



# Wi-Fi<sup>®</sup> in Healthcare:

## The solution for growing hospital communication needs



Wi-Fi Alliance<sup>®</sup>  
February 2011

The following document and the information contained herein regarding Wi-Fi Alliance programs and expected dates of launch, is subject to revision or removal at any time without notice. THIS DOCUMENT IS PROVIDED ON AN "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. THE WI-FI ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

## Executive Summary

Wi-Fi is widely used today in hospital settings as the communications backbone for traditional PC networking. It offers clinicians and IT departments reliable, security-protected transmission of data and messaging. Wi-Fi systems are flexible to grow and adjust to the changing needs found in hospital settings – from PC networking growth to the proliferation of Wi-Fi devices on the network, ranging from smartphones and tablets to patient monitoring devices. The use of Wi-Fi CERTIFIED™ products ensures that devices will interoperate and meet government-grade security requirements.

The number of Wi-Fi CERTIFIED devices in hospitals is growing significantly as the advantages of networking between devices, applications, clinicians and systems are realized. Wi-Fi communication may be present on a hospital floor in everything from infusion pumps and sensors to PCs, patient monitors, smartphones and wearable wireless devices (WWDs). As hospitals make greater use of electronic medical records (EMRs), more and more devices that interact with these records will find their way onto hospital Wi-Fi networks. For a majority of hospital systems, medical devices are just beginning to transition from proprietary private networks to Wi-Fi networks. As this transition continues and the balance of Wi-Fi devices begins to shift toward an increasing number of devices, system designers and administrators will face new challenges such as network capacity and scalability, device coexistence, mobility and power consumption.

### Wi-Fi Benefits for Medical IT Networks

- Fundamental to mobility
- Provides proven, reliable performance
- Helps secure transmissions for mission-critical applications
- Interoperability validated through rigorous testing
- Currently available in millions of devices ranging from smartphones and laptops to special-purpose medical devices

Careful planning, implementation and monitoring of the enterprise Wi-Fi network helps ensure that hospital network administrators address these challenges effectively. Properly designed and maintained Wi-Fi networks offer hospital environments a proven, interoperable and security-protected system for handling a broad range of devices and data transfers.

This white paper is intended to identify technology areas that should be given special consideration in developing and maintaining Wi-Fi networks in hospital settings in order to maximize their performance and benefits. Hospital IT groups should consult service providers and equipment manufacturers for further planning details, as this paper serves as a guidance document only. The actual design and implementation of Wi-Fi networks is based upon the unique requirements of the devices and applications used in each hospital environment.

## Introduction

Today, most hospital wireless local area networks (WLANs), or Wi-Fi networks, provide network connectivity primarily for computing devices. For patients and visitors, Wi-Fi networks provide convenient Internet access from laptops and smartphones. For clinicians and administrators, Wi-Fi networks provide access to hospital networks and record-keeping databases from workstations on wheels (WoWs), tablet computers, handheld mobile computers, smartphones, and other computing devices. More than 500,000 Wi-Fi infrastructure endpoints, or access points (APs), were deployed in U.S. healthcare facilities in 2010, representing a 50 percent increase from 2009. Worldwide sales of Wi-Fi technology into the healthcare market are expected to reach \$4.9 billion in 2014.<sup>1</sup>

Hospital IT administrators are facing an ever-increasing need to attach medical devices and applications to the Wi-Fi network in order to support EMRs and clinical information systems (CIS), deliver better patient care, improve clinical workflow, and even help speed patient recovery time by providing mobility via wearable wireless devices (WWDs). According to ABI Research, onsite WWD growth in healthcare facilities is expected to skyrocket from 1.67 million estimated devices today to over 294 million in just five years.

Along with this device growth, the adoption of EMRs is rapidly increasing and more hospital systems are integrating clinical and information systems where data flows across the hospital network. Today 30 percent of U.S. hospitals have data electronically extracted for an electronic health record (EHR)/EMR and interfaced into an electronic file.<sup>2</sup>

Wi-Fi networks offer reliable, security-protected, proven technology. In order to maximize the benefits of a hospital Wi-Fi network, several characteristics unique to hospital environments must be reviewed and taken into consideration. Among these are security requirements for patient records, the mobility needs of devices, “always on” network uptime requirements to accommodate patient monitors and applications, real-time access to records and data transfers, and continuously increasing bandwidth demands. Best practices for these areas are provided in this paper.

### Table of Contents

Introduction	Page 3
RF Spectrum	Page 4
Distributed Antenna	Page 6
Mobility	Page 6
Security	Page 7
Infrastructure	Page 7
Network Design	Page 9
Network Monitoring	Page 9
Multi-service Support	Page 10
Power Savings	Page 10
Summary	Page 11

---

<sup>1</sup> ABI Research, 2010.

<sup>2</sup> *Health & Hospital Networks' Most Wired Hospitals* 2010.

## RF Spectrum: Planning, Design and Management

Basic radio frequency (RF) planning guidelines that apply to enterprise and public Wi-Fi systems also apply to the hospital environment. Effective spectrum planning, deployment and management provide for a scalable infrastructure and present strong mitigations against the challenges associated with RF propagation and interference sources.

Hospitals, more than most buildings, incorporate RF obstacles in their construction and contents. For instance, concrete walls with steel rebar make up many of the interior walls and affect RF signal levels more than wood or drywall material. Windows sometimes have coatings that attenuate or block RF signals in the Wi-Fi frequency bands. False ceilings range from foam material, with little RF absorption, to metal-clad tiles which are highly reflective. Radiology or operating rooms sometimes incorporate metal- or lead-lined walls, reflecting or absorbing wireless signals. These physical attributes all affect Wi-Fi signal propagation, and must be taken into account when designing and operating the Wi-Fi network.

A site survey is the starting point for RF deployment. An experienced Wi-Fi engineer should examine the plans for the building, conduct a physical inspection, and perform an RF survey to inventory the existing Wi-Fi and other wireless networks that may already be deployed.

### Risk Management for IT Networks in Hospitals

The recently-approved international standard for the “APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES”, or IEC 80001-1, advises that the application of a risk management process in the design, deployment and management of an IT-Network is essential to the creation of a safe, secure and effective network for use in healthcare delivery organizations. Additionally, the draft accompanying Technical Report titled “Part 80001-2-x: GUIDANCE FOR WIRELESS NETWORKS” applies the concept of risk management to the design, deployment and management of wireless networks in healthcare.

The Wi-Fi Alliance supports and encourages IT organizations to adopt a risk management process as part of their wireless networking strategy.

After defining the requirements for the services and devices to be supported as part of the hospital’s wireless networking strategy, the Wi-Fi engineer will use an RF planning tool to identify the number and placement of access points for the network. This tool could be a standalone tool or one included in the Wi-Fi infrastructure’s functionality.

The recommended design and deployment guidelines for a hospital Wi-Fi network uses dual-band Wi-Fi CERTIFIED n access points to offer simultaneous service at both 2.4 GHz and 5 GHz. This design offers the highest data capacity and immunity to interference while accommodating all generations of Wi-Fi client devices. The Wi-Fi Band Comparison chart below provides a basic comparison of 2.4 GHz vs. 5 GHz specifications. Where a dual-band deployment is not feasible, the IT engineer should diligently identify and remove sources of 2.4 GHz interference, such as the

type that may be created by headsets, cordless phones, microwave ovens or other devices. An additional consideration regarding the use of 2.4 GHz is the client migration from supporting 802.11b-only clients to 802.11g or 802.11n. If 802.11b devices are unavoidable, the engineer should disable lower data rates (i.e. turn off 1 and 2 Mbps rates) in the 802.11b network.

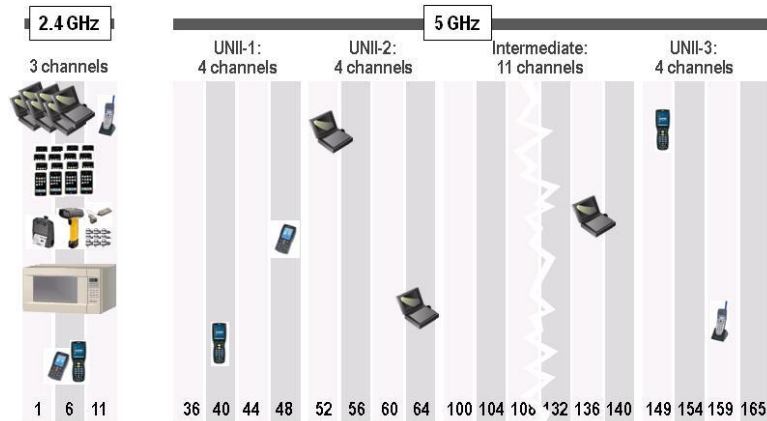
2.4 GHz	5 GHz
83 MHz spectrum	550 MHz spectrum (~7X more capacity)
3 non-overlapping channels	Up to 23 non-overlapping channels
More sources of interference (Bluetooth headsets, cordless phones, microwave ovens, other devices)	Fewer incumbent devices creating interference
Support for 802.11b, 802.11g and 802.11g/n devices	Support for 802.11a and 802.11a/n devices

**Exhibit 1: Wi-Fi Band Comparison**

Other RF considerations that IT managers should review include:

- **RF propagation differences:** 5 GHz has more path loss (i.e. reduction in signal level over distance) than 2.4 GHz. A separate site survey should be used when assessing RF coverage in 5 GHz spectrum. Both bands should be explored independently.
- **Channel planning and DFS:** By supporting IEEE 802.11h, Wi-Fi devices support dynamic frequency selection (DFS), a technique for avoiding radar on certain 5 GHz channels called DFS channels. See the Mobility section for more information on DFS channels.
- **Dual-band 802.11n:** Infrastructure support for dual-band 802.11n (802.11a/g/n) is recommended over support for 802.11a/g because 802.11n improves connection reliability and range for all Wi-Fi clients, even those that support only 802.11a/g.

A hospital is a dynamic environment, changing on a day-to-day and even a minute-by-minute basis. Today's Wi-Fi networks are capable of automatically sensing their RF environment and re-configuring the RF plan for optimal coverage and capacity, dynamically taking account of interference and obstructions. Leveraging both site survey tools and the autonomous RF management capability provided by the Wi-Fi infrastructure, the network or RF engineer can establish and maintain a consistent and accommodating RF setting within the challenging hospital environment.



Today's access points are capable of advanced spectrum intelligence. It is highly recommended to choose APs that can identify the fingerprint of non-802.11 interferers to effectively combat service interruption from interference sources.

## Distributed Antenna Systems

A hospital often has a distributed antenna system (DAS) to provide better indoor coverage for cellular services. Use of a DAS for 802.11n infrastructure complicates the use of spatial multiplexing, a key technology which delivers higher throughput via the use of multiple antennas. When Wi-Fi data is sent between two 802.11n devices that support multiple antennas, the sender splits the data into two or more data streams and sends the streams at the same time using multiple antennas separated spatially. When the streams arrive at the recipient, they are aggregated into a single data stream.

A typical in-building DAS is equipped with a single physical antenna that is branched and distributed. To support spatial multiplexing with a DAS, a hospital must run parallel RF cabling (two or more) or replace the existing single-antenna DAS with a newer DAS system that supports multiple RF streams through an RF-over-packet infrastructure. It is recommended to continue DAS usage to provide cellular services via in-building coverage and to use a separate 802.11n infrastructure to allow high-throughput clients to take full advantage of spatial multiplexing.

## Mobility: Roaming Performance

A Wi-Fi client can be connected to only one AP at a time. When the client moves to a position where its connection to that AP becomes suboptimal, the client will try to switch to an AP that provides better connectivity. The process of switching from one AP to another is called roaming or handover. The decision process and management of the handover is determined by the client device's Wi-Fi radio software, sometimes in collaboration with the infrastructure.

Before a client device connects to a new AP, it must disconnect from the current AP, potentially resulting in packet loss. When evaluating a device or application for use on the Wi-Fi network, IT must understand the mobility performance requirements of the device and whether tolerance to packet loss in a mobile environment is acceptable. If packet loss would negatively impact the clinical functionality of a device or application, then further exploration of the device's roaming performance is warranted.

The larger number of channels available in the 5 GHz band provides for increased network capacity, but it also can lead to longer roam times for mobile devices because effective roaming requires either passive or active scanning of every available channel. When available channels include those that require DFS, scan times are even longer because DFS channels require passive scanning, which is slower than active scanning. Network administrators may choose to reserve DFS channels for non-mobile devices or evaluate Wi-Fi clients for fast roaming capabilities.

After it associates to the new AP, the client must re-authenticate to the network. When WPA2<sup>TM</sup>-Enterprise is used, the 802.1X re-authentication process may require interactions between the AP and an authentication server on the network. Many enterprise Wi-Fi infrastructures support one or more protocols for fast 802.1X re-authentication that eliminates the need for interaction with a server.

IP subnet transitions are especially disruptive to inter-AP point handovers, as obtaining a new IP address from a DHCP server can take several seconds. It is important to ensure that devices can keep the same IP address throughout the network. Where possible, device mobility regions should be aligned within the IP addressing scheme so that a latency sensitive client does not roam from an AP in one subnet to an AP in a different subnet.

Early Wi-Fi deployment models recommended that the broadcasting of SSIDs be disabled for security purposes. Today's Wi-Fi technology has strong security measures that mitigate eavesdroppers and it is no longer advisable that broadcasting of SSIDs be disabled. For shorter scan times it is better to enable the broadcasting of SSIDs so that passive scanning clients can listen for off-channel APs in a shorter period of time. This also leads to improved battery life due to the reduced amount of scanning in clients.

## Security: HIPAA and Wi-Fi

The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, establishing a national set of security standards for organizations that handle protected health information (PHI) that is held or transferred in electronic form. For Wi-Fi client devices and networks, the key part of the Security Rule is section 164.312, which lists technical safeguards in the areas of access control, audit controls, integrity, authentication, and transmission security.

Wi-Fi Protected Access®, or WPA2™, found in all Wi-Fi CERTIFIED devices since 2006, provides strong security measures for meeting HIPAA requirements. While all modern Wi-Fi devices can support full WPA2 security, there may be special cases in the hospital environment where it is necessary to service legacy devices supporting earlier security standards. This can be accomplished on modern Wi-Fi infrastructure, with different vendors offering solutions that segregate the devices and their traffic by using a separate SSID, or by applying more stringent firewall and security policies, to ensure the hospital network and other devices are not put at risk. IT managers should never down-configure the overall network in order to accommodate legacy devices; rather, those devices needing less current security mechanisms should be segregated to the extent feasible.

For more detailed information on Wi-Fi security and WPA2, please see the white paper titled [“The State of Wi-Fi Security”](#).

## Infrastructure: Configuration and Management

All Wi-Fi CERTIFIED devices are tested for interoperability with other Wi-Fi CERTIFIED devices. Additionally, a key consideration associated with the configuration of a Wi-Fi network is the unique functionality that vendors build on top of the 802.11 standard. Some areas that should be explored when configuring hospital Wi-Fi networks include:

- **Initial Configuration:** Rather than relying on default infrastructure configuration settings, an administrator should customize settings to the unique characteristics of the needs of the devices, both medical and non-medical.
- **Auto-configuration:** Automated configuration mechanisms can help meet the networking connectivity requirements of Wi-Fi devices. Some features of the controller software empower the Wi-Fi infrastructure to dynamically change the WLAN RF characteristics. One example of this is to automatically set and adjust the AP operating channel and/or transmit power. These self-organizing and self-optimizing system behaviors can save significant time in network deployment and subsequent maintenance if properly utilized.
- **SSID Management:** Each SSID in a Wi-Fi network requires its own beacon. Each new SSID adds management airtime for beaconing; the more SSIDs enabled, the more management traffic in the air instead of data traffic. It is recommended that IT assign SSIDs based on common device capabilities such as security and Quality of Service

(QoS) vs. that of assigning a SSID for each vendor device type. This should assist in reducing the number of SSIDs deployed.

- **Network Scalability:** The introduction of video streaming devices and smartphones have placed a rapidly increasing burden on the ability to both provision enough infrastructure capacity for all devices as well as manage the use of these devices. Hospital environments are particularly besieged by smartphones as visitors, administrators and clinicians are using these devices for medical and non-medical applications. Additionally, both real-time video services and other bandwidth-intensive applications will significantly increase the demand on the network. These types of services benefit from the use of the 5 GHz band to increase the available capacity as well as the use of Wi-Fi CERTIFIED for WMM® (Wi-Fi Multimedia™) which provides QoS. These mitigations provide higher capacity and network efficiency such that these types of devices do not claim all available network capacity, leaving other devices such as medical devices starved of bandwidth.
- **Networking Software Upgrades:** Wi-Fi infrastructure has an excellent record of feature introduction via software upgrades. This helps to maintain compatibility with older devices and extends the interval between hardware refresh cycles. The network engineer should develop a process for planning and implementing software upgrades taking the following into consideration:
  1. Determine and document a process by which an IT department verifies a new controller software release as part of a risk management process. Verify operation of new software and compatibility with existing and new client devices. Reading release notes, discussing the release with the Wi-Fi vendor technical assistance center and testing on pre-go-live infrastructure are some of the steps that may be involved in establishing risk control measures.
  2. Discuss with the medical device vendor(s) their process for defining compatibility with Wi-Fi infrastructure releases; determine if they have tested to a particular release level as part of their risk management process.
  3. Inform all clinical and biomedical engineering staff of the software upgrade event prior to commencing the software upgrade. This will allow for networking users such as clinicians to mitigate a known loss of connectivity (e.g. by having extra staff on site).

Advanced technologies outside the scope of the 802.11 standard such as intrusion detection and protection, adaptive antenna beam-forming, etc. should be considered and reviewed with the WLAN infrastructure vendors.

## Network Design: High Reliability

As hospital services become more dependent on wired and wireless networks, it becomes increasingly critical that the network is reliable. Wi-Fi CERTIFIED devices have passed rigorous interoperability testing and should be specified in system design requirements. Reliability considerations particularly applicable to hospital Wi-Fi networks are reviewed below.

**Interoperability:** It is important to verify interoperability between the proposed WLAN equipment and the clients as well as between the clients themselves. Specifying Wi-Fi CERTIFIED for all equipment is an important first step in this verification process as Wi-Fi CERTIFIED devices provide an assurance of both interoperability and performance. In addition, infrastructure vendors, medical device manufacturers and implementers have gained experience drawn from a multitude of hospital deployments and can provide guidance as a result. As part of the planning phase, all applicable devices and services must be identified and their correct configuration settings must be determined.

**Redundancy:** The hospital Wi-Fi network must be designed from the start with an appropriate level of redundancy. At the access point level, this usually entails sufficiently close physical spacing. In the event of a single access point failure, neighboring APs can increase their transmit power to maintain seamless coverage over the area. Modern Wi-Fi networks incorporate control software that detects and automatically heals such coverage holes. The other critical reliability consideration for most WLAN architectures is the centralized controller; these should be configured for 1:n or 1:1 redundancy with automatic failover as is typically done for infrastructure routing equipment.

## **Network Monitoring and Management**

Continuous monitoring of the network will ensure that a hospital IT system continues to meet the needs of connected devices and hence the clinical and business needs of the healthcare organization. To ensure the network engineer is alerted to problems before the help desk receives users' calls, it is important that critical network related alarms are escalated in real-time, through email or other means. This, combined with a comprehensive event-logging strategy, allows timely response to outages and trends.

Network performance thresholds for various alerts should be evaluated based on the performance of the network and set to trigger alerts as network conditions degrade. An example of such an alert might be the airtime capacity of the access points: Wi-Fi network management systems should generate alerts when capacity thresholds are exceeded; a guideline for threshold settings is to trigger alerts well before client devices start experiencing performance concerns. Network performance trending should also be reviewed on a regular basis.

A systematic analysis of the Wi-Fi network performance over a period of time can enable an administrator to adjust performance variables and make system enhancements in planned increments, rather than responding to emergency situations after a system has been stressed beyond its physical capabilities. This involves establishing and adjusting a baseline by analyzing performance data over a period of time and plotting trends. Tracking key networking performance parameters such as AP capacity utilization and latency can provide a means to enable predictive alerts. This, in turn, can define specific threshold trigger levels settings that will alert IT about problematic performance parameters before they have a negative impact on the network.

## **Multi-service Support: QoS and Differentiated Services**

In recent years, healthcare Wi-Fi networks have evolved to encompass services such as voice, video and patient monitoring – all requiring service level agreements specifying delay, jitter and packet loss. The Wi-Fi Alliance stepped forward to support these differentiated services with the introduction of Wi-Fi CERTIFIED for WMM (Wi-Fi Multimedia). Wi-Fi network infrastructures that are certified for WMM are capable of simultaneous support of multiple high-priority services, along with lower priority data-oriented usage. WMM enabled at the infrastructure and client levels, allows a single Wi-Fi network to support multiple services, allocating resources to ensure each packet has the appropriate priority.

WMM defines four priority queues which are used to prioritize traffic over the wireless link, as shown in the table below.

WMM Priority	Hospital Applications
1. AC_VO (voice)	Patient safety, mission-critical voice
2. AC_VI (video)	Video, real-time services (e.g. non mission critical voice)
3. AC_BE (best effort)	General data access, non-real-time services
4. AC_BK (background)	Background traffic

Traffic assigned to “AC\_VO” will get highest priority; traffic assigned to “AC\_VI” second priority; and so on. Understanding both business needs and clinical functionality of devices will determine the appropriate WMM queue in which to group devices. For example, guest access may be in the best effort category while patient monitoring would operate in the voice category. Mission-critical voice may also be in the first category; other voice services can be placed in the lower categories.

With the introduction of Wi-Fi CERTIFIED smartphones and video streaming devices into the hospital, the proper use of WMM is critical. The use of WMM to segregate traffic on the network will help to ensure there is adequate airtime available to high priority traffic so that when critical devices need to access the wireless network, the radio channel will be available. Best practices for implementing WMM include:

- Understand both the business needs and clinical functionality of devices to determine the appropriate WMM queue to assign device groups
- Configure WMM to provide end-to-end QoS on the entire network

For more information on WMM, refer to the Wi-Fi Alliance [white paper](#) on the subject.

## Power Savings: Maximizing Battery Life for Mobile Devices

Some Wi-Fi clients such as printers and WoWs operate on AC power from wall sockets so power consumption of the Wi-Fi radio is not a significant constraint. However, many hospitals now provide Wi-Fi phones for clinicians and employees, utilize untethered physiological monitoring devices, and use Wi-Fi tags for asset location. Battery life is a key consideration for these devices, and the Wi-Fi Alliance has developed the WMM-PS (Wi-Fi Multimedia – Power Save) certification to meet these needs. WMM-PS helps to ensure that the infrastructure access point and client devices coordinate periods where client devices can switch off their radios and sleep, minimizing their power requirements. For more detailed information on WMM-PS, refer to the [whitepaper](#) on the topic.

There is ongoing work in the industry to define a common set of requirements for additional power saving capabilities.

## Summary

As greater demands are placed on the Wi-Fi networks found in hospitals to accommodate an ever-growing variety of devices, as well as becoming the primary vehicle for the implementation of automated EHR/EMR data transactions, hospital IT departments must address healthcare-specific challenges in order to maximize the performance of their networks. Several best

practices in system design, deployment and management have been presented, and are summarized here.

The radio frequency environment of a hospital is both challenging and dynamic. It is essential that the planning process and deployed infrastructure can identify and accommodate RF obstructions and sources of interference, to provide continuous coverage throughout the hospital. This will provide a reliable Wi-Fi signal for all client devices, especially those running mission-critical applications.

Mobile devices require secure connectivity service as they move through the building. A combination of contiguous RF coverage, government-grade security as provided for in WPA2, and design for inter-access point handover ensures seamless and secure connectivity.

Client-specific concerns such as minimizing power consumption and customizing WMM should be addressed to meet the service level agreement of clients.

Network reliability is provided by a combination of appropriate redundancy, bandwidth overprovisioning, configuration control and RF self-healing features.

Network management should include continuous monitoring and logging, including both the infrastructure elements and also management of client devices.

Hospital IT departments should apply best practices within a risk management framework such as IEC 80001-1 and its accompanying wireless guidance technical report. In all cases of applied best practices, be sure to consult with your medical device and Wi-Fi CERTIFIED infrastructure suppliers for specific guidance relative to the interoperability needs of your network and devices.

For comments on this whitepaper, or to submit ideas for future topics you would like to see explored, email [whitepapers@wi-fi.org](mailto:whitepapers@wi-fi.org).

## List of Acronyms

AP	Access Point
CIS	Clinical Information Systems
DAS	Distributed Antenna System
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
EHR	Electronic Health Record
EMR	Electronic Medical Record
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IP	Internet Protocol
PHI	Protected Health Information

QoS	Quality of Service
RF	Radio Frequency
SSID	Service Set Identifier
WLAN	Wireless Local Area Network
WMM®	Wi-Fi Multimedia™
WMM®-PS	Wi-Fi Multimedia – Power Save
WoW	Workstation on Wheels
WPA2™	Wi-Fi Protected Access® 2
WWD	Wearable Wireless Device

### **About the Wi-Fi Alliance®**

The Wi-Fi Alliance is a global non-profit industry association of hundreds of leading companies devoted to the proliferation of Wi-Fi technology across devices and market segments. With technology development, market building and regulatory programs, the Wi-Fi Alliance has enabled widespread adoption of Wi-Fi worldwide.

The Wi-Fi CERTIFIED™ program was launched in March 2000. It provides a widely-recognized designation of interoperability and quality, and it helps to ensure that Wi-Fi enabled products deliver the best user experience. The Wi-Fi Alliance has completed more than 9,000 product certifications to date, encouraging the expanded use of Wi-Fi products and services in new and established markets.

Wi-Fi®, Wi-Fi Alliance®, WMM®, Wi-Fi Protected Access®, the Wi-Fi CERTIFIED logo, the Wi-Fi logo, the Wi-Fi ZONE logo, and the Wi-Fi Protected Setup logo are registered trademarks of the Wi-Fi Alliance; Wi-Fi CERTIFIED™, Wi-Fi Protected Setup™, Wi-Fi Direct™, Wi-Fi Multimedia™, and the Wi-Fi Alliance logo are trademarks of the Wi-Fi Alliance.