# Wi-Fi® in Healthcare:

## Security Solutions for Hospital Wi-Fi Networks

Wi-Fi Alliance®

February 2012

## Executive Summary

Connecting medical devices to a hospital Wi-Fi network improves clinical workflows, ensures access to real-time patient data, and provides a secure and robust solution for Clinical Information Systems (CIS). Hospital staff and patients must have confidence that a hospital's Wi-Fi network is able to protect sensitive patient information, provide reliable data connectivity, and effectively support all connected devices, both medical and non-medical.

This white paper provides the hospital IT professional more specific recommendations for using WPA2™-Enterprise security and 802.1x authentication protocols to protect a Wi-Fi network from unauthorized access, such as compromised passwords, data exposure, "man-in-the-middle" threats. Also included are recommendations for establishing and managing a secure Wi-Fi network and considerations around the mobility needs of network devices in the hospital environment and bring-your-own-device (BYOD) policy management. All of these recommendations can be considered best practices and may be included as risk control measures when implementing a risk management plan per the international standard IEC 80001-1:2010 (see sidebar on Risk Management).

Another white paper, published in February 2011, pertaining to Wi-Fi in healthcare (link) also outlines general technology areas that should be given special consideration when deploying Wi-Fi in a hospital.

## The Need for Security

Hospital IT staff must protect sensitive data (see sidebar on HIPAA), such as patient medical records, that travel between medical devices and Wi-Fi networks. Data security mirrors the more well-known physical security needs of hospitals. Like physical security, data security is concerned with safeguarding facilities, properly restricting access to resources, and protecting vital information. Unlike physical security, deficits in data security are not always easy to spot.

**Fig 1. A wide range of devices connect to hospital Wi-Fi networks**

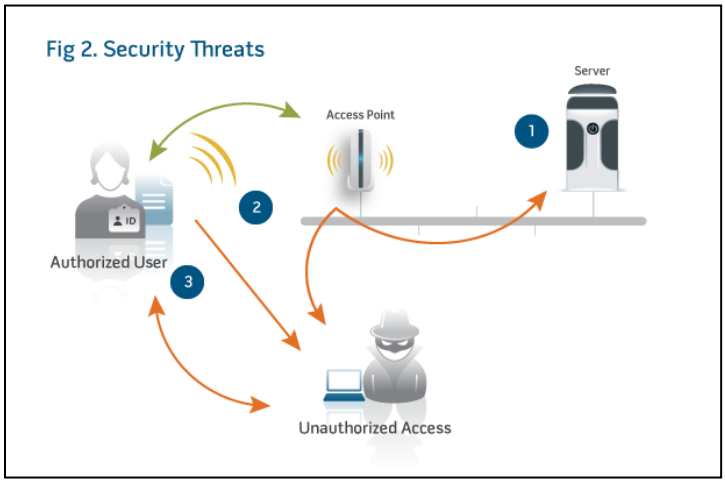
Hospital networks must support a broad range of devices. Fig 1 shows some of the devices that will become connected using Wi-Fi technology. These devices have unique relationships to the hospital information system and different networking performance

requirements. Hospital-managed devices, as well as those devices brought in by hospital staff and guests, contribute to the diversity and complexity of network management.

## Mitigate Potential Security Vulnerabilities

Wi-Fi client devices, such as those depicted in Fig 1, communicate with a hospital's wired network via Wi-Fi access points (APs). Wi-Fi radio waves don't travel just between a client device and an AP; they travel over the air and can reach waiting rooms and other public areas and even go through the walls of the facility to areas where unauthorized users may be able to "see" Wi-Fi traffic.

Without proper Wi-Fi security in place, an unauthorized user could use intercepted Wi-Fi packets to gain access to the hospital network and view sensitive information that is transmitted over the air. Fig 2 illustrates these types of possible security threats.




Path ① shows unauthorized network access. In this example an outsider poses as an authorized user and gains access to the hospital information network via the Wi-Fi network. Once on the network, the outsider may gain access to sensitive information and other critical resources.

Path ② shows data exposure. Some of the data packets that travel between a Wi-Fi client and a Wi-Fi network may contain sensitive information. If the packets are not encrypted, the unauthorized user may be able to view sensitive information, such as Electronic Protected Health Information (ePHI).

Path ③ is often called the "man-in-the-middle attack." The unauthorized user's laptop poses as a hospital AP and attempts to trick clients into connecting with it instead of a trusted AP. Once a Wi-Fi client connects to the unauthorized user's laptop, that user may be able to obtain sensitive information from the client, including credentials required to gain access to the trusted network. The unauthorized user also can induce the client to send potentially sensitive information onto this untrusted network.

Wi-Fi security threats are mitigated through good security practices. The foundation of strong security is the Enterprise version of Wi-Fi Protected Access® (WPA2™). WPA2 provides both access control (you can control who connects) and privacy (the transmissions cannot be read by others) for communications as they travel across your network. WPA2 creates fresh session keys on every association. The benefit is that the encryption keys used for each client on the network are unique and specific to that client ensuring that every packet sent over the air is encrypted with a unique key.

Hospital IT administrators should look to deploy Wi-Fi CERTIFIED™ equipment and devices, as all are required to implement WPA2 security protocols.

### WPA2-Enterprise

There are two versions of WPA2: Enterprise and Personal. Both use AES-CCMP for strong encryption of all transmitted data. The difference between the two is the type of information used for authentication. WPA2-Personal authentication is designed for home networks and other small networks that do not have an authentication service. WPA2-Enterprise authentication is designed for enterprise environments, for example a hospital which has a central authentication service such as AD (Active Directory), or LDAP (Lightweight Directory Access Protocol). The risk analysis conducted by hospital IT staff should dictate the level of security required for each device or application. The WPA2 version selected should balance the interaction between the three key properties of data security, clinical effectiveness, and patient safety in a Medical IT wireless network. Reliance on WPA2-Enterprise is a best practice for strong Wi-Fi security in the enterprise environment. While this paper stresses the use of WPA2-Enterprise for hospital Wi-Fi networks, it is recognized that some devices and applications may require the use of WPA2-Personal. See the sidebar “WPA2-Personal” for details on authentication with WPA2-Personal.

With WPA2-Enterprise, authentication utilizes 802.1X, a ratified IEEE standard for network access control. By design, 802.1X is flexible and supports a variety of Extensible Authentication Protocol (EAP) types, most of which support mutual Layer 2 authentication of the client device and the network to which the client is trying to connect.

EAP is a framework that allows a client device and an authentication server to authenticate each other through an authenticator – an AP, in the case of Wi-Fi. The authentication server sends authentication requests to the client through the AP. The client then sends responses to the server through the AP.

Most EAP types rely on public key infrastructure (PKI), which has been used for over 15 years for e-commerce and other secure Internet applications. PKI relies on digital certificates as well as encryption and decryption using public and private keys. Properly implemented, PKI provides strong security but requires the creation and deployment of digital certificates. With most EAP types, the only certificates that must be managed are CA certificates, which are digital certificates for a certificate authority on the network.

Five EAP types that are included in the WPA2-Enterprise certification test bed are widely-used in hospitals. Table 1 provides an overview of these EAP types:

| EAP Method | Credentials | Notes |
|---|---|---|
| EAP-Transport Layer Security (EAP-TLS) | client certificate | Server and client authenticated in the same EAP exchange. |
| EAP-Tunneled TLS with EAP-MSCHAPv2 inner method (EAP-TTLS/MSCHAPSv2) | username and password | MSCHAP: Microsoft Challenge Authentication Handshake Protocol with inner method |
| Protected EAP with EAP-MSCHAPv2 inner method (PEAP- MSCHAPSv2) | username and password | PEAP supports other inner methods. |
| Protected EAP with EAP-GTC inner method (PEAP-GTC) | username and password | GTC: Generic Token Card Supports non-static (one-time) passwords. |
| EAP Flexible Authentication through Secure Tunneling (EAP-FAST) | username and password | Option of protected access credential (PAC) instead of digital certificate |

*Table 1. EAP types that are widely-used in hospitals*

EAP-TLS differs from the other four types in the nature of the credentials used to authenticate the client. With the other EAP types, the credentials are a username and password configured on the client device or entered by the user of that device. With EAP-TLS, the credentials are in the form of a digital certificate that is unique to the client device. Configuring a unique digital certificate for every user and storing each user certificate on the user's client device can pose an administrative challenge in an environment where there are hundreds or thousands of client devices.

Types other than EAP-TLS use two EAP exchanges between the client and server. The first EAP exchange is referred to as the "outer method" and the second EAP exchange is referred to as the "inner method":

- The client uses the outer method EAP exchange to validate the network via the authentication server and establish an encrypted tunnel for the inner method. Note that PEAP and TTLS both use a server-side certificate for the outer tunnel. Proper authentication of the authentication server is paramount to guaranteeing that clients are talking to a trusted authenticator, an AP in this case.
- With the inner method EAP exchange, the client provides credentials so that the network (or authentication server) can validate the client. Different inner methods allow for different types of passwords and interaction with authentication servers that support those password types. For example, the inner method of EAP-MSCHAPv2 is for authentication servers that support a Microsoft password type, whereas EAP-GTC allows for one-time passwords.

At the conclusion of the EAP authentication process, the client and network derive a key that is used for AES-CCMP encryption (and decryption and integrity) of all data packets.

Hospitals already using authentication servers supporting Microsoft-formatted passwords often select PEAP-MSCHAPv2 for client authentication due to its use of a username and password. EAP-TTLS and PEAP were designed at the same time and offer many similar capabilities, but PEAP is more popular because laptops and other Windows-based computers have offered

native support for PEAP-MSCHAPv2 for nearly a decade. Use of PEAP-GTC is limited to those installations with databases that do not support Microsoft-formatted passwords. EAP-FAST offers an alternative to CA certificates called protected access credentials (PACs), which can be deployed manually or in an automated fashion.

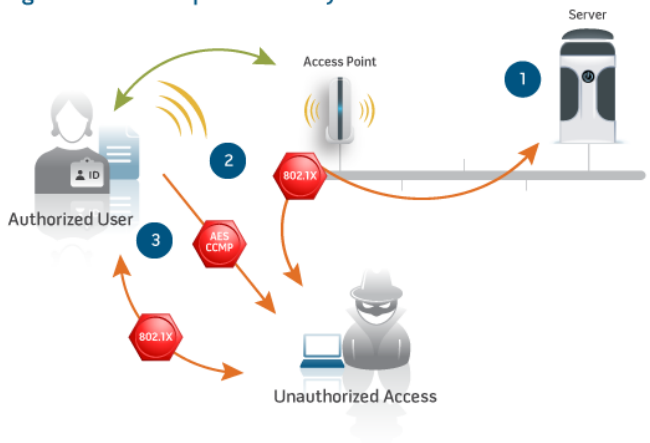
### Mitigating Risk with WPA2-Enterprise

With 802.1X and AES-CCMP, WPA2-Enterprise addresses the three security threats mentioned earlier, as illustrated in Fig 3.

1. Unauthorized network access: When every Wi-Fi client uses WPA2-Enterprise and its 802.1X authentication and user credentials are not compromised or stolen (e.g. passwords are not written on sticky notes), then IT managers can be confident that an unauthorized user cannot pose as an authorized user to gain access to the network.

2. Confidentiality or non-exposure: WPA2-Enterprise uses AES-CCMP encryption, a security protocol widely-used in military and sensitive government environments worldwide, to ensure that all over-the-air data is protected from being viewed by unauthorized users. Packets are encrypted in such a way that only the intended recipient can decrypt the packets and view the data in its unscrambled form.

Fig 3. WPA2-Enterprise Security




3. "Man-in-the-middle" attacks: To mitigate against this threat, hospital IT staff must configure every Wi-Fi client device to ensure that it connects only to trusted networks and authenticates a network before connecting to it. It is not enough to use an EAP type that supports mutual authentication; the client must validate the presented certificate of the AP or server.

In most cases WPA2-Enterprise should be used on every client device that supports it. Devices that do not support WPA2-Enterprise should be segregated onto a distinct Wi-Fi network (SSID) that is mapped to a distinct OSI Layer 2 (Data Link Layer) domain. Sharing or mixing devices of varying levels of security on the same SSID is not recommended. Similarly, client devices of hospital guests, as well as devices that are brought in and used by hospital staff but not managed by hospital IT, should be on a different SSID than hospital-managed devices.

The rapid adoption of smartphones used for both personal and business applications has created new challenges for IT management. In many hospitals, doctors and other practitioners want to run healthcare applications on personal devices such as smartphones and tablets. Hospitals that embrace the "bring-your-own-device" (BYOD) phenomenon must recognize that

the security policies and practices for unmanaged personal devices will differ from the security policies and practices for hospital-managed devices. It is important that hospital IT administration address the security of BYODs in their risk management policy. In hospitals where IT administrators do not manage personal devices, those administrators cannot configure the devices for security. Administrators should not rely on device owners to configure security properly on personal devices.

Risk management security policies should address the use of unmanaged personal devices that do not rely on Wi-Fi industry standards such as WPA2-Enterprise. One critical best practice in a hospital that allows personal devices to gain access to hospital networks is to ensure that hospital-managed devices are on a different Wi-Fi SSID than unmanaged personal devices, with each Wi-Fi SSID assigned its own network management policies such as bandwidth limiting, network access control, logical network segregation, etc. Additionally, there are other higher layer tools available such as swipe applications that remotely erase data, or device virtualization applications that prevent data from being stored locally on the device, that can assist with BYOD risk management. Such tools are outside the scope of this paper..

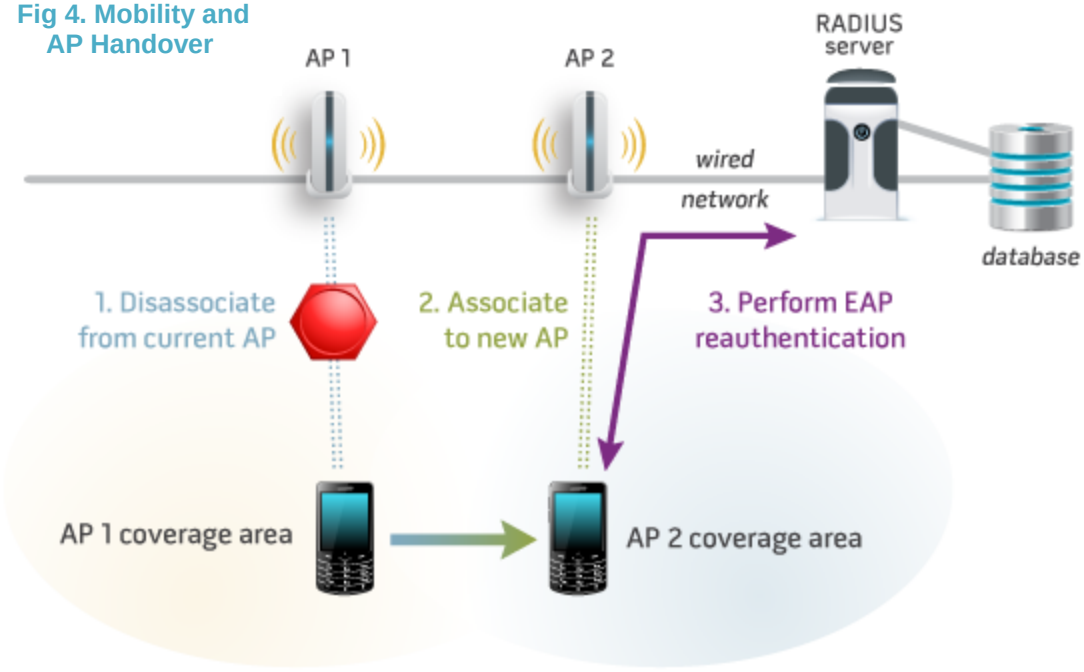
### Mobility with WPA2-Enterprise

WPA2 not only delivers strong security, it does so in today's highly-mobile environment. However, the ability for client devices to move to different locations in the hospital requires important deployment considerations.

The EAP authentication process with WPA2-Enterprise occurs when a client device attempts to connect to a Wi-Fi network for the first time. The process also occurs when a client moves from one AP to another AP on the same network. A client typically decides to roam from one AP to another when the client determines that its connection with the current AP is becoming suboptimal.

A client device cannot be associated to two APs at the same time. Once the client decides to roam to a new AP, it must first disassociate from its current AP and then associate to the target AP. It also must re-authenticate to the network on which the new AP resides, even if both APs belong to the same network. The process of disassociating from one AP and re-associating to another AP typically takes less than 100 milliseconds. The process of re-authenticating to the network, however, can take hundreds of milliseconds because standard EAP authentication requires several interactions between the client and an authentication server on the network and is completed while a device is performing scanning and handover algorithms. Re-authentication when roaming may be slowed to the point where it causes problems for applications and devices that require a persistent connection.

Fig 4. Mobility and AP Handover




There are two standardized methods for accelerating EAP re-authentication:

1. Pairwise Master Key (PMK) caching (introduced in IEEE 802.11i)
2. Fast BSS transition, which may not be widely supported until 2013 (based on standards within IEEE 802.11r)

The goal of PMK caching and fast BSS transition is to speed up roaming between APs by eliminating unnecessary communication with the authentication server.

As mentioned above, when a client joins a Wi-Fi network, the client and AP perform EAP authentication by exchanging information with the authentication server. When PMK caching is used, the client and AP cache the results of this exchange. While this process is repeated when the client roams to a new AP, when the client roams back to an AP with which it was previously associated, the cached results can be used instead.

When fast BSS transition is used, the concept of a "mobility domain" is introduced. The results from the initial exchange with the authentication server not only are cached by the client but are also shared with and cached by all the APs within the mobility domain. As a result, when the client roams to any AP within the mobility domain, the cached results can be used instead of repeating the exchange with the authentication server.

Hospital IT professionals should be aware of the implications of roaming and consult with their wireless local area network (WLAN) infrastructure vendor and each device manufacturer to understand the mobility needs of a device and the proper deployment and configuration of the WLAN infrastructure to support those mobility needs.

## Summary

Wi-Fi provides strong Layer 2 security through the use of WPA2-Enterprise and is a critical part of any a hospital's security risk management strategy. Hospital IT administrators should look to deploy Wi-Fi CERTIFIED™ equipment and devices for network use. Wi-Fi CERTIFIED provides independent, third-party validation to ensure the latest security protocols are implemented in new devices, along with interoperability testing to ensure Wi-Fi CERTIFIED equipment and devices will successfully communicate with each other.

The recommendations in this white paper emphasize the importance of the proper deployment and configuration of WPA2-Enterprise. Use of WPA2-Enterprise is the best method of protecting highly sensitive data in a hospital or health care facility. It is recommended that the Wi-Fi devices are managed by the hospital administration thus allowing for the use of 802.1X and associated client supplicants. The rapid acceleration of devices such as smart phones and tablets pose a unique challenge to IT administration. The security tools and framework used to manage devices not owned by the hospital (e.g. captive portal, virtualized applications, etc.) are outside the scope of this paper, but are important components of a successful security policy.

The risk management concepts detailed in the international standard IEC 80001-1:2010 (see sidebar on Risk Management) are a source for further information regarding the application of risk management to hospital networks, and the draft IEC 80001-2-3 Wireless Guidance technical report provides specific guidance for applying risk management concepts in the creation of healthcare wireless networks. These standards are useful in the safe and effective deployment of Wi-Fi for hospital networks. The Wi-Fi Alliance white papers are complementary to these risk-management standards, providing best practices and serving as a basis for designing, deployment and management of wireless networks.

## About the Wi-Fi Alliance

The Wi-Fi Alliance is a global non-profit industry association of hundreds of leading companies devoted to seamless connectivity. 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 12,500 product certifications to date, encouraging the expanded use of Wi-Fi products and services in new and established markets.

## Additional Resources

The State of Wi-Fi® Security: Wi-Fi CERTIFIED™ WPA2™ Delivers Advanced Security to Homes, Enterprises and Mobile Devices (2009). http://www.wi-fi.org/knowledge-center/white-papers

## Sidebar 1: WPA2-Personal

With WPA2-Personal, authentication is done through a four-way handshake using a pre-shared key (PSK) that may be derived from a passphrase. If the PSK on the Wi-Fi client matches the PSK on the AP to which the client is trying to associate, then the authentication succeeds.

The PSK or passphrase must be statically configured on every client device (analogous to assigning passwords at the device level) and within the Wi-Fi network. Configuring a few devices in a home or small office is feasible; configuring scores or hundreds of devices in a larger organization can be a challenge. For this reason, organizations that have large Wi-Fi installations generally prefer to use WPA2-Enterprise for wireless security.

A PSK must be long enough and complex enough that an unauthorized user cannot “guess” it using a dictionary attack. In such an attack, the attacker captures packets that were created using the PSK and then, using a dictionary of potential PSKs and the published algorithm for WPA2, tries to recreate the capture packets. If successful, the attacker has determined the PSK and can use it to join the Wi-Fi network. To avoid being vulnerable to a dictionary attack, a PSK or passphrase must be a random string of at least 20 characters, including characters other than letters and digits.

A key challenge to using WPA2-Personal within large healthcare organizations is the administrative overhead required if a PSK is lost or compromised. When such an event occurs due to staff attrition, theft or device compromise, each and every device must be physically reconfigured with a new PSK. Doing so in an expeditious manner while at the same time not impacting patient care typically is the key influencing factor on why healthcare organizations choose WPA2-Enterprise over that of WPA2-Personal.

Although the WPA2-Personal key is unique to each device, it can be computed by another device that is associated with the AP and that follows the association and hand-shake messages. This means that if an intruder can get initial access to the network, it can “crack” all user logins. From strictly a security perspective, the use of WPA2-Personal is less desirable in a hospital setting.

## Sidebar 2: HIPAA and WPA2-Enterprise

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the U.S. Health and Human Services (HHS) Secretary to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published two documents:

1. The HIPAA Privacy Rule, which establishes national standards for health information protection
2. The HIPAA Security Rule, which establishes a national set of security standards for organizations that handle protected health information that is held or transferred in electronic form

The Security Rule is found in the Code of Federal Regulations (CFR) Title 45, Part 164, Subpart C, entitled “Security Standards for the Protection of Electronic Protected Health Information”.

The portion of Subpart C that is applicable to Wi-Fi client devices and networks is section 164.312, which lists technical safeguards for these areas:

1. **Authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information (ePHI) is the one claimed.
2. **Access control:** Ensure that only authorized users can gain access to ePHI.
3. **Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.
4. **Integrity.** Implement policies and procedures to protect ePHI from improper alteration or destruction.
5. **Audit controls.** Implement mechanisms that record and examine activity in information systems that contain or use ePHI.

A security system that relies on WPA2-Enterprise provides the capabilities needed to address the requirements in the first three areas because it ensures:

- Strong, mutual authentication between every properly configured client device and a hospital network where ePHI is present to ensure that:
  - Only trusted Wi-Fi clients can gain network access
  - Trusted Wi-Fi clients are not tricked into connecting to an untrusted network
- Strong encryption of ePHI that is transmitted between a Wi-Fi client and the hospital network

HIPAA requirements for item numbers 4 and 5 shown above are outside the scope of the Wi-Fi Alliance but can be addressed through traditional network and data security best practices.

### Sidebar 3: Risk Management for IT Networks in Hospitals

The 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 80001-2-3: 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.