Publicly available March 12, 2014, revised March 22, 2018.

Building a Reliable Wireless Medical Device Network

By D Hoglund,[1] and V Varga[2]

[1]Integra Systems, Inc.

[2]Global Technology Resources, Inc.

ABSTRACT

How to design and test the most effective and secure wireless medical device connectivity applications that will provide the true mobility experience that is needed in the 2018 healthcare marketplace. Today's medical devices will need to be connected to provide the data to the electronic medical record. This connectivity will be either real time or on a non real time basis. In either case; the majority of this data transfer will move toward a wireless medium from a legacy wired connection. The following will discuss best practices for wireless network design based upon application requirements; but also the protection of any data regarding cybersecurity requirements. The author has over three decades of medical device knowledge sense but also two decades of wireless and security integration knowledge sense. The take away is to understand the best practices and how to apply this to product design and the overall enterprise implementation into the healthcare ecosystem of connected devices.

Keywords – *wireless, WLAN, network, acute care, patient monitoring, IEEE802.11, WMTS, telemetry.*

INTRODUCTION

A brief history of the WLAN-enabled medical device.

Historically, patient-wearable monitoring – commonly referred to as telemetry – required its own custom designed and proprietary radio system and coaxial cable infrastructure for unidirectional communication. This infrastructure was built around regulatory domain-controlled technologies, such as Wireless Medical Telemetry Service (WMTS) in the United States. While these designs proved to be reliable, they were often expensive, unique to each manufacturer, and lacked enterprise management and/or troubleshooting capabilities. These telemetry systems were generally confined to individual care units within the healthcare facility and utilized several to 100 or more dedicated telemetry patient channels.

For the past several decades networked bedside (or acute care) patient monitoring was confined to proprietary, standalone networks for communication from the bedside monitor to the central station. This was, and is even today, often the de-facto standard methodology in the majority of critical care units on a global basis.

Over the past decade, many medical device manufacturers have incorporated WLAN in their devices for a multitude of use requirements. This has included the next generation of smart infusion pumps, portable patient monitoring, and within the past five years, telemetry.

Modern enterprise networks, both wired and wireless Ethernet systems, have progressed to the point where they, if designed and installed correctly, have proven to be cost effective and reliable – as demonstrated by hundreds of thousands of mission-critical WLAN networks deployed on

a global basis in many industries. As a result, both medical equipment manufacturers and healthcare institutions are looking to leverage their nearly ubiquitous WLANs by utilizing them for network-enabled medical devices.

Clinical benefits of having a WLAN throughout the healthcare institution

The healthcare industry was an early adopter of WLANs because they enabled more timely and accurate bedside medical statistics recording, voice-over-IP-over-Wi-Fi, asset location, and guest Internet access – which benefitted clinicians, IT and biomedical groups, as well as patients and their families.

This new methodology of networked patient monitoring has many clinical benefits. Specific to telemetry and patient monitoring, an omnipresent WLAN can now enable the following:

- **Expansion of telemetry area coverage:** The telemetry system can operate across the entire facility, and not be limited to specific care areas. The trend is to increase telemetry usage across a common enterprise network, versus managing hundreds of standalone monitors.
- **Increased reliability:** Patient monitoring can leverage proven networking technology that is consistent in design and deployment. This networking infrastructure can provide true bi-directional communication for increased overall system reliability.
- **Increased space utilization and patient safety:** Having all monitors networked through the WLAN gives the hospital the flexibility to monitor patients anywhere in the hospital. For example, if the Emergency Department is at capacity, they can add extra monitored beds in another unit, thereby keeping the patient in the delivery network, versus having to divert the patient to another facility because of the lack of monitored beds. Having additional monitored beds also enables hospitals get patients out of higher acuity, and higher cost, settings.
- **Reduced risk of undetected events:** For example, if a prior cardiac patient comes in for an orthopedic procedure, the orthopedic nurse could easily have a cardiac trained nurse observe that patient using WLAN monitoring while the patient is being treated for that orthopedic procedure.

SUITABILITY OF WLAN FOR PATIENT MONITORING

Overview

Any wireless network is dependent upon proper planning, design, and implementation, taking into consideration the internal and external variables that may impact the network's performance and reliability. Such internal and external factors include high availability (HA) network infrastructure, radio frequency (RF) interference, Quality of Service (QoS) requirements, and cost budgets. In terms of suitability of the WLAN for patient monitoring, the healthcare institution must consider the requirements of the specific applications that will run over the WLAN. Any patient monitoring network has to be 100% reliable around-the-clock, 365 days a year, while communicating alarms, events, and recordings in real time.

Suitability Factors

The following factors influence the suitability of a WLAN to support a patient monitoring system:

- **Design of the WLAN:** Over the last 15 years, WLAN design has migrated from a simplistic paper-based approach to a very scientific methodology utilizing computer-based predictive modeling tools and onsite RF spectrum analysis to identify the sources of any potential RF interference. This methodology takes into account building materials, client device density, Wireless Access Point (WAP) placement, antenna patterns, RF link speeds, and RF channelization/ power and then creates a predictive model with 98% to 100% accuracy of design. In addition, a proper logical design must be created to define IP addressing, VLANs, multicast, DHCP, QoS, and other network-layer settings that affect WLAN quality and reliability. When using these tools, the hospital can have confidence that the network they install will need little to no modification after installation.
- **Installation and troubleshooting:** A well planned and designed LAN and WLAN is the foundation for a well performing patient monitoring system. As mentioned above, predictive WLAN modeling tools ensure a design with over 98% accuracy before implementation. For the few instances where the

WLAN design may incorrectly place Wireless Access Points (WAPs), WAP location modifications can easily be made in the field at the time of deployment. When installing a WLAN, all operational settings are configured in a central WLAN controller that interfaces with the facility's core network and allows for efficient network communication. In addition, depending on the size of the WLAN, a separate WLAN management system may also be implemented to provide a single "pane of glass" for the management, monitoring, alarming, troubleshooting, reporting, and assurance of consistent configurations across multiple WLAN controllers. All of these improvements make the implementation of a reliable LAN and WLAN scientific and predictable.

- **Interference:** While RF interference is always a possibility, the modern WLAN generally has spectrum analysis functions built into the network as a whole. This allows for constant monitoring of the network for any interference and acts to either issue an alarm to the network administrator or automatically mitigate those specific interferers. As good design practice, an onsite spectrum analysis should be performed to determine any RF interferers present in the facility in the 2.4GHz and 5GHz bands and their potential impact.
- **Reliability:** Today's WLAN is an intelligent network. Although WAPs have a mean time between failure (MTBF) of over ten years, this network can automatically sense and alarm if a WAP fails or is not performing as expected. Good WLAN design practices dictate overlapping adjacent WAP cells to ensure seamless client device roaming across the network. Even if an individual WAP fails, radio output power in adjacent WAPs can be set to automatically increase/decrease to ensure adequate coverage. In addition, High Availability (HA) designs feature redundant WLAN controllers that will failover in a seamless fashion in the event of a network controller failure.
- **Scalability:** In the past, understanding how the WLAN client density may increase was a challenge. WLAN designs must anticipate the potential number of client devices such as patient monitors that will be used over the life of the WLAN. Today there are tools from such companies as Ixia (www.ixiacom.com) that allow end users and WLAN device manufacturers to assess the scalability of a WLAN. Given the new higher-speed WLAN standards, it is common to build and scale networks to thousands of users to support data, voice, video, and WLAN-enabled medical devices.
- **Two-way communication:** Previous generations of proprietary wireless communication for telemetry was unidirectional; WLANs offer two-way or bi-directional communication. Two-way communication supports the latest generation of patient-worn monitoring devices. These devices send patient vital signs data to the central monitoring station for display and alarming, as did yesterday's telemetry transmitters, but they also display and alarm locally. So, if the patient accidentally walks outside of the Wi-Fi network coverage area, the patient will continued to be monitored locally. The caregiver is therefore able to monitor the patient without compromising the mobility of ambulatory patients.
- **Cost issues:** Healthcare systems are under tremendous cost pressures, so the more value that they can realize from a technology investment, the better. In the case of patient monitoring, this is yet another application across which to allocate the fixed WLAN cost. More than likely, the investment in the WLAN was made for Bar Code Medication Administration (BCMA), wireless voice-over-IP (VoIP), real-time location services (RTLS), and/or "smart" infusion pumps. Adding WLAN-based patient monitoring may add some small incremental costs, but this application can be amortized over a number years with the other applications to improve the return on investment (ROI).

Wi-Fi vs. WMTS cost comparison

The costs of implementing patient monitoring on Wi-Fi are significantly less than on a WMTS network. The following cost comparison tool provides a general indication of costs involved.

TABLE 1. WLAN vs. WMTS cost comparison tool

WMTS vs. WLAN Infrastructure Price Model		
WMTS DESCRIPTION	**INPUTS**	**COMMENTS**
Current area for WMTS telemetry	200,000 sf	Diversity antenna coverage
Desired area for WMTS telemetry	1,000,000 sf	Diversity antenna coverage
Cost psf for WMTS telemetry	$1.50	Cost per square foot
	RESULTS	
Additive new WMTS area coverage	800,000 sf	
Total cost for **additive** new area coverage (608MHz-1.4GHz)	**$1,200,000**	
WLAN DESCRIPTION	**INPUTS**	**COMMENTS**
% of 'Desired area for WMTS telemetry' currently covered by WLAN	60%	
Does WLAN provide for -67 dBm coverage?	No	
Cost psf for WLAN	$1.00	Hardware, software, licensing, design & deployment services
Qty of services currently on WLAN	3	Examples: data, VoIP-over-WiFi, video, biomed/infusion pumps, RTLS, guest access
	RESULTS	
Additional WLAN area for 'WMTS additive new area coverage'	400,000 sf	To satisfy the clinical requirements for patient monitoring
WLAN area needing remediation	600,000 sf	
Costs for extra WLAN coverage for patient monitoring	$400,000	
Costs for WLAN remediation coverage to -67dBm	$240,000	Remediation for the patient monitoring area only, not the complete WLAN coverage
WLAN validation services costs	$100,000	
Total WLAN costs	**$740,000**	
Total WLAN costs amortized over services	$246,667	
WLAN vs WMTS Infrastructure Cost	**$460,000**	**WLAN savings over WMTS**

BEST PRACTICES

The following are best practices for maximizing reliability and uptime when implementing patient monitors on an existing wireless LAN:

Start with the right "wireless radio design" within the medical device

One popular misconception that frequently compromises performance is that "all IEEE802.11a/b/g radios are created equal." On the contrary, the quality of radio devices varies, and if a medical device manufacturer selects a sub-par, low-cost radio, it can undermine the performance of a life-critical medical device that costs thousands of dollars. Device testing is the key to protecting

yourself from buying a device with a sub-par radio. More on that in the next section.

Another costly misconception is that a radio obtaining a stamp of approval from the Wi-Fi Alliance means everything will work fine; but there's more to it than that.

The Wi-Fi Alliance was founded in 1999, the same year that the IEEE approved the extended version of 802.11 (802.11b) standard for the specific purpose of ensuring interoperability between client radios and wireless access points.

The interoperability testing conducted does not include modeling the specific characteristics of a data, voice, video, or medical device client or the simulation of different mixed client traffic load environments; nor does it measure application performance. Obtaining the Wi-Fi Alliance's stamp of approval is a great start, but it's far from the end. The fact that a radio is Wi-Fi approved, or subscribes to 802.11i and 802.11e, does not demonstrate how well the roaming algorithms will work, or assess the passing of security supplicants. Many healthcare institutions employ WPA2 or other enterprise-level WLAN security methods but differ in how they implement security methodologies, which in turn impacts device and application performance.

In selecting the optimal WLAN-embedded radio, device manufacturers must assess the ability of the components to meet their intended use for quality of service, roaming, and varying security implementations. As the mobile healthcare ecosystem grows ever more complex, embedded radio strategies must be able to accommodate all enterprise-grade security strategies and effectively roam amidst a myriad of traffic types throughout a highly mobile environment.

It behooves the hospital to choose devices that contain radios that meet their current requirements in order to provide a foundation for future requirements.

Device testing: what it is and why it's important

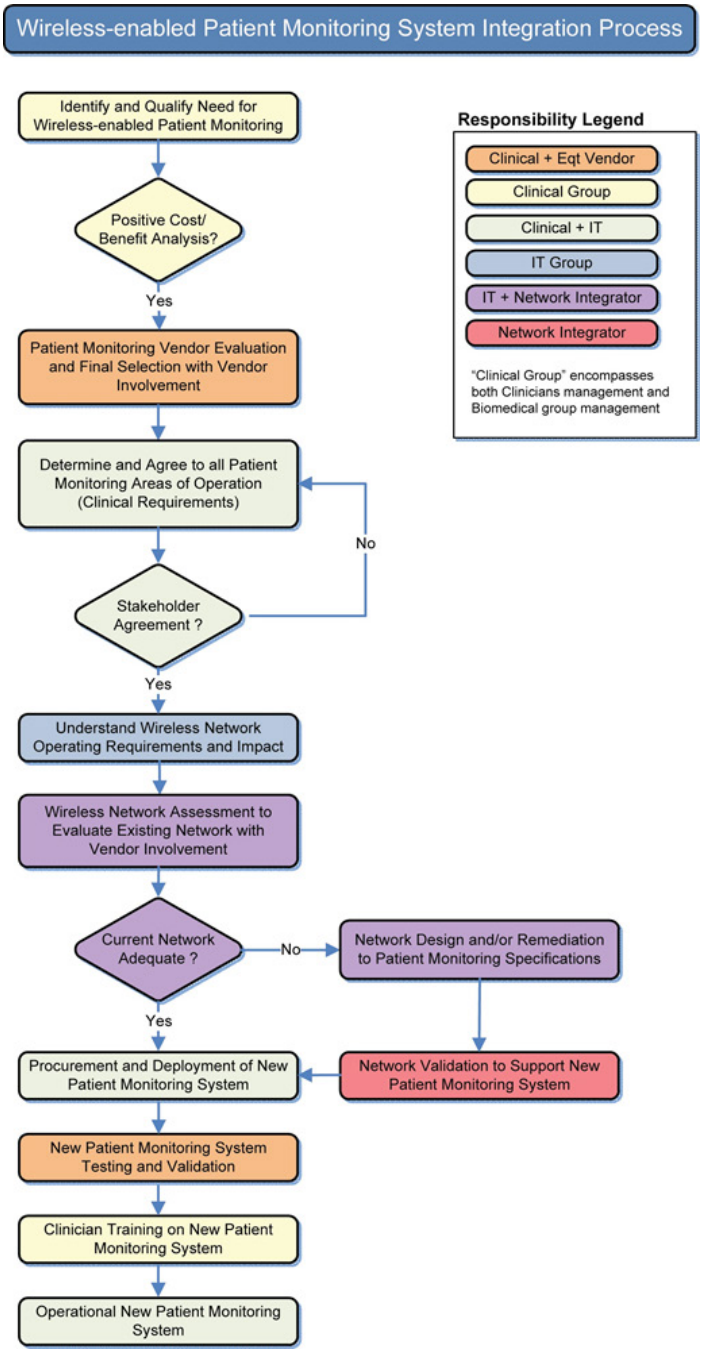
The device manufacturer is responsible for testing medical client devices during validation and verification. A comprehensive methodology for testing the device proceeds from highly controlled lab testing to assessing performance in the field via open air. Testing should include validating components such as radios, chipsets, and driver firmware and, once that is completed, progress to assessing the real-world performance of the medical device itself.

Hospitals have the right to ask manufacturers if their devices have been tested or installed successfully in a similar configuration to what they are considering. The proven methodologies should include:

1. Base-lining network performance using "golden" clients to obtain a "best-case" use model
2. Base-lining device performance under ideal network conditions where it's the only client communicating with WAPs under optimal conditions
3. Assessing range and roaming capabilities by varying RF signal attenuation to prompt devices under test (DUTs) to move away from and between specific WAPs. This includes:
   - Determining device association to the WLAN at various ranges
   - Measuring the accuracy of device throughput, latency, and packet loss characteristics
   - Assessing performance as devices travel across multiple WAPs to emulate patient mobility. Testing should progress from simple setups using only two WAPs at a time to complex scenarios where the device sees multiple available access points broadcasting at different signal strengths.
4. Assessing real-world performance and security by simulating live network conditions. Generating high traffic loads and interference allows the resilience, coexistence, and security capabilities of devices to be realistically and thoroughly assessed. User-configured clients should be generated to populate a realistic network ecosystem containing device traffic typically found in healthcare environments – voice over IP, data from wireless infusion pumps, wireless laptop transactions, video, etc. – all generating simultaneous network traffic.
5. Measuring interoperability with multiple WAPs and mobile clients and major customers' preferred WLAN equipment vendors
6. Quantifying application performance and quality of experience (QoE) from the user perspective

7. Reproducing field conditions and modeling "what if " scenarios in the lab to simulate individual hospital environments

FIGURE 1. Wireless patient monitoring integration process



8. Onsite assessment to ensure successful deployments out of the gate

9. Ongoing lab and site testing of network firmware changes and devices software upgrades

The WLAN patient monitoring deployment: what and why

In the area of patient monitoring, the actual patient-use model is critical to a successful monitoring selection and implementation. Before the technical requirements can be solved, the clinical requirements need to be addressed and understood, including:

- Where are the patients going to be monitored? A good starting point is to sit down with CAD drawings of the hospital floor plan and have clinical staff highlight all the areas where patients need to be monitored. For example, would a patient need to be transported from the ICU down the elevators to radiology and/or therapy areas? If so, then adequate wireless coverage would be needed to ensure real-time connectivity.
- How many patients are going to be monitored simultaneously, at maximum patient census?
- Where will the staff monitoring these patients be located?

Once the clinical requirements are vetted out and agreed to, then the technical requirements can be addressed. The following questions should also be discussed:

- What are the anticipated growth requirements (scale)?
- What is the current network infrastructure in place to support the new patient monitoring system requirements?
- What, if any, network remediation needs to be completed?

Based upon an understanding of the medical device's network characteristics and the existing network infrastructure, an accurate WLAN design can be initiated. The

FIGURE 2. Example of marked up hospital floor plan, highlighting all places where patients will be monitored

design tasks may include creating a completely new design or modifying the existing WLAN. This design can be then handed off to the hospital's integrator for any potential remediation and/or additional infrastructure.

FREQUENTLY ASKED QUESTIONS

Why is it common for hospitals to use Wi-Fi for bedside and transport monitoring, but not for telemetry?

It has been easier for medical equipment manufacturers to design Wi-Fi into a bedside and transport monitor due to the looser constraints around Wi-Fi power consumption and associated battery life. Portable monitors tend to be powered by battery and AC line power and tend to be used for shorter periods of time. Until most recently, Wi-Fi radios tended to be relatively power hungry. Telemetry monitoring is wearable, requiring smaller batteries to conserve weight and space, and has a requirement for the devices to be worn for days.

When I look for Wi-Fi based patient monitoring, is the particular WLAN technology important – such as 802.11a, b, g, n, or ac?

	Year Approved	Year Marketed	Radio Band (GHz)	Max Speed (Mbps)	Comments
802.11	1997	1998	2.4	2	Limited speed, limited adoption
802.11b	1999	2000	2.4	11	First widely adopted WLAN standard
802.11g	2003	2003	2.4	54	Backward compatible to .11b
802.11a	1999	2004	5	54	First widely adopted 5GHz WLAN standard
802.11n	2009	2009	2.4 & 5	300	Backward compatible to .11b/g/a, very widely adopted
802.11ac	2014	2014	5	~800	Next-generation Wi-Fi

TABLE 2. History of IEEE 802.11

The evolution of Wi-Fi has been driven by the radio manufacturers and IEEE standards seeking increasingly higher performance networks with increased radio spectrum efficiency. Here is the history of IEEE 802.11.

What is important is to focus on the application and use model. Patient monitoring data throughput requirements are extremely low and do not need the high speed capabilities of 802.11n and 802.11ac chipsets. The choice of radio is really dictated by chipset availability (for example, one would be hard pressed to find an 802.11b radio in 2014), power consumption, and feature set required by the patient monitor. Wi-Fi clients built on earlier 802.11 standards will communicate with the same QoS (Quality of Service) and security but simply may not be able to take advantage of capabilities inherent in 802.11n and 802.11ac. These include but are not limited to Channel Binding at 40/80MHz, MIMO Spatial Streams and Multi-Use MIMO, High Modulation 64 QAM and 256 QAM, beam-forming and co-existence mechanisms for 20/40/80/160MHz. When the healthcare enterprise desires to move forward with 802.11n and then 802.11c, adding the low bandwidth requirements of patient monitoring will have little to no impact on the overall wireless infrastructure.

How do I know that Wi-Fi will be reliable for a life-critical medical application when the spectrum is already crowded with data, voice, etc.?

The evolution of Wi-Fi has been to primarily increase networking speed, quality of service, and security. Wi-Fi has evolved to a level of performance capability whereby it is now displacing the wired Ethernet network at the access layer. Those applications with low bandwidth requirements, such as infusion pumps and patient monitoring, will reliably function in the 802.11g (2.4GHz) and/or 802.11a (5GHz) spectrums. Since 802.11n is backward-compatible with both 'g' and 'a', those same monitors will work well in a 802.11n WLAN infrastructure. Applications such as high-end video will tend to migrate to 802.11ac operating in the 5GHz band. Therefore, all applications can co-exist successfully on a modern WLAN network.

Modern WLAN systems increase overall system reliability using:

- Persistent spectrum analysis to identify RF interferers and proactively reconfigure RF channelization to work around the interference
- Applying best practices for networking design and deployment for Quality of Service (QoS) to prioritize patient monitor system traffic over other traffic types
- Applying best practices for networking design and deployment for network segmentation via VLANs that address scalability, security, and network management

I'm adding Wi-Fi patient monitoring to my hospital network. How can I design wired and wireless redundancy into the network?

The practices for designing redundancy into a network do not change by adding patient monitoring. Standard networking practices which can be planned in conjunction with hospital networking staff and/or third-party providers will meet your needs. Most WLAN vendors have capabilities for High Availability (HA) for their WLAN controllers (WLC) and offer near zero failover time to a secondary or tertiary WLC. In addition, modern WLANs can automatically modify the WAPs output power to increase the surrounding WAPs cell coverage in the event of WAP malfunction.

Although the network access-layer is typically not configured for redundancy, the access layer switches generally will, in healthcare facilities, have redundant Ethernet connections to the core network.

Are there differences in the way redundancy works with Wi-Fi wireless monitoring compared to monitoring suppliers that utilize WMTS?

The principal difference is that redundancy can be cost-effectively built into an 802.11 wireless network. Due to the proprietary nature of WMTS telemetry antenna systems, it is either technically impossible or too costly to design redundancy into the system.

WMTS, or realistically all "telemetry" antenna and receiver designs, use antenna diversity: if there were a null (lack of signal) from one antenna, the other adjacent antenna may likely receive the signal. However, this is highly dependent upon the quality of design which is more of an art, versus a proven, scientific WLAN enterprise design.

Several things need to be taken into consideration for a WMTS implementation. Upon installation of a WMTS antenna system, it must be balanced. These coaxial antenna designs consist of splitters, power supplies (to supply power to the specific legs of the antenna system), attenuators, exact cable lengths, and connections. In large designs this could amount to thousands of connections and hundreds of antennas, which have be at the exact right place and with the right connections made with the ultimate two home runs to the receiver sections.

Multiple points of failure potentially exist to either cause dropout of the signal or the introduction of noise into the system as whole. This could result from a bad connection, removing an antenna, adding an antenna, relocating an antenna, or a receiver section failing. This coaxial WMTS antenna design is what is considered to be "non-intelligent". It is simply an active powered coaxial TV based diversity antenna infrastructure that is connected to powered telemetry receivers.

Unlike with WLAN, no software exists in a WMTS design to actively monitor the air space for interferers or adjust power for changes in WLAN signal coverage. Nor are there provisions for redundant failover of receivers (in case a receiver fails). In addition, the network management for a patient monitoring system operating on a WLAN will be absorbed into the overall network management costs as the patient monitoring system is operating on a common network infrastructure versus a proprietary WMTS-based system.

CONCLUSIONS

1. Wi-Fi is safe and reliable for patient monitoring.
2. The key to success is in the design, implementation and management of the network.
3. Wi-Fi opens the door to unprecedented benefits to the hospital, such as the ability to monitor a virtually unlimited number of patients house-wide, improved patient mobility, significant cost savings and more.
4. Wireless monitoring gives hospitals the ability to provide continuity of patient care across the enterprise for the entire patient stay, which is only financially feasible with Wi-Fi.

ABOUT THE AUTHORS

DAVID HOGLUND, President and CEO of Integra Systems, Inc., has more than 30 years of experience in patient monitoring networking and has authored over 20 white papers and publications. (www.integrasystems.org)

VINCE VARGA, Business Development Manager for Mobility at Global Technology Resources, Inc. has over 13 years of experience in wireless networking technology, worked with clients across multiple vertical markets, and has managed more than 40 wireless LAN patient monitor deployments at healthcare facilities across the US since 2004. (www.gtri.com)