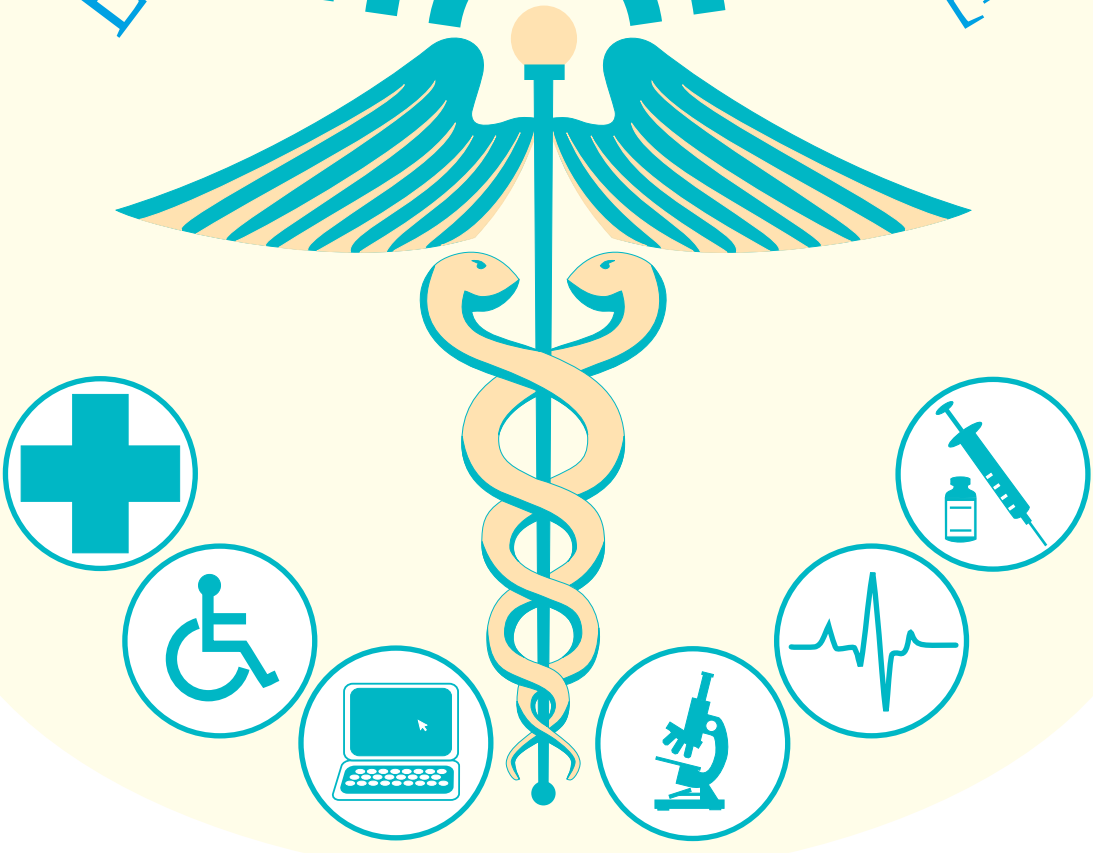
WI-FI ENABLED HEALTHCARE



Ali Youssef • Douglas McDonald II
Jon Linton • Bob Zemke • Aaron Earle

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

WI-FI ENABLED HEALTHCARE

Ali Youssef • Douglas McDonald II
Jon Linton • Bob Zemke • Aaron Earle

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

AN AUERBACH BOOK

Contents

Wi-Fi Enabled Healthcare
Ali Youssef, Douglas McDonald II, Jon Linton, Bob Zemke, Aaron Earle
Print ISBN 9781466560406

Wi-Fi Enabled Healthcare
Ali Youssef, Douglas McDonald II, Jon Linton, Bob Zemke, Aaron Earle
Print ISBN 9781466560406

Foreword

Rapid advancements in wireless technologies are transforming how healthcare is delivered, extending care and access to critical health data anywhere, anytime. This transformation presents health systems and care providers with a host of opportunities and challenges inside and outside their facility walls. The unprecedented speed with which these wireless and telecommunications advancements have converged upon health systems has led to an urgent need for information technology, biomedical, and telecommunication professionals to understand wireless architectures and the technical, regulatory, fiscal, and policy implications for implementing wireless networks in healthcare today and tomorrow. As wireless technology and processing speeds continue to evolve, healthcare providers can expect the demand for and use of more sophisticated untethered care solutions to increase. A focus on infrastructure to provide a solid, safe, secure foundation for these new care solutions is critical. This book seeks to close the knowledge gap on wireless infrastructure and provide practical technical guidance for health systems providers to ensure their systems provide reliable, end-to-end communications necessary to surmount today's challenges and capitalize on new opportunities as this technology evolves.

Highlights of wireless opportunities for healthcare providers include improvements in

- Workflow: point-of-care delivery and workflow enhancements provide remote and bedside registration, diagnostics, and treatment, as well as staff and patient tracking.
- Communications: real-time connectivity between nurse, staff, and patients.
- Transportation: real-time connectivity to emergency medical services and transport services, allowing for the transfer of critical information while patients are in route between care settings or departments, or in the home.
- Consumer engagement: consumers and care providers may now interact through remote communications and monitoring devices, enabling clinicians and patients to communicate timely health information, reminders, and support to each other in real time, changing patient–caregiver relationships.
- Workforce shortages: provides infrastructure for new care models and a flexible mobile workforce.
- Asset management: provides new tools for asset tracking.
- Data access: allows for the ability to collect, analyze, and share critical patient data, including access to electronic health records and health information exchange.
- Usability: provides introduction to consumer-based devices with a high level of user-centered design, improving ergonomics, and user interface flexibility.
- Innovation: provides the foundation for new applications such as Body Area Networks, deploying body sensors, untethering patients from monitoring devices, diagnostic testing equipment, and the need to remain in traditional health facilities for observation and treatment.

Challenges of wireless technologies include:

- Privacy and security: ensuring data and patient confidentiality are secure through both technical means and operational policies is essential.
- Regulatory requirements: federal, state, local, and institutional regulations may be nonexistent and/or may vary with regard to definitions of mobile medical device applications, physician and provider licensure and liability for use, etc., effecting how these tools are to be deployed and used.

- Infrastructure coexistence: very few healthcare providers have the luxury of building wireless infrastructure from scratch. A multitude of applications exist inside facilities, such as wireless LAN, telemetry, cellular and public Wi-Fi, with hundreds if not thousands of untethered devices producing interference and security challenges. Lead walls, elevator shafts, and historical piecemeal construction challenge essential reliable coverage.
- New infrastructure: staying abreast and understanding the technical, policy, and procedural requirements of new policies such as mBAN spectrum capacity and allocation is essential, but can be daunting.

Surpassing these challenges and capitalizing on current and future opportunities will require a solid understanding of wireless infrastructure. The shared experience and lessons learned from the authors provide essential guidance for large and small healthcare organizations in the United States and globally.

Edna Boone
Office of National Coordinator of Health (ONC)

Wi-Fi Enabled Healthcare
Ali Youssef, Douglas McDonald II, Jon Linton, Bob Zemke, Aaron Earle
Print ISBN 9781466560406

Wi-Fi Enabled Healthcare
Ali Youssef, Douglas McDonald II, Jon Linton, Bob Zemke, Aaron Earle
Print ISBN 9781466560406

Preface

Why write a book focused on wireless in healthcare? If you are interested in this topic chances are it's because you are somehow involved in this space either from IT operations, IT leadership, clinical engineering, healthcare administration, or a related field.

The backgrounds of the authors vary from network engineering to IT security, to biomedical engineering. Our knowledge is founded upon formal study and graduate studies, but what we have to offer that is unique comes from many hours spent in the trenches of healthcare IT operations. What we all have in common is that as we began designing, deploying, and supporting wireless networks for various healthcare accounts, we soon learned that these types of inpatient and outpatient facilities have unique mobility requirements that lead to interesting challenges. During the early years of WLAN deployments at the turn of the twenty-first century, most organizations that we jokingly referred to as "cube lands" had relatively simple requirements of employee laptop connectivity in conference rooms and workspaces. Seamless roaming, handheld devices, guest access, and mobile medical devices were years away from becoming mainstream. We were fortunate to be working in a complex environment that from the beginning had greater demand for mobility, complex user requirements, unique radio frequency challenges, and a plethora of use cases for mobile devices. Whitepapers on best practices for design and support did

not seem to cover the areas that we were working to address, such as clinicians with personal devices (including access points), VoWLAN coverage in elevators, and FDA-certified biomedical devices. BYOD was not a term a decade ago but that did not stop the demands for employee and patient personal devices on the networks.

What was out there was vendor-specific marketing focused around how their technology could solve all of our mobility aspirations. Sounds familiar? As our projects grew in scope, complexity, and outright quirkiness we began to document operational run books for the teams. Technology choices are only a small component of the operational support challenges that await a network deployment. These ops manuals become the basis for our architecture standards and best practices guidelines for support. Lessons learned in the trenches so to speak. As the wireless standards evolved from 802.11b to 802.11n, and mobile devices grew from a handful of Microsoft PDAs to thousands of IOS clients, so have our ops manuals. The one constant we have seen is that dependency and mission criticality of the wireless network is growing with no signs of slowing down. With this in mind the team thought we would share our experiences and lessons learned, and provide a guide that we could have made use of when we first embarked on our wireless journey in one of the largest healthcare systems in the country. We hope it will be of help.

6
Mobile Medical Devices

Wireless technology has played a significant role in reshaping healthcare over the last two decades. Wi-Fi began to impact the clinical workflow in a significant way starting in 1999. The two key catalysts that have propelled increased adoption within healthcare institutions are FCC regulations, as well as the evolution of the IEEE standards, and increasing maturity of the Wi-Fi Alliance. The other two major organizations that have helped push adoption are the Food and Drug Administration (FDA), and the Association for the Advancement of Medical Instrumentation (AAMI). Recent federal government mandates like the push to attain meaningful use have also contributed to driving increased adoption. Many areas have been impacted by mobility, including devices supporting voice and video, but the area that has seen the most dramatic workflow improvements is the medical device arena. With wireless medical telemetry systems (WMTS) on the decline, using Wi-Fi as a means of transporting data from medical devices to the network, and between sensors and medical devices, has been a growing field. Medical device vendors continue to struggle to integrate Wi-Fi into their devices, with hit-and-miss results. Prior to diving into specific use cases, the following section will address the roles that the various government and regulatory agencies have played in shaping the Wi-Fi-centric mHealth arena.

The FDA is heavily involved with clearing different types of medical devices to be introduced to the U.S. market. The Medical Device Amendments Act of 1976 lays the foundation for the 510(k) process, which is used to clear upwards of 90 percent of medical devices to be sold in the U.S. market. Thankfully this process is not as stringent as the processes that are used to introduce a new drug to market. Medical devices are classified into one of three classes as follows.

Wi-Fi Enabled Healthcare
Ali Youssef, Douglas McDonald II, Jon Linton, Bob Zemke, Aaron Earle
Print ISBN 9781466560406

Class I: Devices that are not intended to sustain life do not require undergoing the 510(k) process or clearance but needing to follow general controls. Tongue depressors and latex gloves are examples of Class I devices.

Class II: Devices that need to meet minimal performance requirements and need to be cleared for safety and efficacy using the 510(k) process. IV Pumps are a Class II device.

Class III: This class of devices is necessary to sustain life, and must undergo the 510(k) premarket approval process, and are often used in clinical trials prior to release. These include devices such as defibrillators and implanted medical devices.

Generally only Class II and Class III devices will require network connectivity and thus can potentially leverage Wi-Fi. The 510(k) process is often lengthy and involves substantial testing which is generally focused around patient safety and the efficacy of a given device. Network communications capabilities are often taken for granted and are an afterthought. Areas like how a device will function in a dense Wi-Fi environment, preferred frequency bands, and supported authentication and encryption schemes are generally farmed out to the manufacturer of the wireless card being used, with little consideration for wireless best practices. The line of demarcation between regulating a device as a medical device and regulating it as a communications device has prompted the FDA to work closely with the FCC when dealing with wireless medical devices. In 2011, the FDA released draft guidance on mobile device applications (Medical Device Data systems rule). The integration between these two organizations is crucial for the success of the mHealth space.

The FCC released the MBAN proposal in 2012 which allocates a dedicated spectrum for body sensors to transmit data in real time. The idea is that these types of sensors will result in a substantial return on investment for healthcare institutions by decreasing the risk of infections and promoting early decisions and better outcomes.

Although the FDA is starting to move in a direction that is helping drive mHealth forward, there is still much lacking. When medical device vendors design a device, it often takes upwards of a year to introduce it to market. In the telecommunications space, the span of a year can see tremendous improvements from the perspective of

standards, security, or bandwidth availability. By the time a device makes it to the market, the integrated Wi-Fi capabilities are often outdated. The device can have a lifecycle spanning upwards of 5 years, or longer in some instances. It is crucial for these types of medical devices to have a flexible networking architecture that allows for upgrading drivers and even hardware if needed, with minimal scrutiny from the FDA. If the sole functionality being impacted is Wi-Fi functionality, it would be beneficial to have a series of high-level wireless tests that can be conducted to clear the firmware, or even hardware upgrade path.

We only touch the tip of the iceberg when discussing medical devices. A new type of medical device that integrates with smart phones and tablets is really pushing the traditional boundaries with the FDA. This area, compounded by the explosive growth of healthcare-related mobile applications, has been forcing the organization to rethink and reinvent its review mechanisms.

In June of 2013 the FDA released a draft guidance pertaining to the cybersecurity of medical devices. The target audiences were primarily medical device manufacturers, and the document entitled "Content of premarket submissions for management of cybersecurity in medical devices" calls attention to intentional threats to medical devices. These range from Malware and viruses infecting medical devices to organized penetration and Denial of Service attacks. The ruling urges medical device manufacturers to develop a set of security controls to assure medical devices maintain information confidentiality, integrity, and availability. In part, this means implementing two factor authentication mechanisms including passwords, biometric identifiers, or smartcards in order to restrict the number of individuals capable of interacting with the product.

It can be argued that the FCC is one of the key reasons that wireless technology was able to thrive in healthcare. Since the organization released the ISM band for unlicensed use in 1985, and more recently dedicated a portion of the radio spectrum to WMTS in 2000, it laid the foundation for medical device manufacturers to start to focus on this space. The FCC continues to play a fundamental role in driving mobility in healthcare. The organization's National Broadband Plan released in 2010 along with the ruling allocating 40 MHz of spectrum—2360 to 2400 MHz—for use by medical body area networks

(MBAN) devices in 2012 is a testament to this. They have also been involved in creating some best practices documentation around securing wireless devices. In an effort to remain a leader in the mHealth space, in 2012 the FCC announced that it would be adding a position of Health Care Director to continue to drive innovation in this space. The FCC continues to work with the FDA to ensure that available spectrum is allocated to promote mHealth as much as possible. They have been making every effort to foster innovation.

The AAMI has always been a fundamental player in medical device innovation and design. The organization has been developing standards for medical device design for decades. Wireless medical devices have traditionally been viewed like any other medical device. The typical AAMI audiences are clinical or biomedical engineers who generally deal with the maintenance and repair of medical devices. As medical devices become more dependent on networks and make use of Ethernet and Wi-Fi, the organization has been promoting the need for collaboration between IT and clinical engineering. Many healthcare institutions have taken this mantra to heart, and have shifted their reporting structure so that clinical engineering staff reports to IT leadership. This is an inevitable step given the growth of Wi-Fi-capable medical devices.

By leveraging Wi-Fi, medical device manufacturers have ventured into a shared medium that is outside of their control. When one also considers that many medical devices leverage fairly widespread core operating systems, like Windows, the number of variables that can cause data transmission issues grows. AAMI released the IEC 800001-1 series of standards between 2008 and 2012. These are intended to apply appropriate risk management to IT networks that support medical devices. This is in line with ISO 14971. The standards address safety, system security, and effectiveness, which are generally regarded as necessities for patient well-being. It incorporates best practices for risk management as well as change release management. These are in line with ITIL is the most popular and widely accepted approach to service management. It stands for information technology infrastructure library methodology which is well adopted in the pure IT arena. "Accordinding to the AAMI (Association for the Advancement of Medical Information) IEC 80001-1 it defines responsibilities for parties such as medical device manufacturers,

non-medical device manufacturers, the responsible organization, IT-network integrator, and potentially others, engaged in installing, using, configuring, maintaining and decommissioning IT-networks incorporating medical devices." There are four key areas that the standard highlights:

- The three risk components to be managed are safety, effectiveness, and security—and in that order of priority.
- It is ultimately the responsibility of the "responsible organization" (typically, the healthcare provider) for risk management of medical devices interacting with an IT network.
- "Responsible organization" includes health-delivery organizations of all size, such as physician single and group practices, as well as hospitals, clinics, etc.
- For the objective of 80001 to be met, the "responsible organization" will need to work closely with medical device manufacturers and providers of information technology.

The AAMI has paved the way for healthcare IT staff to be able to reach out to medical device manufacturers directly and work on fine tuning the network performance of a given device. Some examples of this are highlighted in the use case section of this chapter. The organization continues to provide best practices for managing wireless medical devices in their publication *Biomedical Instrumentation and Technology*. In addition, the AAMI established the Wireless Strategy Task Force (WSTF) in 2013. The group, comprised of manufacturers, regulators, users of technology, and other interested parties—is developing educational resources and tools and sharing best practices to address wireless challenges in healthcare. Group priorities include clarifying roles and responsibilities in the wireless arena, managing spectrum to improve safety and security, designing wireless infrastructure for high reliability, learning from other industries, managing risk and preventing failure. The group released a special compilation of articles in 2013 entitled "Going Wireless", which is a great resource for anyone working with mobile medical devices (https://www.aami.org/hottopics/wireless/AAMI/Going_Wireless_2013.pdf).

There are many other organizations that can be mentioned in these sections, such as the National Institute of Standards and Technology (NIST), the Healthcare Information and Management Systems

Society (HIMSS) and its mobile initiative mHIMSS, and the federal government, but the last one that will be discussed is the Wi-Fi Alliance. The background of this organization was discussed in the introduction, but for the purposes of this chapter, it is important to note that the Wi-Fi Alliance has been instrumental in publishing guidelines for deploying, securing, and leveraging Wi-Fi in healthcare.

New wireless medical devices are a blessing; they can also be difficult to troubleshoot, as many large medical device manufacturers such as GE, Medtronic, Philips, Baxter, and CareFusion, are designing and adapting medical devices for use on unlicensed radio frequencies. Often, manufacturers will cut costs by using noncompliant or out-of-date wireless devices (adapters, bridges, etc.) embedded in the medical devices. This effort to reduce cost and to gain market share has been a growing challenge for network administrators in healthcare. From diagnostics and monitoring, to the operating theatre and managing patient medical records, demand on wireless technology is more complex and mission critical in the healthcare industry. As medical device manufacturers race to introduce new devices, in many cases they must adhere to HIPAA-HITECH requirements and the FDA's 510(k) approval process. Healthcare organizations often face a lack of central control over procurement because departments have their own budgets and purchasing power. As ubiquitous Wi-Fi is becoming a reality, it is increasingly challenging to manage existing and legacy wireless medical devices while continuing to drive forward and utilize the latest available technology. Often manufacturers will take shortcuts by introducing an add-on Wi-Fi integration using wireless bridges, or will opt to utilize lower-end, cheap wireless cards in their equipment. This makes managing wireless medical devices a challenge requiring a close working relationship between clinical engineering and IT.

When it comes to patient data, securing medical devices and their data is vital to providing safe and effective healthcare. As Wi-Fi is growing the risks associated with the technology are inherent and are becoming more lucrative for hackers to try and take advantage of. Some of these risks are associated with security, availability, quality of service (QoS), and privacy. As the healthcare industry continues to expand and enter the ever-growing wireless space, including patient monitoring equipment, physicians' PDAs and laptops, and

Wi-Fi Enabled Healthcare
Ali Youssef, Douglas McDonald II, Jon Linton, Bob Zemke, Aaron Earle
Print ISBN 9781466560406

wireless-enabled medical devices, the risks associated with their use also rise. Some healthcare organizations have stayed ahead by deploying secured wireless networks for their medical devices. They often have to tweak their network to accommodate nonstandard or legacy medical devices.

Different organizations and departments within the hospital often mandate the wireless medical devices to purchase. In order to avoid a chaotic situation, they must be required to utilize risk management techniques and to thoroughly test each and every device that is being proposed for deployment on the Wi-Fi network. If any of the devices cannot meet minimal security requirements, they need to be identified.

The rapid pace of wireless medical device procurement presents an opportunity to create a focused certification process for the wireless medical devices. The certification process entails thoroughly testing the wireless medical device, and clearly identifying clinical workflow and support expectations. The IT department and clinical staff can work together to create a detailed inventory of all the wireless medical devices deployed in the hospital. Once that is done an OLA (operational level agreement) and SLA (service level agreement) can be set up to describe the maintenance and support matrix for each type of device. Proper planning and design are important to ensuring that the wireless network will support certain devices. Healthcare institutions wishing to manage their wireless medical devices should develop a consistent process for onboarding devices as well as phases for bringing all of their wireless medical devices up to a minimal set of authentication and encryption requirements.

The current industry consensus is that the best practice for wireless medical device authentication and encryption is using 802.1x with EAP TLS and AES encryption. This enforces mutual authentication and requires each medical device to have an x.509 certificate installed before it is allowed onto the wireless network. Due to the wide spectrum of device wireless capabilities, it is often necessary to use a phased approach to manage wireless medical devices and promote ongoing authentication and encryption best practices. HIPAA advisory and wireless interoperability-certifying Wi-Fi Alliance has acknowledged that the typical 802.11 security features such as WEP and/or shared key authentication are not secured enough. The phases are outlined in the bullet points below:

- **Phase 1:** All medical devices that support a certain authentication and encryption should be configured to use a dedicated SSID, keeping the number of SSIDs as low as possible. This phase is targeted at minimizing the amount of wireless overhead traffic. IT and clinical engineering staff need to consolidate a detailed inventory of all wireless medical devices in the hospital. This should include the make and model of the device, network connectivity requirement, device classification, supported spectrum, and high bandwidth requirements. This process will provide more insight into which wireless medical devices are capable of handling and supporting certain authentication and encryption methods.
- **Phase 2:** The purpose of the medical device policies on the network is to ensure that each device is suited for its purpose and meets clinical and patient needs, to make sure that the device complies with safety and quality standards. Since medical devices are regulated by the FDA, their design and operation cannot be modified by the end user. For many years, device manufacturers have been responsible for the installation, service, and support of their devices, including the network. This has resulted in several small independent networks in the hospital. As wireless technology continues to expand, hospitals feel the increasing financial pressure to deploy medical devices on their existing enterprise network. Network policies need to be applied to limit medical device network access to required IP addresses.
- **Phase 3:** Continuously refresh medical devices that do not support WPA2 EAP TLS. This should eventually result in one SSID using EAP TLS.
- **Phase 4:** Implement EAP TLS. The complexity associated with deploying EAP TLS is dependent on whether the hospital has a PKI and a certificate authority in place. Building such a system can be an expensive undertaking.
- **Phase 5:** Develop an overall stringent wireless security policy for medical devices that is interdepartmental and ties into IT governance, security, and procurement. Part of the policy needs to be ongoing device certification as a part of onboarding.