally, and the ability to remotely wipe the device in case of theft or loss.

Finally, personal devices are not tested to the electromagnetic interference (EMI) standards of medical devices. Whether emissions from these devices will produce harmful interference, causing a medical device to malfunction, is an unknown potential risk. Educating clinicians and healthcare technology management professionals that personal devices should be considered as part of investigating device malfunction is prudent (since restricting personal devices isn't realistic!).

4. What are the biggest mistakes that healthcare delivery organizations (HDOs) make in managing wireless issues?

Top 10 mistakes from AAMI's *Going Wireless*[8] publication:

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, 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

At a high level, these mistakes may be summarized as: *The biggest mistake an HDO can make with wireless is failing to create a strategic plan on how to use and implement wireless technologies*. Implementing each wireless technology—whether WMTS telemetry, cellular telephones, Wi-Fi networks, Bluetooth, or proprietary technologies for RFID—requires planning as each may present multiple risks, including security breaches, patient safety issues, and adverse impacts to other wireless applications.

Failure to create a foundational strategy increases the probability that the risks become adverse events. Lack of a dedicated, qualified wireless team is common. Hospitals need to invest in the appropriate technical staff and ensure that they are trained appropriately.

5. Is there a glossary of terms that would help me understand all of the acronyms people throw around?

You will find a glossary of terms in *Appendix B* of this document. Additionally, the books and websites referenced in Question 1 provide material containing many of the terms and their definitions.

6. I'm a healthcare technology management professional. Why should I care about wireless when it's not in my job description?

If you are working with medical devices, you are touching devices with wireless technology. Whether it's specifically written into your job description or not, a certain level of understanding of wireless technology is essential to doing your job well. Developing the skills to address wireless issues will make you a more valuable part of the team. In some hospitals, IT personnel may focus on the networking aspect of wireless and may not understand the technical aspects of RF or the potential clinical impact.

In some cases, this lack of understanding has severely affected patient care. The healthcare technology management professional can serve a critical role in bridging IT and clinical viewpoints. As medical devices continue to be more mobile and connected, understanding wireless, RF, and basic IT concepts is becoming a core requirement for clinical engineers, whose electronics training provides a solid base to which wireless skills may be added.

7. Why are there so many contradictions in best practices from different MDMs?

Many standards allow for various settings to allow the users to modify operation to improve performance. Best practices for wireless devices are specific to the application and vendor, each of which is optimizing the performance of their medical devices. The HDO needs to understand from each vendor why each “best practice” was selected for those products, and then determine what set of wireless practices are best for the HDO. This determination would typically include a risk analysis, which in turn depends on clinical importance, hazard level, probability of occurrence, and business needs. As an example, an 802.11 delivery traffic indicator map (DTIM) period of 10 might be used to optimize run time, but a different vendor trying to minimize response time might choose a DTIM period of 1. As another example, a vendor might choose to preferably run at low data rates to maximize range and data reliability, but the hospital IT group prefers high data rates to maximize data throughput and the number of supported devices.

8. What skills and tools do my team need to support a Wi-Fi network?

To be successful, team members need to have good communication amongst themselves and within the HDO concerning the challenges and requirements of a wireless network addressing: published policies, change control, security, guest access, devices supported, and general access. The team needs a willingness to keep up with technology and must have the discipline to plan and test the changes before going live.

The team should have available people with expertise in the following areas:

- Communications standards used in the hospital
- Wired networking: routers, switches, VLANs, trunking, servers, architecture, QoS, etc.
- Wireless networking: data rates, security, wireless architecture, RF concepts and experience with the various tools (see below)
- Wired and wireless security: authentication, encryption, authentication servers, certificates, penetration testing, intrusion detection/prevention
- Risk management
- Clinical workflows
- Requirements of the various medical devices

The team needs tools to test, monitor, maintain, and troubleshoot infrastructure (wired and wireless) and devices, and know how to use the tools. Such tools include:

- RF spectrum analyzer to view the RF environment, irrespective of the source of the RF signals. The spectrum analyzer requires a bandwidth of at least 6 GHz to support 802.11 standards through 802.11ac, and at least a 60 GHz bandwidth to support 802.11ad.[18]
- Wireless packet analyzer (also known as an RF sniffer) to capture wireless packets, preferably multi-channel.[19]
- Wireless site survey tools to measure and map coverage by APs.[20]

Radio/Network Choices, Options, and Coexistence

9. What are the differences between WMTS and Wi-Fi?

WMTS and Wi-Fi telemetry monitors send patient data to a central station and allow patients to ambulate throughout the hospital, but that is where the similarities end.

WMTS is a set of frequencies comprising 14 MHz of bandwidth within 608–614 MHz, 1395–1400 MHz, and 1427–1432 MHz, and set aside by the FCC for medical telemetry. In various parts of the country, the 608–614 MHz band experiences adjacent TV channel interference. Within the 1427–1432 MHz band, medical telemetry operates on a secondary basis in half of the band (which half depends on location).[21] Different manufacturers' telemetry devices use different, often proprietary, communication protocols and cannot coexist in the same frequency band. The WMTS only exists in the United States.

Some telemetry equipment operating in the WMTS band has a dedicated transmitter-receiver pair for each patient that operates on a fixed frequency and uses one-directional communication. The design of these systems predates cybersecurity issues and mitigation strategies and requires interference-free spectrum to operate.

Newer telemetry equipment protocols that operate in the WMTS support two-way communication and provide features that allow the system to operate safely and effectively, even in the presence of interference. These include frequency hopping, multiple channels, encryption, and authentication. These protocols may include encryption and authentication to help reduce the probability of a successful cyberattack.

Wi-Fi is a standards-based communication protocol (IEEE 802.11) and operates worldwide in several shared-spectrum frequency bands, primarily the 2.4–2.5 GHz and 5.150–5.875 GHz bands. This is more bandwidth than all broadcast television, AM, FM, cellular, and Personal Communication Services (PCS) bandwidth combined. Wi-Fi has no legal protection from interference; rather, the 802.11 communication standards were *designed to coexist and reliably transmit data in the presence of interference.* Medical devices following the 802.11 standards use spread-spectrum technologies that are resistant to interference and are able to move to channels within a 555 MHz bandwidth (in the 5 GHz band) to minimize interference. Wi-Fi further includes retransmissions, traffic prioritization, and forward error correction to further minimize the effects of interference. Wi-Fi includes AES encryption and enterprise-class (802.1x) authentication, which protects patient data and the network. Because all Wi-Fi medical devices communicate to the hospital wired network via access points (APs), a single wireless network infrastructure can support them. However, this shared network may be subject to security attacks that can come from any Ethernet or Wi-Fi device in the enterprise, particularly when the network must support older medical devices that lack support for Advanced Encryption Standards (AES) and 802.1x. Please refer to the *Security* section for a guide to reducing the chances of a successful cyberattack.

10. What are MedRadio, MBAN, and MICS, and how are they related? Are there coexistence problems with Wi-Fi or WMTS?

MedRadio, MICS, and MBAN are FCC services used to communicate with body-worn or implanted medical devices.

MICS (Medical Implant Communications Service) is the oldest of the three and operates in the 402–405 MHz portion of the radio spectrum. These radio frequencies were chosen because RF signals here readily pass through human tissue with minimum attenuation, an important feature when communicating with an implanted device. MICS was originally created to allow communications between implanted devices such as pacemakers and their programmer/controllers.

As implanted and body-worn devices became more sophisticated and required more bandwidth than allowed under MICS, the Medical Device Radiocommunications Service (MedRadio) was created to address the problem. Spectrum for MedRadio was originally created by expanding the MICS band to allow operation in the 401–406 MHz portion of the radio spectrum, encapsulating the older MICS band. This was later expanded to include the 413–419 MHz, 426–432 MHz, 438–444 MHz, and 451–457 MHz bands on a secondary basis. These later, expanded frequencies are shared with other users on a non-interference basis, i.e., with amateur radio and government users who have priority in interference cases. Interference is expected to be minimal as MedRadio devices operate at very low power levels to prevent interference with other devices, while incorporating error-correcting protocols to overcome external interference.

The MBAN (Medical Body Area Network) service was created for body-worn devices to communicate with hub devices and operate in the 2360–2400 MHz band, just below the 2.4 GHz ISM band commonly used for Wi-Fi, Bluetooth, and industrial, scientific, and medical (ISM) technologies. The original concept was to modify Bluetooth hardware to operate in the MBAN frequencies, thereby leveraging the economies of scale of consumer Bluetooth technology to provide a low-cost wireless solution and operating in spectrum reserved for medical devices. As of 2019, MBAN remains largely unused, likely due to MDMs who are more attracted to Bluetooth and the ability to use smartphones as readily available hub devices.

For more detail, please see the FCC MedRadio[22] page and FCC 11-176.[23]

11. Is there an issue with Bluetooth and Wi-Fi coexistence?

These systems both include technologies that work in the presence of other transmitters and generally coexist without issue. For more detail, see Question 75, "How does Bluetooth coexist with 802.11?" in the *Bluetooth* section.

12. Does it work to have two different manufacturers' Wi-Fi networks operating in the same space? What are the key considerations?

With careful design and monitoring, two overlapping systems can be installed using the 2.4 GHz band, which has only three non-overlapping channels, but such shared spectrum requires serious constraints on the use of systems installed this way. Overlapping systems are much easier to support in the 5.8 GHz 802.11a band, where there are 24 non-overlapping channels.

An HDO might have two wireless infrastructures while changing to a new wireless vendor. Other hospitals might prefer to keep clinical data completely separate from other IT data.

Key considerations when dealing with two or more disparate Wi-Fi networks in the same airspace include:

- Creating a channel plan to minimize co-channel interference.
- Managing AP power settings for optimum coverage.
- Considering whether seamless roaming is a requirement.
- Considering whether channel bonding, which uses multiple 802.11 channels to support a higher bandwidth, will be used when creating the channel plan.

13. Is telemetry for patient monitoring considered wireless?

Yes: Any communications system that doesn't use wires to communicate is wireless.

Prepurchase/Preinstallation

14. What should I look for in a medical device and the company that supplies it in terms of wireless capabilities, expertise, and support?

The medical device needs to meet the functional and clinical requirements for the job to be performed. The manufacturer should have a solid and demonstrable understanding of the wireless technologies they have chosen for their device. The manufacturer also should be able to provide documentation adequate to ensure that it meets the interoperability and security requirements of your facility, as well as adequate instructions to ensure that the device can be supported in a manner that ensures its safety and efficacy when installed on the chosen wireless infrastructure. The manufacturer should provide a network disclosure statement to the HDO detailing the constraints and capabilities of the device, as well as the requirements from the organization's infrastructure. The manufacturer should also provide information mentioned in the *Security* section.

15. What wireless specifications should I be writing into my RFPs for medical devices?

The RFP (request for proposal) should include specifications that reflect the HIPAA, wireless security, and wireless operational policies of your facility. It should include requirements for the vendors of both the medical equipment and IT equipment to provide information necessary to ensure the proper functioning of the medical equipment and continued support. For more detailed information, you should consult the IEC 80001-1 risk management standard and its technical reports covering wireless network design considerations and responsibility agreements. Support of hospital authentication/encryption requirements and specific wireless standards are two specific concepts to include. Please see *Appendix A, Example Prepurchase Questionnaire*, for a sample of questions that might be asked of MDMs.

16. How can I engage my C-suite and encourage them to invest in the wireless infrastructure?

One option is to consider security, consistency, and timeliness of data, as all of these have an impact on clinical outcomes—the heart of quality and affordability agendas that guide decisions made by virtually every health system. To support your argument, be prepared to discuss how your particular initiative (strategy and tactical plan) can improve quality (perhaps including impact to brand) and be affordable.

A healthcare technology management leader at a large health system shared these experiences:

“We removed the veil of technical secrecy from the requests and communicated very clearly the value of the investment from the standpoint of clinical efficiency and improved patient outcomes. Including very specific data on how proposed wireless and wired infrastructure upgrades would improve clinician access to the system, reduce downtime, and speed up transactions made it very obvious to the C-suite that the resources needed to be approved.

“It was common several years ago for IT infrastructure requests to be among the first items cut when there was a need to cut the capital budget. The turning point was the integration of mobile and fixed computing devices into the clinical workflow. When we were preparing to implement our EHR at our first sites, it became readily apparent that our existing infrastructure would negatively impact clinical workflow and ultimately patient outcomes.

“Wireless VoIP (Voice over Internet Protocol) phones transitioned from being ‘nice to have’ to a critical part of the clinical workflow. Communicating how the investment in better phones and enhanced wireless infrastructure would better support clinical workflow and patient outcomes helped the C-suite understand the importance of the investment.

“Quantifying costs using indirect measures such as communicating return on investment (ROI) in dollars may be difficult. Executives realize that every clinician waiting an extra 30 seconds for a refresh from the EHR server multiple times per day adds up to wasted dollars. Similarly, the count of lost connections that have to be restarted due to inadequate wireless infrastructure adds up to wasted dollars and clinician frustration. Frustrated clinicians lead to turnover, and the costs of clinician turnover have been well documented. Similarly, the cost of EHR downtime (estimated by a large hospital chain at more than $10k per hour) may be used to justify upgrading the system to reduce downtime.”

Regulatory Questions and Guidance Documents

17. Where does a medical device vendor's responsibility end and my responsibility begin for managing the wireless infrastructure, network, and wireless devices?

ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT Networks incorporating medical devices—Part 1: Roles, responsibilities and activities,* provides a definition of roles for the hospital and MDM.

A wireless network infrastructure vendor is responsible for ensuring that any 802.11 wireless hardware they manufacture meets IEEE standards and FCC (or other regulatory body) requirements. They are also responsible for providing a reference architecture, configuration guides, deployment guides, and ongoing hardware and software maintenance, depending on the level of support the HDO contracts for. This includes software security patches and alignment with new standards. They are also responsible for providing a healthcare organization with a product roadmap on a routine basis.

The MDM is responsible for ensuring that the device meets all relevant IEC, FDA, FCC, and AAMI regulations and guidelines. As part of this, the MDM should also ensure the radios comply with applicable standards such as 802.11/Wi-Fi and Bluetooth. The device manufacturer must clearly communicate any network requirements for the device to function in an optimal manner. In addition, the MDM is responsible for ongoing security patching of the device and the underlying operating system, and explaining to the HDO the migration plan when updates for software created by and/or purchased by the MDM are no longer provided. MDMs may reasonably require that only a subset (sometimes referred to as "mainstream releases") of wireless controller releases will be tested and supported, as the burden of testing every minor release is unrealistic.

The HDO should understand the vendors' support plans for when the software the MDM purchases is updated and/or no longer supported, and preferably negotiates with IT and MDM support agreements prior to purchase and includes these in a contract. See the interview with Dr. Kevin Fu, *XP Device Support Ends: Now What?*[24]

18. What is IEC 80001-1?

The inclusion of medical devices directly on the IT network introduces a level of risk that needs to be qualified, quantified, and managed. ANSI/AAMI/IEC 80001-1 is an international consensus standard that outlines how to identify, assess, and manage risks associated with medical devices. It focuses on HDOs that connect medical devices to their facility's IT network. AAMI has published a free document, *Health IT Risk Management: A Practical Tool to Help Hospitals and Medical Devices Stay Secure in a Complex World*[25], that explains the 80001 standard.

19. What is risk management in the context of wireless networks and how do you perform it? What are the essential elements of it?

Risk management in the context of wireless is much the same as risk management in connecting a medical device to any network, wired or wireless, and is described in the 80001 standard. This involves retaining the three key properties of the networked medical device—patient safety, device efficacy, and system security. The essential elements include network change management, identification of life cycle support issues, and system monitoring. Consider also reading *Application of IEC 80001 in Avoiding Pitfalls of Wireless LAN System Design.*[26]

20. How expensive is it to comply with 80001?

80001-1 defines the roles and responsibilities of the entities and personnel needed for the HDO to establish a risk management program. The associated technical reports provide detailed examples for implementation. While it is not possible to give definitive values for the costs of compliance with 80001, most of the elements required by 80001 already are known by HDOs, even if they aren't already being used. 80001 does not need to be implemented overnight, but can rather be implemented in crawl, walk, and run phases. The crawl phase could be creating a detailed inventory of all networked medical devices and a risk assessment framework, while the walk could entail establishing the medical IT–network risk manager role and mitigating the highest-risk issues. The run phase can translate to full alignment with 80001 and a mature risk assessment framework.

AAMI has published a free document, *Health IT Risk Management: A Practical Tool to Help Hospitals and Medical Devices Stay Secure in a Complex World*[25], that explains the business case for adopting ANSI/AAMI/IEC 80001-1.

21. What do the FDA's guidance documents on cybersecurity, mobile devices, and use of wireless technologies mean for my organization?

The guidance documents published by the FDA can be used by HDOs to understand the variables that MDMs must consider when designing their products. This, in turn, allows the HDO to examine what must be done to ensure that the medical device operates safely and reliably in the intended environment. They also inform the HDO when altering the medical device or network equipment might cause the HDO itself to become an MDM regulated by the FDA. The HDO should be familiar with these documents to understand whether any activities within the HDO are FDA regulated and to allow the HDO to ask specific questions of the MDM. For example, "What attack surfaces were analyzed and what mitigations are in place?"

Maintenance and Management of the Wireless Network

22. What tools do I need to check my wireless network?

Spectrum analyzers, 802.11 protocol analyzers (aka 802.11 network analyzer, 802.11 sniffer), and site-survey kits are used in conjunction with tools available on the wireless controller and wired infrastructure. Please see the table below, which outlines some examples of issues that prevent wireless communication and how different tools could be useful for debugging. Please note that the table is not comprehensive. The order of checks moves up the stack because none of the higher layers will work unless the lower layers are in place. That is why debugging a client that won't connect begins with checking to see whether the client is transmitting, followed by 802.11 connectivity, authentication, and then IP-level connectivity.

For proprietary networks such as those that support WMTS, tools other than a spectrum analyzer are typically only available if provided by the vendor.

Problem	802.11 Protocol Analyzer (Sniffer)	Radius Server Logs	Spectrum Analyzer	Wireless Controller and Wired Network
No or Unreliable 802.11 Connection	• Determine if client is transmitting packets and, if so, the retry rate for the client and the AP • Verify client packets are acknowledged • Data rate of the transmissions • 802.11 channels in use	N/A	• Is client transmitting? • Signal strength and SNR of AP(s) at client • Signal strength and SNR of client at AP • Duty cycle of interference	• Any traffic from client? • Signal strength of client as seen by the AP • Retry rate of packets transmitted to client • Data rate of received and transmitted packets
No IP Connection	• Verify authentication is received from authentication server • Verify DHCP request/response occurs • Verify gratuitous ARP occurs	• Verify client authentication credentials are received • Verify client is authenticated	N/A	Verify authentication packets are received from the client
RADIUS Authentication Failure	Verify 4-way handshake occurs properly	Verify 4-way handshake	N/A	
Roaming Issues	Is full or fast authentication occurring at each roam?	Verify server is only contacted for initial connection to Wi-Fi network	N/A	Verify fast roaming is enabled

NOTE: AP = access point; ARP = Address Resolution Protocol; DHCP = Dynamic Host Configuration Protocol; RADIUS = Remote Authentication Dial-In User Service; SNR = signal-to-noise ratio

23. How do I know if my devices/wireless network are experiencing a high rate of interference? How can I troubleshoot it?

Interference occurs when two or more transmissions occur at the same time, in the same place, and in the same frequency band. It is analogous to having two people talking to you at the same time. A whispered comment causes little interference compared to a loud voice. If the interference is strong enough and occurs often enough to cause unacceptable delays, jitter, or transmission failures, the term "harmful interference" might be applied.

RF emissions may be characterized as intentional and unintentional. Intentional transmissions are due to devices such as radios that purposely transmit data. Unintentional interference is due to emissions that occur as a consequence of device operation, such as sparks on motor bushings, faulty/failing fluorescent light ballasts, high-speed switching of data and address lines in a computer, etc.

A symptom of interference is the user having connection problems. These might be exhibited by dropped calls, missing audio and/or video, or a device that can't reliably connect or stay connected. Devices might display an error message akin to "network connection lost." Possible causes include low signal strength, software issues, compatibility issues (for example, authentication mismatch), or interference. When there is a low signal strength, interference is more likely to cause the symptoms listed above.

To troubleshoot, check the RF performance of the devices at both ends (and possibly in the middle with a sniffer or spectrum analyzer) while the symptoms are evident. Check signal strength, retry rates, noise level, data rate, and existence of acknowledgement packets. For examples and more detail, see *Appendix C, Troubleshooting 802.11 Connectivity Issues*.

24. Do I have enough capacity for all our wireless initiatives?

Network capacity issues are typically the result of inadequate planning by HDOs to understand how they use wireless technology and ensure a proper design and installation of infrastructure. Acute changes in capacity can be caused by sudden increases in the number of wireless clients, physical changes to the building, and "bugs" in software/firmware upgrades.

The best way to solve these problems is to plan for network growth in the first place, following the guidance from ANSI/AAMI/IEC 80001-1:2010 and its technical report, ANSI/AAMI/IEC TIR80001-2-3:2012. Use the tools mentioned in Question 22, "What tools do I need to check my wireless network?" to determine whether there truly is a bandwidth issue. It may be that data isn't arriving as intended because of interference.

Assuming more bandwidth is required, one possible solution is to take advantage of the large number of channels available in the 5 GHz band. It is possible to reuse channels (analogous to the solution used by cellular providers: install more APs with lower transmission powers). Ensure that all areas are covered by strong signal (at least -65 dBm for 802.11a/g) so that devices can transmit at the highest data rates. Upgrade to 802.11n and 802.11ac where there is high spectral efficiency (the number of bits that can be transmitted per hertz of bandwidth).

It is important to understand that wireless networks can comprise several service set identifiers (SSIDs) or network names that cater to different user/device types. These various SSIDs have to share the limited bandwidth and contend with each other for air time over the 2.4 GHz and 5 GHz frequencies. When evaluating capacity, it is important to remember that as the number of SSIDs increases, the overhead burden of wireless traffic management increases, which ultimately decreases the available bandwidth. It often makes sense to have several SSIDs (e.g., for separate guest and medical networks), but try to minimize the number of SSIDs used.

With respect to WMTS systems, the FCC-allocated bandwidth is limited to about 14 MHz. Working with a vendor that provides a higher spectral efficiency than older telemetry systems can make better use of the 14 MHz available for WMTS.

25. Which team should own the wireless network and/or manage spectrum use?

Successful management of a wireless network that supports medical devices depends on strong collaboration and good communication between IT and HTM groups so that medical device, clinical, and IT needs are all considered. Some hospitals have an employee whose role includes spectrum management. The HTM group can bring in concepts including clinical workflows, patient safety, IEC 80001, and IEC 60601-1-2. Ideally, HTM has at least read-access to the appropriate wireless controllers and understands the operation of the wireless network as it pertains to medical devices.

26. What factors should I consider before upgrading my network software?

The following items are generally considered when evaluating a network software upgrade:

- A thorough read of the release notes
- Results of a risk analysis of not updating the software, including mitigation strategies
- Results of a risk analysis for updating the software, including mitigation strategies
- Installation and operational test plan (might include testing in a lab environment first)
- Backout plan (in case the upgrade fails)

Update the network when the risk/reward ratio of updating is lower than the risk/reward ratio of not updating: compare the benefits (bug fixes, new features) and risks of updating (untested medical devices might not operate correctly) vs. benefits (stable system) and risks of not updating (e.g., security vulnerability). In an easy example, if the WLAN vendor implements a patch to support 802.11ac and the HDO has no 802.11ac devices, the reward for updating is zero, so the risk/reward ratio is infinite.

A more common scenario to consider is when there is a security patch. From an IT security vantage point, one would install the patch as soon as possible to quickly remove the risk of a security vulnerability. The hazard and probability of occurrence of the security vulnerability being exploited needs to be weighed against the probability and occurrence of potential issues that might include:

- Infusion pumps may not be able to update formularies
- Patient monitors may not be able to deliver alarms
- Roaming doesn't work
- Picture archiving and communication systems (PACS) may not be able to upload images
- Mobile EHR interfaces may not to be able to access patient records
- Voice over WLAN systems may not operate correctly

Typically, an update adds more than just one feature, includes bug fixes, and sometimes introduces new bugs. The probability of hazardous events is generally higher for new releases that haven't had time to mature. Consequently, large providers usually have very stringent and exhaustive tests to qualify new network equipment and software. Once qualified, they stick with the same versions for a long time because of the time and cost of qualification. As some are fond of saying, "Tried and true is better than new."

The only real way to know whether the upgraded network software works is to test it, preferably in a lab environment. The highest priority is to test against those devices whose failure causes an unacceptable risk. HDOs should be prepared to do this testing because MDMs typically require weeks to months to test against a new release of WLAN firmware, while an IT department may want to immediately deploy the new release to address a security vulnerability. The presentation, "Risks, Challenges and Opportunities of Wireless Technologies in Healthcare: Wireless Testing in a Hospital," provides guidelines for risk analysis and testing to guide a decision on whether to upgrade the WLAN operating system before the medical device companies have validated it.[27]

27. How do I determine the performance of medical devices on my wireless environment?

There are several tools available to gauge the performance of wireless medical devices on the network. In the interest of cooperation and communication, it is a good practice to work with your IT department here and in other areas where IT network testing is needed. Based on the performance indicators and metrics desired, this can be quite complex. The tools can be broken down into the following groups:

a. Most wireless medical devices have built-in monitoring systems to some degree or another. These will usually indicate a relative signal strength and whether the device is connected to the network. The more sophisticated systems illustrate additional metrics such as signal power (in dBm or RSSI) and number of retries.

b. Wireless medical devices typically send data to a central server, which has management functions. In some cases, these systems allow for SNMP (Simple Network Management Protocol) monitoring. SNMP monitoring can also be used on the wireless infrastructure to proactively identify when systems are offline or predefined thresholds are reached. For example, a system administrator can be notified that a wireless AP or controller is offline. In some cases, metrics such as signal strength can also be captured via SNMP.

c. Wireless management platforms and wireless controllers often offer metrics and insight into device connectivity trends.

d. Tools are also available that can provide a view of wireless performance. Combining the results of these tools with those above provides a full wireless system picture. These include 802.11 wireless sniffers (e.g., Wireshark) and they can provide a good picture of what is going on in your network with all of the different types of devices you are required to support. Wireless sniffers are useful because they detect some things that won't be visible and/or are hard to detect at the wireless controller, e.g., a high rate of beacons and high incidence of broadcast/multicast traffic.

28. What is a wireless LAN site survey and how often should I do one?

In this context, a "site survey" is a measurement of RF performance in an area (and the adjective "wireless" or "RF" is often omitted). The performance measures can include power, interference, redundant coverage, noise levels, and signal-to-noise ratio (SNR). There are at least two types of site surveys. An "installation site survey" is typically done to increase confidence that the planned AP locations are correct. The installation site survey typically uses a single AP, always on the same channel, that is moved to each planned AP location. Once placed in a planned location, the RF signal strength is measured in the area around that location.

In contrast, a "verification site survey" is a manual measurement and mapping of the RF coverage after the WLAN is operational. Because the APs are all active, in their final locations, and transmitting on a myriad of channels, the installer is able to verify whether the final installation meets the requirements.

At a high level, to perform a site survey, one imports a facility floor map into site survey software and walks around the building while the software records the signal strength of each AP. Postprocessing provides heat maps or other ways to visualize the RF coverage. Different tools add other features, such as overlays for RF utilization and methods to indicate redundant coverage (as opposed to just the strongest coverage in that area), SNR, and co-channel interference.

A verification site survey should be updated any time there is substantial change to the network or the physical environment. Since automatic RF coverage algorithms running on wireless controllers may change the AP transmission power and channels, a site survey may be used to objectively evaluate the effect of the algorithm, particularly when it is first enabled. Periodic evaluations should be run, and the time between these evaluations depends on the output of a risk analysis. As a guide, an annual site survey is prudent and may also include looking at the noise floor using either the site survey tool or a spectrum analyzer.

Some WLAN vendors' tools and third-party applications build RF coverage maps using information each AP collects about how strong it hears other APs. If one compares this data to a manual site survey and there is a strong correlation, it may make sense to use these tools.

Security

29. How does cybersecurity affect the choice of medical devices?

Purchasing medical devices that don't support the highest levels of security provides opportunities for hackers to exploit vulnerabilities on the device and/or wireless network. A system that has wonderful clinical attributes, but with security vulnerabilities, creates a risk the HDO should evaluate and understand.

Some hospitals may be constrained to continue use of existing medical devices that don't meet the highest levels of security. As part of a security framework and plan, the hospital should minimize security risks and plan responses for if/when those devices are compromised as part of a medical device security program.

For more details and understanding, please consider industry-created guidance documents. A favorite is *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.*[28]

30. How do I deal with legacy medical devices with obsolete security features?

HDOs are grappling with legacy systems in a few ways and, preferably, include the following as part of a security framework:

1. Segment network-connected medical systems so that those medical systems are shielded from other types of devices on the same network. Segmentation may include virtual local area networks (VLANs), firewalling (only include the specific IP addresses, ports, and protocols that are required by the medical device) and/or using a VPN to connect the non-secure device to the hospital network.

2. Develop a process for replacing medical devices that includes security considerations (e.g., devices running unsupported operating systems).

3. Restrict the purchase of medical devices that fail to meet security guidelines by creating a process for assessing medical systems that includes analyzing and addressing the risk(s) of the system before the systems are actually purchased. Preferably include in the requests for quotation (RFQs) sent to vendors the HDO's security requirements, such as WPA2-AES, to communicate to MDMs that security is important.

31. What is a medical device security program and why is implementing one a worthwhile endeavor?

Medical devices are a key and potentially vulnerable set of devices at any HDO. Aging legacy systems, lack of inventory management, lack of risk awareness and education, lack of security intake processes, and inability to patch make medical devices a big challenge for any hospital. Without a security program in place to actively address these challenges, your organization is at a much greater risk of a successful attack or breach and also in a weak position to respond rapidly to an attack.

32. What is a key to starting a successful medical device security program?

One of the first steps is gaining support from senior leadership for instating a medical device security program. To do that, explain the “why,” in their language. For example, explain the costs of a data breach or a ransomware attack and the subsequent impact (potential patient diversion and lower revenues). Including the risk of physical and financial harm to patients further bolsters the argument for a medical device security program. Finally, emphasize that once a medical device is compromised, all networked systems—including HR and finance—are at risk.

33. What are the top priorities for a new medical device security program?

1. Develop an intake process for new medical equipment that allows for security-related questioning and analysis.

2. Discover each network-connected medical device connected to your internal networks, since networked medical devices will make up the bulk (if not all) of the device scope for the medical device security program.

34. What are the top things to be concerned about when assessing a new medical device?

1. Software patching (updates): Ensure the provider has a reliable and secure method for distributing patches and that the provider actively assess new vulnerabilities as they are discovered. Routinely patching devices is one of the better ways to minimize your overall risk landscape.

2. Supported operating system: Making sure you understand the operating system on the device in question and how long that operating system will receive security updates is a big part of knowing what types of risks need to be addressed.

3. Default passwords: Require that all default passwords be removed before the new system is installed.

4. Encryption: Consider the highest level of encryption your network supports and the highest level of encryption the organization would like, e.g., WPA2-AES or WPA3-Enterprise. Set a standard for encryption that supports BOTH the HDO’s requirement and the most recent industry standard. Ensure the device encrypts electronic protected health information (ePHI) not only in transit, but also at rest.

5. Authentication: Ensure the device supports the latest industry standards for secure methods to authenticate the device to the network. The device should also provide a secure method to authenticate software updates and any apps added to the device.

6. Software bill of materials (BoM): In order to ensure a full picture is created during the initial assessment of the device, having a database of all the software on the device is vital. This allows determination of known vulnerabilities by comparing the software BoM to the National Vulnerability Database. The MDM should provide the software BoM and agree to provide updates to the HDO when software is patched. Understanding how to patch and which vulnerabilities exist for each piece

of software is a major component when assessing a new medical system and when assessing the threat of new vulnerabilities. As part of device life cycle management, the MDM should routinely assess software for vulnerabilities and provide this information to customers.

7. The MDM's analysis of attack surfaces and mitigations and any vulnerability testing completed by the manufacturer.

If the manufacturer cannot or will not provide this information or will not address known vulnerabilities, consider it a warning about the security posture of the manufacturer and its devices.

For Bluetooth devices, see Question 80, "What are some Bluetooth-specific security considerations?"

35. Where should a medical device security program reside: HTM/clinical engineering or IT/IS security?

It does not really matter where the program officially lives as long as its guiding principle is to reduce network and device security risks that impact patients and employees. It is more important that the two groups work together for an integrated plan and execution.

36. What are some materials our organization should look at to help get started on building a medical device security program?

- *Health Industry Cybersecurity Practices,* particularly Table 6, "Suggested Practices to Combat Attacks Against Medical Devices That May Affect Patient Safety"[28]
- *Medical Device and Health IT Joint Security Plan*[29]
- *Framework for Improving Critical Infrastructure Cybersecurity*[30]
- *Medical Device Cybersecurity: A Guide for HTM Professionals*[31]

37. What's the difference between encryption and authentication?

Encryption is the process of converting data into a form that is not readable/understandable by an unauthorized person or device. Authentication is the process of ensuring that a person/device is actually the person/device it claims to be. Secure communication requires both authentication and encryption.

38. Are there any security risks if I broadcast my service set identifier (SSID)? Is there any reason to hide SSIDs?

No. Hiding the SSID provides no real security. Even if the SSID is hidden, it is transmitted in the clear by every device that is connected to that SSID and also by the AP in probe-response frames. Moreover, many clients send out probe requests with the SSID visible even when outside of the facility. Microsoft TechNet has an excellent article with a section explaining why non-broadcast networks are not a security feature.[32]

Some hospitals have found that hiding SSIDs for all but guest networks helps patients and their families to identify the proper SSID for guest access. Before hiding SSIDs on clinical networks, ensure that all devices can connect correctly. Devices that strictly follow Dynamic Frequency Selection (DFS) requirements fail to connect to APs on DFS channels that don't broadcast SSIDs, because clients are not allowed to transmit until after receiving a transmission from an AP.

39. What security-related information should an MDM provide to an HDO?

The ANSI/NEMA HN 1-2019 *Manufacturer Disclosure Statement for Medical Device Security* (MDS2)[33] is an industry standard that provides a set questions to which MDMs can respond for each device model. This information supports the HDO's risk management.

Reliability

40. What is wireless quality of service (QoS) and how is QoS quantified?

Quality of service refers to providing preferential treatment to high-priority data. QoS can be applied to wired and wireless protocols.

Typically, throughput (bits/second), latency (ms), jitter (ms), and dropped packet rate are the parameters used to quantify QoS, although a particular medical device might specify other parameters.

802.11 provides four access categories (QoS levels): voice, video, best effort, and background (listed in descending order of priority). Devices with voice settings have the best opportunity to connect to the network and so, statistically, should have the lowest jitter, dropped packet rate, and latency. The article "Medical-Grade, Mission-Critical Wireless Networks" provides a good discussion of QoS.[34] See section 5.5 of ANSI/AAMI/IEC TIR80001-2-3:2012 for information on QoS mechanisms.[35]

Wired Ethernet (802.3) has QoS mechanisms including ToS (type of service) and 802.1p.

41. What QoS level is required for a Wi-Fi wireless network with medical devices?

There is no one QoS level for every medical device—QoS requirements depend on specific medical devices, manufacturer recommendations, and the HDO's existing QoS policy.

It is important to remember that QoS settings must be applied in both directions. That is, a device that requests a high QoS setting for data it *transmits* does not automatically cause the data *transmitted to* that device to have the same QoS settings. Also, the wired and wireless network segments handle QoS differently: organizations should plan a combined wireless and wired QoS mapping and classification scheme for all critical traffic.

Generally speaking, most organizations do not need to modify the *wireless* QoS settings from defaults. Usually enabling QoS in WLAN infrastructure hardware enables the Wi-Fi Alliance–recommended settings that work for voice, video, background, and best effort traffic. When the wireless traffic enters the wired segment of the network, wired QoS tags may be applied.

Determining the QoS required for devices in your organization should include these steps:

a. Obtain the specifications for each type of wireless device supported on the WLAN. *NOTE*: As long as someone is putting the list together, consider keeping it up to date as a tool for the future as new devices are brought online and old devices are removed.

b. Refer to your WLAN infrastructure and wired LAN infrastructure best practice guides for healthcare or enterprise deployments.

c. Quantify medical device or application-level thresholds that exceed acceptable levels. These metrics include maximum allowed jitter, latency, and packet loss rate in addition to any other parameters a device manufacturer may include. These parameters will guide decisions for marking the traffic: those that require the lowest jitter, latency, and packet loss rate will generally receive the highest QoS settings.

d. Since the wireless network is connected to a wired LAN, the wired LAN must also be configured in parity with the wireless network settings. For example, if medical telemetry needs to be marked as high priority, the wired LAN must either trust those markings (recommended) or—if configured to inspect and police the traffic—it must apply a level of priority consistent with the wired LAN QoS policy. Wired QoS policies have many more options than wireless networks do.

e. See section 5.4 of ANSI/AAMI/IEC TIR80001-2-3 for more information on network performance requirements.[35]

Risks

42. Are there wireless devices for which a communication failure can interrupt patient care?

Yes. Communication failure for any device that requires connectivity to fulfill its intended use could adversely affect patient care. Devices on which clinicians depend for patient care should be considered as part of an overall risk management strategy. Medical devices that use data for “real time monitoring” such as a vital signs monitor have a high risk factor for patient safety if the data stream is interrupted. *NOTE*: For a correctly designed medical device with FDA clearance, no medical device connectivity issue may directly result in harm to the patient.

43. What are the hazards for a wireless medical device and for a clinical wireless network? Where can I go to learn about risk mitigation strategies?

Hazards may be generally classified in three areas: internal issues, communication issues, and security threats.

Internal issues are the responsibility of the supplier: either the MDM or the infrastructure provider. These include hardware failures, software failures, and software updates. Communications issues like delayed data transmission can result in delayed alarm notifications, which can in turn cause harm to the patient. Security threats are a joint responsibility of the HDO and the supplier. A security vulnerability may expose more than just that device and its data; it may also compromise the security of the network, application, or protocol involved.

The supplier should:

- Provide timely updates and a secure method to upgrade software.
- Ensure no known vulnerabilities exist in the software, e.g., by checking the NIST National Vulnerability Database, running penetration tests, and performing negative testing.

The HDO should:

- Purchase devices with the strongest security implementation that is available for the technology and appropriate to the application and the data assets stored and transmitted. For Wi-Fi, 802.1x authentication and AES encryption should be used or a justification made if not. For Bluetooth, the strongest encryption and authentication mode should be used or a justification made if not.
- Ensure they are abiding by best security practices provided by the MDM, including enterprise-class authentication and encryption for Wi-Fi devices.
- Provide a method for device software to be securely upgraded.
- Keep the wired and wireless networks secure.

ANSI/AAMI/ISO 14971 and ANSI/AAMI/IEC 80001-1 are excellent reference documents on how to conduct a risk analysis. Risk control measures for wireless devices are covered in section 8 of TIR80001-2-3. For more information and examples, see *Appendix D, Example of Risk Analysis and Risk Mitigation for a Medical Device Using a Wireless Network*. For more detail on mitigating cybersecurity risks, please see the *Security* section.

44. What are some of the common hazards encountered on the 802.11 wireless network?

Common hazards include:

- Exceeding the threshold for the number of devices per wireless AP
- Interference from BYOD patient devices brought into the hospital
- Failure of IT switch, router, or wireless controller
- Ethernet cable unplugged (often on an AP)

- Insufficient PoE (Power over Ethernet) from the data closet switch
- Configuration changes to the wireless network, including AP power and channels
- Firmware upgrade to network resulting in undocumented bugs
- APs vacating DFS channels when a radar signature is detected
- Power surges/power outages
- Failure to properly configure and test controller/AP configuration

Architecture and Network Design

45. How is a network design documented and how is the current status of the network viewed?

A network physical and logical design is typically documented using Visio. This allows a network architect to graphically represent the various physical devices, how they are interconnected, and any relevant IP addresses. Each network device uses at least one IP address on the network and is able to access a pool of dynamic IP addresses for clients joining the network. In some cases, medical device vendors require static IP addresses for their devices, and these can be documented in the Visio diagram. The documentation in Visio is static and relies on manual revisions and revision control in order to remain up to date.

In addition to the Visio architecture documents, a wireless network design tool like Ekahau or AirMagnet can be used to perform an on-site RF validation survey and produce floor plans that illustrate the RF footprint, including the media access control (MAC) address of each AP, signal strength, SNR, and co-channel interference. The RF survey is a manual walkthrough to gather data and produces a *static report*. If any auto channel or auto power provisioning is enabled on the system, this data can become outdated and inaccurate quickly.

Wireless management platforms and wireless controllers allow for a current, *real-time view* of the RF environment, including floor plans with AP locations, signal strength, SNR, and interference. If APs go offline for any reason, this is reflected in the maps and in the error logs on the wireless management platforms.

46. What is a distributed antenna system (DAS) and what are the pros and cons?

A DAS is an antenna that physically extends over a large area, with the idea that it can aggregate RF signal to and from devices across that large area to a single point, e.g., a microcellular tower in a hospital. With a network of small, active antennas serving as repeaters, a DAS can extend RF coverage deep into a building where RF signals such as cellular have difficulty penetrating. This may work well to provide RF coverage in high-rise buildings, stadiums, and the like.

DAS for Wi-Fi hasn't been as successful as with cellular. There was some adoption of DAS for Wi-Fi for 2.4 GHz systems when fat APs (which were very expensive) were the norm, but the physics supporting multiple-input multiple-output (MIMO) requires multiple, separate signals on separate antennas rather than the aggregated DAS model.

Some newer DAS systems have active antenna units that support MIMO, but AP vendors report that location functions won't work properly, so network management suffers. Additionally, the automatic RF channel-power algorithms are designed for standard antennas and would need custom designs for every DAS installation to avoid confusion. Similarly, any time there is an object between the AP and its antennas, troubleshooting becomes more difficult. Finally, there are RF coexistence issues if the DAS units mix the cellular and WLAN distribution—AP vendors have added RF filtering in the APs to reject cellular frequencies.

A DAS may make sense for your HDO, but you should carefully evaluate and validate that these systems meet their requirements and perform to expectations for all medical devices that will use the DAS for the lifetime of the investment.

47. What is bandwidth? Why is bandwidth important in wireless communication such as 802.11 (Wi-Fi), Bluetooth, WMTS, and cellular?

In a communication system, bandwidth can have two definitions:

1. The range of frequencies used to transmit a signal, measured in Hertz (Hz)
2. The capacity for data transfer of an electronic communications system, measured in bits per second

For definition 1, subtracting the lower frequency from the upper frequency gives the bandwidth, expressed in Hertz, for the channel. For example, channel 36 for 802.11 a/n in the 5 GHz ISM band extends from 5170–5190 MHz and has a 20-MHz bandwidth. It is important to know frequencies used by each type of radio in the HDO to support planning of frequency use and understand when co-channel interference with other radios in the same area might occur.

RF bandwidth often is confused with definition 2, the capacity for data transfer (data throughput). Data throughput is a measure of how much data can be sent per unit of time across a network, channel, or radio interface. The amount of data that can be transferred between two points in a set amount of time is expressed as bits per second (bps). One kilobit per second (Kbps) equals 1,000 bps. One megabit per second (Mbps) equals 1,000,000 bps, and one gigabit per second (Gbps) equals 1,000,000,000 bps.

Spectral efficiency is the ratio of the two types of bandwidth: bps/Hz. For example, 802.11n can transmit 72.2 Mbps in a 20-MHz channel, so the spectral efficiency is 3.61 bps/Hz. Older one-directional telemetry transmits 12 Kbps in a 25-kHz channel with a spectral efficiency of 0.48 bps/Hz.

Bandwidth is to communication as blood is to oxygen. The more devices that are transmitting and the more data being transmitted, the more bandwidth (both definitions) is required. With insufficient bandwidth, the communication doesn't occur fast enough to support the needs of the system.

48. How do I ensure that my wireless network remains reliable?

A first step is to design the WLAN for reliability. Apply a design principle from IEC 60601-1: avoid single-fault failures. This principle is applied to WLAN design that:

- Installs APs to provide redundant coverage
- Alternates AP PoE connectivity to different switches
- Installs high availability (HA) wireless controllers

Other guidelines include:

a. Use patch management tools to ensure the deployment of software/hardware/security patches. Review and test these prior to deployment to ensure that they do not cause other issues in your network.

b. Keep a current inventory of all types of clinical wireless devices running on the wireless network and understand the device requirements and best practices.

c. Use multiple monitoring tools. Apply network monitoring and set up alarms and triggers for fault events, and ensure the proper notification list is set up.

d. Complete a wireless survey/heat map, design for primary and secondary wireless coverage, and review when necessary, depending on your environment.

e. Implement standards-based wireless security such as WPA2-Enterprise, EAP-TLS (Extensible Authentication Protocol—Transport Layer Security), and SHA-2 certificates (Secure Hash Algorithm 256 bit).

f. Require device vendors to provide technical specifications documents. This documentation will be essential for device deployment and network configuration. Understand product requirements, best practices, performance, and expectations. Provide performance feedback for product improvement.

49. Should I let the wireless controller dynamically set the power on my APs? That is, should I allow ARM (Aruba) or RRM (Cisco) to change the power levels? Will a statically assigned power setting of 100 milliwatts (mW) result in better coverage?

If ARM, RRM, or other algorithm is allowed to set the AP transmission power, consider limiting it to be no more than 3 dB higher than the client device's transmission power. For example, if client devices can transmit at 14 dBm, then the AP should be limited to no more than 17 dBm. While setting the AP to 20 dBm will allow client devices to hear the AP, the AP will not be able to hear some of those client devices. Further, since client devices use signal strength as a factor for roaming decisions, a high AP transmission power can adversely affect client roaming.

The purpose of AP manager software such as RRM or ARM is to set the coverage area of a wireless AP to overlap with a certain signal strength (typically ±3 dBm by default) to neighboring AP(s). This is so a wireless device can roam seamlessly between wireless APs.

Proper coverage overlap is extremely important when deploying a VoIP phone communication system, continuous patient monitoring, or other system that depends on continuous connections. If the coverage area is set too large by turning the power all the way up (typically 100 mW), the roaming device will get “sticky” and hold on to the pre-roam AP and drop the call as it moves to another coverage area.

A device walkthrough with the wireless device can be done to determine whether the dynamic settings are sufficient for proper roaming. Statically assigned power can be done for individual APs if the dynamic setting algorithm provides an insufficient or overly strong power setting.

See also Question 52, “Will AP power settings work the same for all wireless devices supported at the same location?”

50. Should I assign the channels on my APs?

This depends on whether your infrastructure provider’s automatic algorithm works to your satisfaction. A common name for automatic channel assignment is dynamic channel assignment (DCA). Early versions of these algorithms had some “features” that some hospitals found objectionable, and they found that hand-tuning the channel assignment and power levels worked best. Unfortunately, for a large installation, this becomes difficult to maintain.

Many 802.11 infrastructure providers allow setting groups of APs to use subsets of channels. For example, a hospital that chooses to run clinical data on one set of APs and IT data on another set of APs might assign some channels for clinical use and some for IT use.

When tuning your wireless network for optimum performance for a specific device, you should follow the manufacturer’s recommendations. Consult an expert if there are any doubts about power and channel settings.

If using DFS channels, where the AP may be forced to suddenly vacate a channel, DCA (allowing the wireless controller to make/change channel assignments in real time) may be required.

51. What is the best method for setting up 802.11 APs to provide strong signal coverage and optimum performance in a “greenfield” installation?

A “greenfield” installation is an installation in a new building or area where wireless has not been installed previously. It is important to understand the requirements to which you are designing. Do you need RFID tracking? Are there latency-sensitive medical devices that use wireless? What kind of signal and data rates do you need to support? Is there a lot of interference expected in all or parts of your environment?

Once the wireless requirements are defined for all areas of the new building, one can use Wi-Fi planning tools to obtain a rough plan for the number and location of APs. The next steps are to conduct a pre-installation site survey and adjust the coverage by modifying the rough plan by adding and/or moving APs. It is important that you set the APs to no greater than 25 mW and your production devices’ lowest supported data rate during this review so that you can get a more realistic picture of coverage area issues such as gaps between APs.

There are usually several phases to a Wi-Fi deployment:

- Gather wireless device requirements
- Plan AP placement per requirements and create "heat map" proposal
- Installation site survey: pre-installation walkthrough with a site survey tool to determine/verify the installation locations for APs
- Acquire and install necessary wireless and wired network equipment per proposal
- Verification site survey: manual walkthrough after all APs are up with channel and power settings stabilized
- Validation: postsurvey walkthrough of the site with actual wireless devices to ensure coverage and roaming capability (make adjustments to power and channels if necessary); this validation constitutes acceptance testing and is preferably called out as a requirement in the request for proposal and contract

52. Will AP power settings work the same for all wireless devices supported at the same location?

No. Communication is a two-way process that works best if both sides are able to hear the other. Consider an analogous case where two people are trying to talk but can't hear one another. One person increases his transmission power by using an amplified megaphone. The second person can now hear the first person speaking, but not vice versa. A typical system may have an AP capable of transmitting at powers up to 20 dBm (100 mW) and a typical client device transmits at 14 ±2 dBm (16–40 mW). If the AP is configured at 100 mW, then the client may indicate acceptable coverage, but the AP's received signal is only 16% of what the client detects. For many areas of so-called AP coverage, the AP cannot successfully decode the received data, and communication failures occur.

Ideally, client devices should support the 802.11d power constraint element so that if the client is transmitting at a higher power than the AP is using (as might be the case in a very dense deployment), the client automatically adjusts its transmission power down to match the AP. You may have to consult an expert on the best power setting compromise. Usually, latency-critical data such as VoIP and alarms take precedence and system settings are optimized for these wireless clients.

802.11

53. Which 802.11 standards will I most likely encounter in my environment? What are some of the more important amendments?

IEEE 802.11-1997 is a wireless networking standard published by the IEEE. Many amendments and additions have been made. Amendments are indicated by a letter or pair of letters, e.g., 802.11b, 802.11g. Once the alphabet was exhausted, a second letter is used, e.g., 802.11ac. Regularly, the existing amendments are rolled up into a new version of the general standard, e.g., 802.11-2007 and 802.11-2016. See the IEEE GET Program for

802 standards web page[36] and the Wikipedia 802.11 web page[37] for more information. The Wikipedia IEEE 802.11 web page includes a full list of the 802.11 amendments.

A WLAN, or wireless LAN, is a network that allows devices to connect and communicate wirelessly. 802.11 can be thought of as the wireless Ethernet, also known by its standard title, IEEE 802.3. Wi-Fi devices operate in a group of frequencies called ISM (industrial, scientific, and medical) bands. These bands are available for use by anyone who chooses to buy government-authorized equipment and are shared with other technologies, including Bluetooth and amateur radio. Wi-Fi uses powerful tools to achieve highly reliable data links, even when operating with other devices transmitting in the same spectrum. These tools include protocols to retransmit packets if no acknowledgement of receipt is received; forward error correction, which allows reconstruction of a packet even if the some of the data were corrupted; a cyclic redundancy check to verify all the packet was received/reconstructed correctly; QoS mechanisms to prioritize important data; a cellular architecture, which allows for many, closely spaced APs; more bandwidth (555 MHz in the 5 GHz band alone) than in all broadcast TV, AM, FM, cellular, and PCS services combined, which allows for many APs to be placed in an area, all on different channels; and authentication and encryption, which provide secure communication to support HIPAA policies.

Some of the more common amendments are:

802.11-1997. The original 802.11 specification covering direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), and infrared (IR) physical layers at 1 and 2 Mbps data rates. Of these, only DSSS still has any support in manufactured products. DSSS uses 24 MHz–wide channels and FHSS uses 1 MHz–wide channels.

802.11-2007. New release that includes amendments a, b, d, e, g, h, i, and j.

802.11-2016. New release that includes amendments k, n, p, r, s, u, v, w, y, and z.

802.11a. Introduced orthogonal frequency division multiplexing (OFDM) with data rates from 6 to 54 Mbps in the 5 GHz band using 20 MHz–wide channels.

802.11b. Introduced complementary code keying (CCK) to provide 5.5 and 11 Mbps data rates in addition to 1 and 2 Mbps DSSS. Operates in 22 MHz–wide channels.

802.11e. QoS enhancements that provide for prioritized traffic flow.

802.11g. Added OFDM support with data rates from 6 to 54 Mbps in the 2.4 GHz band using 20 MHz–wide channels. Achieves backwards compatibility with 802.11b (which in turn is backwards compatible with legacy 802.11 1 and 2 Mbps DSSS) through transmission of management frames using legacy modulation and channels.

802.11h. Spectrum management. Introduced rules for European compatibility, specifically DFS (802.11 masters detect protected RF signatures on some channels and dynamically move to different channels) and transmit power control to ensure that devices don't exceed the regulatory maximum for the current country and channel.

802.11i. Security enhancements. Introduced the Advanced Encryption Standard (AES), aka WPA2, to remediate the security flaws in Wired Equivalent Privacy (WEP). Also introduced an interim solution, Temporal Key Integrity Protocol (TKIP), aka WPA, as a stopgap solution to improve security on legacy devices, as implementing AES required new hardware. Provided for both pre-shared key (PSK) and certificate-based authentication using the Extensible Authentication Protocol (EAP).

802.11k. Defines and exposes radio and network information to facilitate the management and maintenance of a mobile WLAN. Provides information for the client to discover the best available AP.

802.11n. Allows higher throughput up to 600 Mbps, achieved by multiple radios to simultaneously transmit (or receive) on MIMO, wider bandwidth (up to 40 MHz–wide channels) and improved efficiencies in the MAC layer such as frame aggregation (send more than one frame per transmission) and shorter guard intervals.

802.11r. Sets standards for fast base station subsystem (BSS) transitions (fast roaming from one AP to another), specifically while using EAP authentication. 802.11i allowed these features, but this led to multiple vendors having different methods.

802.11ac. Provides higher speed improvements to 802.11n for the 5 GHz band, primarily through 80- and 160 MHz–wide channels and additional, simultaneous transmission (or reception). Supports data rates up to 866.7 Mbps per spatial stream and up to four spatial streams for a total of 3.467 Gbps.

802.11ax. Once again, speed improvements in the 5 GHz, using multiple-user MIMO (MU-MIMO). Simultaneous uplink and downlink over multiple spatial streams (carrier antennas). New trigger frame containing packet transmission scheduling information.

Wi-Fi 6: Wi-Fi 6 (802.11ax): The 6th generation of 802.11 (Wi-Fi) physical standards with data rates of up to 1.2 Gbps per spatial stream and eight spatial streams for a total of 9.608 Gbps. 802.11ax can simultaneously operate in the 2.4 and 5 GHz ISM bands. Note that previous 802.11 versions have been rebranded.

Wi-Fi 1: 802.11b (1999)

Wi-Fi 2: 802.11a (1999)

Wi-Fi 3: 802.11g (2003)

Wi-Fi 4: 802.11n (2009)

Wi-Fi 5: 802.11ac (2014)

“Extended” 802.11 channels are subject to FCC 47 CFR Part 15.407(b), sometimes referred to as “regulatory -B domain.” The channels are at the upper range of the 5 GHz ISM band. These are called out because some wireless adapters do not support the extended channels. If a wireless adapter doesn’t support these channels, it cannot associate with an AP that is using an extended channel. (The upper frequencies of the 5 GHz ISM band are subject to different regulatory requirements than the lower frequency bands. Wireless adapter manufacturers that chose not to test to these standards are prohibited from using these frequency bands).

54. What are the reasons to maintain or stop support for 802.11b?

802.11b is an amendment to the IEEE 802.11 standard that dates back to 1999. It uses a different modulation method and has a lower data rate than 802.11a/g/n/ac. Additionally, because 802.11b and 802.11g use different modulation methods, when an AP has even one 802.11b client, all of the management traffic must be transmitted at the slow 802.11b data rates. This creates a data bottleneck that can be relieved by phasing out devices that only support 802.11b.

The only reason to maintain support for 802.11b today is if the HDO has a high density of 802.11b clients, and if that is the case, consider a refresh to ensure that all clients can support 802.11g at a minimum and preferably 802.11 a/g/n. The vast majority of Wi-Fi–capable medical devices today are equipped with 802.11 g/n or newer wireless cards. Those that only support 802.11b generally do not support the most secure authentication and encryption solutions.

Once 802.11b clients are off the network, a good practice is to disable the legacy data rates of 1, 2, 5.5, and 11 Mbps to prevent 802.11b clients from using the network.

55. What is the difference between WPA2-PSK and WPA2-Enterprise?

WPA2-PSK is a method of encrypting data and authenticating wireless clients to the network and vice versa, using a pre-shared encryption key (PSK). The PSK is used with all devices connected to the same network. While the use of a PSK is generally considered adequate for consumer use in the home environment, it is generally not considered sufficiently secure for enterprise environments. To overcome the deficiencies of PSKs, a Remote Authentication Dial-In User Service (RADIUS) server is used to provide unique encryption keys for each user via centralized authentication, authorization, and accounting (AAA) management.

56. Why are WEP and WPA-PSK/TKIP no longer considered secure? What kind of wireless encryption should HDOs be using? How will this impact organizational support for wireless medical devices?

WEP and Wi-Fi Protected Access Pre-Shared Key—Temporal Key Integrity Protocol (WPA-PSK/TKIP) are no longer considered secure. Both protocols use a PSK, which is the essential weakness of these security schemes. Once the key has been shared to the wrong individual, access can be gained to the network, making any medical device connected to the network vulnerable to attack and potentially exposing protected health information (PHI). In addition, any PSK encryption is more vulnerable to “brute force” attacks.

57. What are the advantages of 802.11ac Wave2 over 802.11a/b/g/n? Are there any disadvantages besides the cost of replacing my wireless APs?

As with many other discussions of specific Wi-Fi protocol, a detailed discussion of 802.11ac Wave2 is beyond the scope of this document. Generally, 802.11ac Wave2 is considered to have greater range and data throughput than 802.11a/b/g/n. Part of this increase in data throughput is achieved by using MIMO. Another increase in throughput is due to “channel bonding,” allowing up to eight Wi-Fi channels bonded simultaneously into a single channel providing 160 MHz bandwidth. Channel bonding has the disadvantage of reducing the number of usable Wi-Fi channels in an enterprise environment by one half while increasing the throughput across the bonded channel.

In the 2.4 GHz 802.11b/g bands, there are only three orthogonal (non-overlapping) channels. So, although channel bonding is possible, it is considered a best practice not to allow it in a high-density enterprise environment. In the 5 GHz 802.11 band for 802.11n and the successor standard 802.11ac, there can be up to 12 bonded orthogonal 40 MHz channels.

58. Should I turn off lower 802.11b data rates to get better performance on my 802.11b/g network?

Many companies and hospitals have embraced the strategy of obsoleting 802.11b support to improve network efficiency. Since 802.11b and 802.11g use different modulation schemes, the network has to transmit management frames using 802.11b modulation to ensure that old clients can "hear" the management traffic. The lowest 802.11g data rate is 6 Mbps, so keeping the 5.5 Mbps 802.11b rate isn't a big hit, but keeping the 1 Mbps data rate means that management frames essentially take six times as long to transmit as they would on a pure 802.11g or 802.11g/n WLAN.

It is important to have a plan that includes an inventory of devices to ensure 802.11b is supported as long as 802.11b devices exist. Often, a first step is to disable the 1 and 2 Mbps data rates and leave 5.5 and 11 Mbps data rates. Only the oldest (earlier than ca. 2000) devices support just 1 and 2 Mbps, and these support the original 802.11 (not 802.11b) standard. 802.11b introduced 5.5 and 11 Mbps. 802.11g devices (starting ca. 2003) are backwards compatible to run on 802.11b networks and add data rates 6, 9, 12, 18, 24, 26, 48, and 54 Mbps.

59. What are Dynamic Frequency Selection (DFS) channels and what are the pros and cons of using them?

DFS is a Wi-Fi function that enables WLANs to use 5 GHz frequencies that would otherwise be reserved for radars, on the condition that if radar signatures are detected, the channel is vacated within 10 seconds.

DFS support almost triples the available channels in the 5 GHz ISM band. This allows for higher densities of APs, more Wi-Fi devices, and faster data transfer rates. For the U.S., there are nine non-DFS channels: 36, 40, 44, 48, 149, 153, 157, 161, and 165. There are 16 DFS channels: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, and 144. These channels are in the 5.25 GHz and 5.73 GHz frequency range. The IEEE 802.11ac standard takes advantage of the expanded range from eight to 16 DFS channels known as "regulatory -B domain" support. Wikipedia includes a table of all the DFS channels for various regulatory domains.[38]

When an AP detects a radar, it must vacate the channel. Most enterprise-class APs are constantly scanning other channels and can move quickly to another channel. Even so, some latency and jitter-sensitive applications such as VoIP might experience an interruption.

Before enabling DFS channels:

- Ensure that all client devices support those channels.
- Conduct a DFS survey to determine how often radar events occur. An Aruba Networks document[39] describes the behavior of 5 GHz client devices in the presence of radar and describes how to conduct a DFS survey. If the survey detects that particular DFS channels are often vacated, those can be excluded from the AP channel list.

- Conduct a risk analysis comparing the advantages of the increased bandwidth to the probability (based on the DFS survey) and hazard level of an 802.11 communication issue when a radar is detected. Consult 80001-1 and the associated technical reports for more guidance on managing IT networks that support medical devices.

Wireless Medical Telemetry Service

60. What is wireless medical telemetry?

Wireless medical telemetry is used to wirelessly monitor patients' physiological data in real time and detect life-threatening events. Patients wear wireless sensors that send real-time physiological data to a computer, which allows clinicians to monitor patients' conditions and detect events that require prompt intervention (e.g., cardiac arrhythmias).

61. What is the Wireless Medical Telemetry Service (WMTS)?

The FCC "allocated new spectrum and established rules for a Wireless Medical Telemetry Service (WMTS) that allows potentially life-critical equipment to operate on an interference-protected basis."[40] FCC 00-211 created the WMTS as a licensed-by-rule service that allows hospitals around the country to use these frequency bands for medical telemetry: 608–614 MHz (TV channel 37), and 1395–1400 MHz and 1427–1432 MHz (the L-band)[*], and notes that "these bands each have significant constraints, such that the entire allocation is unlikely to be available in any individual market."[41]

62. Why was the WMTS created?

The WMTS was created after an incident at Baylor University Medical Center in March of 1998. A dozen telemetry monitors suddenly stopped working due to a new DTV station that came online and operated in the same frequency band as the telemetry monitors. Please refer to this article, written by *The New York Times*.[42]

63. What does licensed spectrum mean?

Licensed spectrum is a band of radio frequencies in which licensees are legally entitled to operate free from interference from lower-status (e.g., unlicensed) users. See the FCC licensing web page.[43]

64. Does medical telemetry operating in the 608–614 MHz band experience interference now?

The root cause of interference for medical telemetry operating in the 608–614 MHz band has typically been due to one of the following reasons:

1. Two or more WTMS devices operating in the hospital (e.g., one ward was not aware of another ward's WMTS devices).

[*] There are some minor geographical modifications to the exact L-band frequencies.

2. Adjacent-channel interference from local DTV, which was anticipated in the rulemaking that created the WMTS.

3. A variety of in-hospital sources (including noisy motors in floor polishers [buffer problem], metal gurney rolling past a receiving antenna, CT scanners, and faulty fluorescent ballasts) have caused unintentional interference to telemetry systems that have no ability to confirm proper receipt of that data by the receiver, i.e., acknowledgments.[44]

65. What is the FCC 600 MHz incentive auction?

As part of the Middle Class Tax Relief and Job Creation Act of 2012, Congress required that the FCC repurpose and auction spectrum for commercial use (Section 6403 of the Act). The 608–614 MHz band of the WMTS is included in that law; the 1.4 GHz band of the WMTS is not. Since remaining DTV stations will be more optimally repacked into less spectrum, the eventual effect of the auction will be a more tightly spaced and more efficiently used broadcast band than we currently have; but this results in less "white space" between broadcasters for unlicensed use. To help appease supporters of unlicensed white space operations in the UHF band, the FCC proposed and adopted a sharing regime between medical telemetry and unlicensed operations in the 608–614 MHz band.

66. How did the FCC incentive auction impact devices operating in the WMTS and does it impact the 1.4 GHz WMTS bands?

The FCC revised its rules in 2015 to allow unlicensed TV white space (TVWS) to operate in WMTS 608–614 MHz band (TV channel 37), assuming the unlicensed TVWS devices stay a minimum distance from the hospital. In other words, each hospital should have a protective bubble around it where unlicensed TVWS devices are not allowed to operate on channel 37. The current rules do not guarantee that medical devices will NOT experience interference (e.g., the bubble is not big enough). Tests performed using real hospital WMTS systems have shown that interference can occur when unlicensed TVWS devices are within 2 km, whereas the FCC's rules allow such devices to operate within 350 m. Telemetry systems operating in the 608–614 MHz band depend on a noise-free environment to receive signals reliably. In the presence of interference, where the spectrum is not quiet, they experience data loss during patient monitoring.

The FCC incentive auction does not affect the 1.4 GHz channels of the WMTS.

67. How can hospitals respond to interference?

The FCC's current rules put the burden on the hospital to identify interference and file a waiver to increase the distance that applies to a facility. While investigating the source of interference and waiting for a waiver to be approved, the hospital must find alternate ways to monitor patients. By monitoring system performance, the hospital identifies an increased rate of interference, perhaps by observing physiological data dropout at the central monitoring station. The hospital investigates the source of the interference, which requires specialized experience and tools. If the source of interference is internal (e.g., another hospital ward using the same channels, a noisy motor, or a failing fluorescent light ballast), address the problem internally. If the problem is due to a TVWS device, file a waiver.

68. Why doesn’t the FCC reallocate the 2.4 GHz band for the WMTS?

In the FCC report and order that created the WMTS, the FCC allocated 14 MHz (more than the 12 MHz of bandwidth than the American Hospital Association requested). The FCC also wrote, “We wish to underscore that we do not anticipate any further allocations for medical telemetry devices and expect manufacturers and the health care community to ensure that this spectrum is used efficiently to meet long term needs.”[41] Viewed from another perspective, allocating the 2.4 GHz band for WMTS would require displacing several billion-dollar industries comprising Wi-Fi, Bluetooth, Zigbee, cordless phones, baby monitors, and other radios. It is worth noting that several physical layers that operate in the 2.4 GHz band support medical devices and medical telemetry. Finally, the 2.4 GHz band is an ISM band, which is reserved internationally.

Bluetooth

69. What is Bluetooth wireless technology?

Bluetooth is a wireless technology and standard for a two-way radio communication system operating in the 2.4 GHz ISM radio band for creating personal area networks. It is utilized license-free worldwide. Today it is included in every smartphone, laptop, and desktop computer, as well as many gaming consoles, and has versions that support very low power, relatively high speed, and relatively long distances (although not necessarily simultaneously).

The radio transport uses a technique called frequency-hopping spread spectrum (FHSS), dividing up that spectrum into “channels” and hopping between them in a pseudorandom sequence at 1,600 times per second. All data is transmitted using strong error detection methods so that, if a data packet is lost or corrupted, it will be rapidly retransmitted on a different channel than the troubled one, minimizing the effects of the interference.

70. What are the different kinds of Bluetooth (“classic,” “low energy”) and what are their frequency characteristics?

Bluetooth wireless technology comprises two “flavors” with many common characteristics. The original Bluetooth introduced in 2001 is often called “Bluetooth classic” but is formally called BR/EDR (Basic Rate/Enhanced Data Rate). The newer type of Bluetooth is called “Bluetooth low energy,” often abbreviated BLE or BTLE. BLE was introduced as part of the Bluetooth 4.0 specification released in 2010. As the name implies, BLE is significantly lower in power usage, but at lower data transmission rate than BR/EDR.

Although they share the same spectrum and many core characteristics and benefits, Bluetooth classic devices will not interoperate directly with single-mode BLE devices. Devices such as phones, tablets, and laptops will operate with both types of Bluetooth since they contain circuitry and software that can “talk” to both. These are commonly called “dual mode” devices.

Bluetooth range is typically 10–100 m (both classic and BLE), depending on many factors including implementation, power output, intervening walls and their composition, and antenna/device position and orientation.

Bluetooth BR/EDR divides the RF spectrum differently from BLE. BR/EDR divides the RF band into 79 channels of 1-MHz bandwidth, while BLE divides the RF band into 40 channels of 2-MHz bandwidth. Additionally, BLE dedicates three channels to advertising from devices to allow for faster connection and resulting in lower power consumption.

71. What are the different Bluetooth revisions? (Bluetooth 1, 2, 2.1, 4.0, 5, etc.)

Bluetooth wireless technology evolves to support new features and capabilities, as well as to resolve issues that are discovered (e.g., security). The Bluetooth standard revisions not only involve new features to match marketplace and technology needs, but also to address issues that are discovered that can affect security and interoperability between Bluetooth devices.

Features are sometimes deprecated, such as with the use of fixed-PIN for pairing after Secure Simple Pairing (SSP) was introduced, since PIN has many security and usability issues. Beginning with Bluetooth 4.x, a device may not use PIN for built-in authentication and encryption.

All Bluetooth devices are backwards compatible. The backwards compatibility modes default to the earliest of the devices in a connection. This means that many improvements and fixes will not be possible with older devices.

A summary of the Bluetooth revisions and key improvements is shown in the bulleted list below.

- Bluetooth 1.1 (2001)
  - First specification
- Bluetooth 1.2 (2003)
  - Improved coexistence with WLAN (adaptive frequency hopping [AFH])
  - Improved voice quality
- Bluetooth 2.0
  - 1.2 + Errata
- Bluetooth 2.0 + EDR (2004)
  - Enhanced data rate
- Bluetooth 2.1 (2007)
  - QoS, SSP, security improvements
- Bluetooth 3.0 (2009)
  - Bluetooth HS: alternate radio technologies (IEEE 802.11)
- Bluetooth 4.0 (2009–2011)
  - BLE/BTLE added

- Bluetooth 4.1 (2012–2013)
  - Simultaneous dual-role (central/peripheral) devices, IoT architectural enablers
- Bluetooth 4.2 (late 2014–2016)
  - Internet of Things (IoT) additions, IPV6, increased payload (higher data rate), security improvement
- Bluetooth 5.0 (late 2016)
  - Enhanced advertising
  - Higher speed
  - Longer range
  - Errata fixes

The Bluetooth Special Interest Group announced in 2018 that it would be deprecating and withdrawing older core specifications from 2.0 through 4.1 beginning in January 2019. All existing approved devices retain their approvals and listings.

72. What Bluetooth revision should hospitals be using?

While it is understood that existing devices are often difficult to replace, the recommendations below are based on known issues of security and interoperability:

- Device designers and manufacturers should always use the latest specification possible. Use only BLE devices tested and listed to Bluetooth 4.2 or later. Use only BR/EDR devices tested and listed to Bluetooth 4.0 or later.
- New devices and systems should be tested and listed to the latest specification, at least Bluetooth 5.0.
- If earlier versions are deployed, care should be taken to understand the potential security or compatibility issues involved and mitigate them by limiting access to information or areas of use.

73. Do all cellular phones, tablets, and laptop computers work with Bluetooth?

With very few exceptions, all computing devices introduced since 2016 support Bluetooth, including both Bluetooth classic and BLE.

74. What is Bluetooth pairing: How does it work and how has it changed with the various revisions?

Pairing is the process used by Bluetooth wireless technology to establish a secure wireless connection between two devices. Once devices have been paired, the information created may be stored to re-establish the connection in the future. Devices that have stored this information are “bonded.”

Pairing has evolved over the specification revisions. The original PIN code pairing method has been deprecated and should no longer be used due to security issues. Pairing in the latest specification revisions is much more secure.

The latest methods of SSP allow for several modes that depend upon the user interface and device implementation. It is important that the highest modes are used to allow for secure authentication and encryption.

Pairing is an optional process in the specification and suppliers are responsible for implementing and testing to make sure that the methods and modes are suited to the needs of the use model and data security. This should be disclosed as part of the cybersecurity hazard analysis for the device and system.

75. How does Bluetooth coexist with 802.11?

Bluetooth coexists well with 802.11 in the 2.4 GHz wireless spectrum by its use of FHSS technology along with AFH, which avoids transmitting on active 802.11 channels. The Bluetooth FHSS radio transmits for a short time on each channel and moves to another channel 1,600 times per second, minimizing potential interference.

As with 802.11, Bluetooth includes error detection and retransmission mechanisms. When there is a packet error or loss, that packet is quickly retransmitted and on a different channel than the one that experienced the packet error or loss, minimizing the effects of interference.

76. Does our microwave oven interfere with Bluetooth?

Yes, but this rarely occurs at a level noticeable to the user due to the narrow band of a typical microwave oven and Bluetooth error detection and correction methods.

77. How many Bluetooth devices can be in one room?

As with almost all RF performance questions, the answer depends on the exact scenario: What data are being transmitted? What are the power levels? What are the distances between devices? Etc. In practical usage, there is no limitation and multiple BT classic and BLE piconets can coexist in the same room. As an example, testing with 20 Bluetooth devices all streaming multi-channel ECG data worked smoothly and without data loss, and hundreds of devices coexisted during each Bluetooth “UnplugFest.”

78. Can a cellular phone that supports Bluetooth connect to hospital Bluetooth devices?

From the Bluetooth perspective: Yes, it is possible. Especially for BLE, connectivity depends on the application software (app) on the phone. From the perspective of medical devices in the hospital, the manufacturers of those devices must create a system so that only authorized devices are allowed to connect to the medical device safely and securely.

79. Is Bluetooth audio different from Bluetooth data? Can I have a call to my headset while other Bluetooth devices are communicating?

Yes, audio requires a high data rate and a constant connection.

Bluetooth classic supports up to three simultaneous audio devices connected to a computer or phone, or a combination of data and one or two audio devices.

Bluetooth classic can operate at (virtually) the same time as BLE in most devices. This means that a phone can be connected to a headset at the same time as it is connected to many BLE devices. An example is that a phone can be connected to diabetes devices such a glucometer and insulin pump at the same time as the user is making a phone call with a headset.

80. What are some Bluetooth-specific security considerations?

The most vulnerable state for a Bluetooth network is during the pairing process, which is used to establish a connection. Understand how pairing is completed and its requirements to ensure pairing is done securely. Legacy pairing, typically requiring the user to enter a 4-digit PIN, has been deprecated and should not be used.

The current pairing process has four methods of pairing to support different user interfaces, and some are more robust than others. Bluetooth security and privacy features are optional features in the specification, but may be required for medical device security. The manufacturer should be able to describe why the implemented security, privacy features, and pairing process are appropriate for the device.

The manufacturer should describe specifically what Bluetooth features, including security modes, are supported in each device and how they can support the HDO's HIPAA policies.

For more detail, including a complete Bluetooth security checklist, please read the NIST *Guide to Bluetooth Security*, which includes the following points. "Organizations should:

- Use the strongest Bluetooth security mode that is available for their Bluetooth devices.
- Address Bluetooth wireless technology in their security policies and change default settings of Bluetooth devices to reflect the policies.
- Ensure that their Bluetooth users are made aware of their security-related responsibilities regarding Bluetooth use."[45]

81. What are some security concerns for using BLE for wayfinding and patient engagement?

Wayfinding and other applications use BLE's beacon advertising capability to broadcast data. The data can be numbers, clear text information, or encrypted information, and might include ePHI. Depending on the type of data being transmitted, certain security measures may be necessary to comply with the HDO's HIPAA policy. The HDO should ask suppliers to disclose what is being transmitted and how/whether it is being protected, then determine whether this complies with the HDO's HIPAA policy.

Appendix A

Example Prepurchase Questionnaire for a Wi-Fi-Enabled Device

Question	Yes	No
1. Does the Wi-Fi adapter/device support the 5 GHz frequency band?	□	□
2. Does the Wi-Fi adapter/device support WPA2 (Wireless Protected Access) AES (Advanced Encryption Standard) with Enterprise Authentication EAP-TLS (Extensible Authentication Protocol—Transport Layer Security)?	□	□
3. Does the Wi-Fi adapter/device support SHA-2 (256 bit) certificates for network authentication?	□	□
4. Does the Wi-Fi adapter/device support 802.11r (Fast Transition for 802.1x)?	□	□
5. Does the Wi-Fi adapter/device support 802.11k (Neighbor List)?	□	□
6. Does the Wi-Fi adapter/device support 802.11v (Transition Control Management)?	□	□
7. Any restrictions on DFS (Dynamic Frequency Selection) or 802.11h channel announcements?	□	□
8. Any restrictions with channel bonding?	□	□
9. Any restrictions with DHCP (Dynamic Host Configuration Protocol)?	□	□
10. Any restrictions with DDNS (Dynamic Domain Name System)?	□	□
11. Does the device require static IP address?	□	□
12. Any restrictions for using hidden SSIDs (Service Set Identifier/No Broadcast)?	□	□
13. Does your device support the updated regulatory -B domain for the U.S. (channels and adjusted power settings)?	□	□
14. Does your device support IPv6 (Internet Protocol version 6)?	□	□
15. Can your device be set to a specific frequency band (2.4 GHz or 5 GHz)?	□	□
16. Is the wireless adapter 802.11ac capable?	□	□
17. Does the medical device require its own router to connect to the wireless network infrastructure?	□	□

Additional (Open) Questions

Question	Answer
18. Do you have a technical data specification for your devices with a recommended configurations guide? If so, please attach.	
19. Any known interoperability bugs or issues with [hospital] production [IT equipment vendor] WLC (wireless LAN controller) code (at present [current WLC code version], subject to change)?	
20. Any advanced WLAN configuration settings recommended (i.e., such as DTIM)?	
21. Does your medical device/app have an interoperability guide? If so, please attach.	
22. Do you have a central management solution to manage the configurations?	
23. Will your devices work with any MDM (mobile device management) solutions (i.e., AirWatch, Intune)?	
24. What is the recommended RSSI (Received Signal Strength Indicator) for your device to roam between wireless APs?	
25. What are the QoS (Quality of Service/WMM/802.11e) requirements, if any?	
26. Is your wirelessly connected device classified as an FDA Class I, II, or III device?	
27. Does the wirelessly connected device have any latency requirements? Does it use Transmission Control Protocol (TCP)/IP or User Datagram Protocol (UDP)?	
28. Any additional technical specifications/data that need to be shared?	

Appendix B
Glossary

Editor's Note: This glossary of wireless networking terms and definitions is based, in part, 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*.

5G The 5th generation cellular network technology, which has theoretical peak data rates of 10 Gbps.

802.11 A series of IEEE standards that relate to wireless local area networks typically in the 2.4 GHz ISM, 5 GHz ISM, and Unlicensed National Information Infrastructure (UNII) bands.

802.11a An IEEE standard that relates to wireless local area networks in the 5 GHz ISM and UNII bands.

802.11ac The 5th generation of 802.11 (Wi-Fi) physical standards with data rates up to 866.7 Mbps per spatial stream and up to four spatial streams (3.467 Gbps) that operates in the 5 GHz ISM band.

802.11ax (Wi-Fi 6) The 6th generation of 802.11 (Wi-Fi) physical standards with data rates of up to 1.2 Gbps per spatial stream and eight spatial streams (9.608 Gbps) that can simultaneously operate in the 2.4 GHz ISM and 5 GHz ISM bands. 802.11ax brings higher efficiency than its predecessor, 802.11ac.

802.11b/g An IEEE standard that relates to wireless local area networks in the 2.4 GHz ISM band.

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

Adaptive Frequency Hopping (AFH) A version of FHSS where the channel list is adapted (modified) to avoid channels on which there is interference.

Address Resolution Protocol (ARP) A protocol used by the Internet Protocol (IP) to map IP network addresses to the hardware (MAC) addresses. *See also* gratuitous ARP.

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

Attack Surface The sum of all the different points where an unauthorized user can try to enter data to, or extract data from, an environment.

Authentication The process of ensuring that a person/device/software is actually who/what it claims to be.

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

Bluetooth A wireless technology and standard for a two-way radio communication system operating in the 2.4 GHz ISM radio band and used to create personal area networks.

Bluetooth Low Energy (BLE/BTLE) A variation of the Bluetooth wireless technology designed for low power consumption.

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

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

Bring Your Own Device (BYOD) A user's electronic device used for corporate applications.

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

Citizen Broadband Radio Service (CBRS) A shared, broadband radio service in the frequency range of 3550–3700 MHz (3.5 GHz band) the FCC opened to commercial use in 2015 (FCC 15-47).[46]

Data Integrity Assurance that transmitted files are not deleted, modified, duplicated, or forged without detection.

Delivery Traffic Indicator Map (DTIM) Period In 802.11, the DTIM period indicates how often a beacon contains a traffic indication map. The traffic indication map is how an 802.11 AP informs a client's devices that the client needs to "wake up" and receive data from the AP.

Digital Enhanced Cordless Telecommunications (DECT) A digital communication standard primarily used for cordless phone systems and other wireless communications systems, e.g., patient monitors.

Distributed Antenna System (DAS) An antenna that physically extends over a large area such that it aggregates RF signals to and from devices across that large area to a single point.

Dynamic Frequency Selection (DFS) A Wi-Fi function that enables WLANs to use 5 GHz frequencies that would otherwise be reserved for radars, on the condition that if radar signatures are detected, the channel is vacated within 10 seconds. The available channel list is dynamically selected based on whether radar signatures exist in a particular channel.

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

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.

Encoder/Decoder (CODEC) A module that can encode and decode data.

Encryption The process of converting data into a form that is not readable/understandable by an unauthorized person or device.

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.*

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[47] and was updated by RFC 5247.[48]

Extensible Authentication Protocol—Transport Layer Security (EAP-TLS) A specific authentication method using the EAP authentication framework (RFC 5216).[49]

Forward Error Correction (FEC) A technique used in communication to control errors whereby redundant information is transmitted, which allows the receiver to detect and correct a limited number of errors.

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.

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

Gratuitous ARP An ARP response that was not prompted by an ARP request. The gratuitous ARP is sent as a broadcast as a way for a node to announce or update its IP address to MAC address mapping to the entire network.

Hazardous Situation Circumstance in which people, property or the environment is/are exposed to one or more hazards. *[ISO 14971:2019, definition 3.5]*

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

Healthcare Technology Management (HTM) The name of the field responsible for managing the selection, maintenance, and safe and effective use of medical equipment and systems.

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).

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

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.

Information Technology (IT) Synonymous with information systems. IT/IS refers to the development, maintenance, and use of computer software, systems, and networks,

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.

Internet of Medical Things (IoMT) and/or Internet of Health (IoH) and/or Medical Internet of Things (MIoT) The subset of IoT that includes medical- and health-related IoT devices.

Internet of Things (IoT) The extension of Internet connectivity into sensors and everyday objects, such as cameras, toasters, and refrigerators.

Intrusion Detection System (IDS) A system that monitors the wireless environment and detects unauthorized uses such as “rogue” APs, viruses, worms, etc.

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

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 Systems Interconnection reference model.

Medical Device Manufacturer (MDM) A manufacturer of medical devices.

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

Multiple-Input Multiple-Output (MIMO) The use of multiple antennas at both the transmitter and receiver to improve communication performance.

Orthogonal Frequency Division Multiplexing (OFDM) A method of encoding digital data on multiple carrier frequencies used in 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax (technically, 802.11ax uses OFDMA, a multi-user version of OFDM).

Personal Area Network (PAN) A computer network used for communication among computer devices, including smartphones and headsets, 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.

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.*

Signal-to-Noise Ratio (SNR) Signal power divided by noise power.

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

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.*

Temporal Key Integrity Protocol (TKIP) An interim security solution that legacy hardware could support when WEP was found vulnerable. *NOTE: Deprecated in 2012. Avoid purchasing new equipment that does not support WPA2. Also known under the 802.11 branding as WPA.*

Transmission Control Protocol (TCP) One of the core protocols within the Internet Protocol suite. *NOTE: Differs from UDP in that TCP is acknowledged and connection oriented.*

TV White Space (TVWS) Television frequencies allocated to a broadcasting service but not used locally.

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 is connectionless oriented.*

Validation A process or test to determine whether the device, under actual or simulated use conditions, conforms to defined user needs and intended uses.

Verification A process or test to determine whether 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 comprising 50 packets per second.*

Vulnerability A weakness that can be exploited to perform unauthorized actions within a computer system. *See also* 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).

Wi-Fi Multimedia (WMM) A subset of the 802.11e standard that provides a higher QoS 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. *NOTE: Deprecated in 2012. Avoid purchasing new equipment that does not support WPA2.*

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.*

Wi-Fi Protected Access 3 (WPA3) Wi-Fi Protected Access version 3, introduced in January 2018.

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 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).

Appendix C

Troubleshooting 802.11 Connectivity Issues

A first place to check is on the client device's service screen, which preferably provides statistics about the number of packets transmitted and the number of packets that are retried (retransmitted). A high retry rate (above 10%–20%) indicates that the client is having some difficulty reliably transmitting data to its receiver (an AP in the case of 802.11). Note that some low data–rate 802.11 devices can maintain a connection with retry rates as high as 80%. A second place to check is the wireless controller to see if the AP has high retry rates with that client (or all clients). If the SNR is low, move the client closer to the AP and see if the packet retry rate decreases.

High retry rates are due to a low signal level, a high noise level, or both. The next step is to determine whether the signal strength at the receiver is high enough. This can be done by checking the signal with a wireless sniffer, and/or looking at the wireless controller's logs for the AP. Some tools provide measures of both signal and noise levels. Because the wireless controller and packet sniffers can look for packets from a specific device, they can give the signal level for that device *if* the packet is received with the client's MAC address intact. If the packet can't be detected at all by these tools, then a spectrum analyzer may be used. A spectrum analyzer can measure the amount of time interference is present as well as the amplitude of the interference.

If the signal strengths are sufficient (802.11 standards provide tables of the minimum signal strength and minimum SNR to successfully reconstruct a packet) but there is a lot of interference, the next step is to use a spectrum analyzer and systematically go through the area(s) with interference to find the sources of interference and mitigate them. Mitigation might include removing the interference sources, moving the interference sources, decreasing the transmission power of those sources, or changing the frequencies used by either the wireless network or the interference source.

If the signal strengths are insufficient for the data rates being used, the data rates need to be decreased, AP spacing needs to be decreased, or client transmission power needs to be increased (this last option is usually not viable for battery-powered devices).

Look for asymmetrical signal strengths and/or SNRs. The case of APs transmitting at a power level far greater than that of client devices will exhibit client devices that successfully receive transmissions from the AP due to a high signal strength; however, the weaker transmissions from the client radios to the AP results in low signal strength at the AP and many failed packets, as indicated by a high number of retries by the client radios and many missing acknowledgement packets from the AP. In this case, a sniffer near the client would capture the client transmissions successfully, but not detect acknowledgements from the AP. Moving a sniffer near the AP, one would expect that the sniffer would have the same difficulty decoding packets as the AP.

It is helpful to have an RF heat map (i.e., measured amplitudes of RF signals at different points in the hospital across the RF bands of interest) of the hospital at system installation, which can be compared to the amplitudes at later times to determine where noise has increased.

For devices in the 2.4 and 5 GHz ISM bands, the interference is typically intentional; that is, due to other devices trying to transmit and communicate. For WMTS devices in the 608–614 MHz band, the interference might be from adjacent-channel TV stations (intentional) or emissions from faulty/poorly designed electrical equipment and motors (unintentional).

Other possible causes of interference include poor channel planning where neighboring APs are on the same channel (always a problem with 2.4 GHz Wi-Fi, where only three non-overlapping channels are available) and oversubscribing APs where there is insufficient bandwidth to support all of the clients. For more information on the former, see also Questions 12, 24, and 57. Solutions for the latter issue include increasing AP density with lower power for each AP (this works better when clients subscribe to the 802.11d power constraint element), limiting low data–rate support, and reducing the number of SSIDs.

There is a scenario where an AP can be set to high power, so the client measures a strong signal, has a high SNR, and an RF heat map shows full coverage. However, the AP receiving data from a low-powered client device receives the RF signal at a low signal strength and low SNR.

Appendix D

Example of Risk Analysis and Risk Mitigation for a Medical Device Using a Wireless Network

Continuous monitoring of the network is an effective way to mitigate risks by detecting issues before they result in a loss of communication. This monitoring should be done at the wired network and the wireless controller (including its coverage mapping tools). The data rates, retry rates, channel utilization, and performance of the wireless APs should be trended.

A manual site survey is an effective way to ensure that the SNR in the environment is high enough to support required bandwidth. It supplements what the wireless controller can see, as its view is limited by the position of the APs. Review of the signal and noise levels should be performed periodically and also upon major changes. When trends are in the wrong direction, proactively respond to increase the SNR and/or capacity before communication failures occur. For example, removing interfering devices decreases the system noise. Increasing AP density improves capacity and signal strength.

Mitigating risk for a medical device should start with *identifying the hazard*. The hazard could be defined as "not being able to send important alarm status to nursing work station." Once the hazard is defined, describe the *possible harm* and resulting patient outcome. Next you will need to determine the *probability of this occurrence*, or how often this will occur. The combination of harm and probability of occurrence is the risk, which is used to triage the most important items to address.

An example of risk analysis for a wireless patient monitor is given below. In some cases, statistical analysis may be used. When this is not available, seek input from experts.

a. Hazard: Patient monitor unable to transmit clinically important data such as alarm status.

b. Possible harm: Delay in treatment, which may lead to morbidity/mortality.

c. Probability of occurrence

   Primary flow (network operating as designed): Assume that the medical-IT network is designed and tested to support 99.9% successful packet transmission. Assuming 10,000 alarm packets are transmitted each day (average of 50 per patient, multiplied by 200 patients being monitored), then 10 packets would be missed. If patient monitors automatically retransmit alarm packets within a few seconds, typically the second transmission would mitigate the loss of the first packet. Assuming packet losses are independent of each other, one alarm in 1,000,000 would be missed after the first retransmission and one alarm in 1,000,000,000 would be missed after the second retransmission. The probability of occurrence of a missed alarm in this situation is so low that the risk (probability multiplied by harm) is acceptably low and no mitigation is required.

   In the case of primary AP failure: If there is no backup RF coverage, then all alarms for the patient area covered by the failed AP will not be transmitted to the central station. AP mean time between failures is 200,000 hours, so the annual failure rate is $1 - exp([24*365]/200000)$ or 3.13%. One expects 3.13% of APs to fail annually. Repair time is typically one to six hours, and an AP covers about 10 patients. This lack of coverage is determined to be unacceptable.

Mitigation: Install APs for redundant RF coverage so that if one fails, the backup AP provides coverage. Probability of two neighboring APs failing in the same year is 0.1% and failing on the same day is much lower.

d. RF Interference blocks transmissions

Mitigation: Conduct a site survey to ensure the system noise floor is low enough to support required bandwidth. Perform periodic (every six months) review of the noise level and upon major changes. Monitor the RF performance of APs and proactively respond to increases in noise floor (e.g., removing noise source, installing additional APs, etc.).

e. Other possible reasons for loss of data packets include overloaded network; interference from patient devices brought into the hospital; failure of IT switch, router, or wireless controller; AP's Ethernet cable unplugged; configuration changes to network incompatible with patient monitor; or firmware upgrade to network incompatible with patient monitor.

f. Other hazards include poorly protected data intercepted by a hacker, patient monitor's wireless interface is vulnerable to attack, patient moves into an area outside the AP's coverage, patient roams from one AP to another, or AP is on a DFS channel (see also Question 59) and a radar event is detected, causing the AP to change channels.

References

1. Lewis BD, Davis PT. *Wireless Networks for Dummies*. Hoboken, NJ: Wiley Publishing, 2004.

2. Coleman DD, Westcott DA. *Certified Wireless Network Administrator Study Guide*, 5th Ed. Indianapolis, IN: John Wiley & Sons, 2018.

3. Wireless LAN Professionals. WLW 023—Learning Wireless LAN Technologies. www.wlanpros.com/resources/wlw-023-learning-wireless-lan-technologies/. Accessed Oct. 17, 2019.

4. Amateur Radio Relay League. www.arrl.org/shop. Accessed Oct. 17, 2019.

5. Zavrel RJ. *Antenna Physics: An Introduction*. Newington, CT: American Relay Radio League, 2016.

6. Nichols EP. *Propagation and Radio Science*. Newington, CT: American Relay Radio League, 2015.

7. AAMI. HTM Resources Page. www.aami.org/membershipcommunity/content.aspx?ItemNumber=3186&navItemNumber=787. Accessed Nov. 19, 2019.

8. AAMI. *Going Wireless*. Arlington, VA: Association for the Advancement of Medical Instrumentation, 2013. http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/HT_Wireless/Going_Wireless_2013.pdf. Accessed Oct 17, 2019.

9. Hallas J. *Basic Radio: Understanding the Key Building Blocks*. Newington, CT: The American Radio Relay League, 2005.

10. Hudson J, Luecke J. *Basic Communications Electronics*. Lincolnwood, IL: Master Publishing, 1999.

11. National Instruments. RF and Communications Fundamentals. www.ni.com/product-documentation/3992/en/. Accessed Oct. 17, 2019.

12. Stoehr MD. *RF Basics*. https://pdfserv.maximintegrated.com/en/an/AN5300.pdf. Accessed Oct. 17, 2019.

13. Bluetooth Special Interest Group. Bluetooth Technology: Topology Options. www.bluetooth.com/bluetooth-technology/topology-options/. Accessed Nov. 13, 2019.

14. Revolution Wi-Fi. www.revolutionwifi.net/. Accessed Oct. 17, 2019.

15. wirednot. https://wirednot.wordpress.com/. Accessed Oct. 17, 2019.

16. Wireless LAN Professionals. www.wlanpros.com/resource/?wpv-category=blog. Accessed Oct. 17, 2019.

17. Jajszczyk A, Ed. *A Guide to the Wireless Engineering Body of Knowledge*. Hoboken, NJ: John Wiley & Sons, 2012.

18. Spectrum analyzer. https://en.wikipedia.org/wiki/Spectrum_analyzer#Radio-frequency_uses. Accessed Oct. 18, 2019.

19. Packet analyzer. https://en.wikipedia.org/wiki/Packet_analyzer. Accessed Oct. 18, 2019.

20. Wireless site survey. https://en.wikipedia.org/wiki/Wireless_site_survey. Accessed Oct. 18, 2019.

21. Wireless Medical Telemetry Service. https://en.wikipedia.org/wiki/Wireless_Medical_Telemetry_Service#WMTS_rules_by_FCC. Accessed Oct. 18, 2019.

22. Federal Communications Commission. Medical Device Radiocommunications Service (MedRadio). www.fcc.gov/medical-device-radiocommunications-service-medradio. Accessed Oct. 18, 2019.

23. FCC 11-176. Report and Order. https://us-fcc.app.box.com/s/zckv2qncfqrc10b7niy1hcr7klg5awr7. Accessed Oct. 18, 2019.

24. McGee MK. *XP Device Support Ends: Now What? Medical Device Expert Suggests Windows XP Security Strategy*, interview with Kevin Fu. www.healthcareinfosecurity.com/interviews/xp-device-support-ends-now-what-i-2250. Accessed Oct. 18, 2019.

25. AAMI. *Health IT Risk Management: A Practical Tool to Help Hospitals and Medical Devices Stay Secure in a Complex World*. https://rdcms-aami.s3.amazonaws.com/files/production/secure/Publications/Health_IT_Risk_Management.pdf?AWSAccessKeyId=AKIAJ44IQIZSE2C3ITYA&Expires=1582060119&Signature=AHMXjM2SldhNabV%2FJtddIC10lTg%3D. Accessed Oct. 18, 2019.

26. Baker SD. *Application of IEC 80001 in Avoiding Pitfalls of Wireless LAN System Design*. www.welchallyn.com/content/dam/welchallyn/documents/upload-docs/Research/Reference/Application-of-IEC-80001-in-Avoiding-Pitfalls-of-Wireless-LAN-System-Design_Reference.pdf. Accessed Oct. 18, 2019.

27. Raymond P, Baker SD. Risks, Challenges and Opportunities of Wireless Technologies in Healthcare: Wireless Testing in a Hospital. Presentation at: AAMI Wireless Workshop; October 4–5, 2012; Herndon, VA. http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/Summits/WirelessPresentations/Baker_Raymond.pdf. Accessed Nov. 19, 2019.

28. Department of Health and Human Services, Healthcare & Public Health Sector Coordinating Councils. *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf. Accessed Oct. 18, 2019.

29. Healthcare and Public Health Sector Coordinating Council Joint Cybersecurity Working Group. *Medical Device and Health IT Joint Security Plan*. https://healthsectorcouncil.org/the-joint-security-plan/. Accessed Oct. 18, 2019.

30. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed Oct. 18, 2019.

31. Grimes SL, Wirth A. *Medical Device Cybersecurity: A Guide for HTM Professionals*. Arlington, VA: Association for the Advancement of Medical Instrumentation, 2018.

32. Microsoft TechNet. Myth vs. reality: Wireless SSIDs. https://blogs.technet.microsoft.com/steriley/2007/10/16/myth-vs-reality-wireless-ssids/. Accessed Oct. 18, 2019.

33. National Electrical Manufacturers Association. *ANSI/NEMA HN 1-2019 Manufacturer Disclosure Statement for Medical Device Security*. www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx#download. Accessed Jan. 15, 2020.

34. Baker SD, Hoglund DD. Medical-Grade, Mission-Critical Wireless Networks. *IEEE Eng Med Biol Mag*. 2008;27(2):86–95.

35. ANSI/AAMI/IEC TIR80001-2-3:2011. *Application of risk management for IT-networks incorporating medical devices—Part 2-3: Guidance for wireless networks*. Arlington: VA: Association for the Advancement of Medical Instrumentation.

36. IEEE. IEEE GET Program—GET 802(R) Standards. https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68. Accessed Oct. 21, 2019.

37. IEEE 802.11. https://en.wikipedia.org/wiki/IEEE_802.11. Accessed Oct. 21, 2019.

38. List of WLAN Channels. https://en.wikipedia.org/wiki/List_of_WLAN_channels#5_GHz_(802.11a/h/j/n/ac/ax). Accessed Oct. 21, 2019.

39. Aruba Networks. Appendix D: Dynamic Frequency Selection Operation. www.arubanetworks.com/vrd/HighDensityVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=HighDensityVRD&file=AppD.html. Accessed Oct. 21, 2019.

40. Federal Communications Commission. FCC Establishes New Wireless Medical Telemetry Service. https://transition.fcc.gov/Bureaus/Engineering_Technology/News_Releases/2000/nret0009.html. Accessed Oct. 21, 2019.

41. FCC 00-211. Report and Order. https://transition.fcc.gov/Bureaus/Engineering_Technology/Orders/2000/fcc00211.pdf. Accessed Oct. 21, 2019.

42. Lewis PH. HDTV: Not heart-stopping, but a bit too close. *The New York Times*. Mar. 12, 1998:G9. www.nytimes.com/1998/03/12/technology/hdtv-not-heart-stopping-but-a-bit-too-close.html. Accessed Oct. 21, 2019.

43. Federal Communications Commission. Licensing. www.fcc.gov/licensing-databases/licensing. Accessed Oct. 21, 2019.

44. Sherman P, Campbell C. Assessing Existing Telemetry Systems for Risk of Electromagnetic Interference. *Journal of Clinical Engineering*. 2001;26(2):144–154.

45. Padgette J, Bahr J, Batra M, et al. *Guide to Bluetooth Security*. May 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf. Accessed Oct. 22, 2019.

46. FCC 15-47. Report and Order and Second Further Notice of Proposed Rulemaking. https://docs.fcc.gov/public/attachments/FCC-15-47A1.pdf. Accessed Nov. 4, 2019.

47. Network Working Group. Extensible Authentication Protocol (EAP) Proposed Standard Request for Comments. RFC 3748. https://tools.ietf.org/html/rfc3748. Accessed Oct. 24, 2019.

48. Network Working Group. Extensible Authentication Protocol (EAP) Key Management Framework Proposed Standard Request for Comments. RFC 5247. https://tools.ietf.org/html/rfc5247. Accessed Oct. 24, 2019.

49. Network Working Group. The EAP-TLS Authentication Protocol Proposed Standard Request for Comments. RFC 5216. https://tools.ietf.org/html/rfc5216. Accessed Oct. 24, 2019.

AAMI
Advancing Safety in Health Technology

901 N. Glebe Road, Suite 300
Arlington, VA 22203-
Phone: +1 703-525-4890
Web: www.aami.org