# Global Information Assurance Certification Paper

Caroline Low
GIAC Practical
Version1.4b, Option 1
3/25/2003

# Wireless Wellness:
# Wireless LAN Security Considerations for the Healthcare Community

## Abstract

Healthcare organizations contribute to the high growth of Wireless Local Area Networks (WLANs), especially since WLANs significantly improve the capabilities of healthcare operations, clinically and administratively. This paper explores the security issues that the healthcare community needs to consider while embracing wireless technology. It introduces wireless technology concepts, covers wireless security concerns relating to health information privacy and HIPAA, network access control, and network reliability. Finally, this paper will propose measures to address security issues and mitigate threats.

## Mobilizing medicine

In a Washington, D.C. hospital, a doctor in the intensive care unit retrieves an x-ray to check the condition of a patient's lung. The doctor reaches into her pocket to pull out a Personal Digital Assistant (PDA), which within seconds delivers an image of the desired x-ray. Meanwhile, in the University of Maryland Medical System at Baltimore, doctors in the cardiology unit make their rounds with wireless computer tablets, gaining instant capability to input and access patient records and reports on the hospital network. [1]

These scenes are not visions of the future -- they actually reflect the present, where wireless networks are coupled with wireless devices to revolutionize patient care for healthcare organizations (HCOs).

It is not surprising to see the speed at which the healthcare industry embraced this form of technology. Advances in standards, performance, and prices in the last couple years have made 802.11b wireless local area networks (WLANs) a practical solution for increasing communication capabilities within HCOs. According to Gartner, Inc., a technology research and advisory firm, the WLAN is the fastest growing wireless technology. The number of North American WLAN users quadrupled from

[1] Alan Joch, "Wireless Watchdogs", *Healthcare Informatics Online*, July 2002, <http://www.healthcare-informatics.com/issues/2002/07_02/wireless.htm> (2 February 2003), Real World Results.

approximately 4 million users in 2000 to an estimated 16 million users in 2003. Gartner projected that by 2004, about 24 million people will be using WLANs.[2]

WLANs increase HCOs' capabilities to efficiently communicate and store/retrieve medical and administrative information. Examples of different healthcare capabilities offered by wireless LAN technology include:

- Ambulatory medical care – Transmitting and receiving real-time patient monitoring data such as heart rate and blood pressure through the wireless network and enabling patient mobility.
- Access to diagnostic information – Point of care access to patient records, test results, and pharmaceutical information.
- Bedside admitting, discharge, and transfer for hospital patients.
- Referencing – Being able to check drug references, formulations, and side effects by querying pharmaceutical management systems.
- Digital transcription – Electronically translating and storing a physician's verbal notes.
- Voice–over–IP – Using voice communications through the WLAN to talk with staff and patients in the same facility.[3]

Wireless LANs offer many obvious benefits for the healthcare community, especially in the hospital setting. Its lack of infrastructure caters well to the mobile environment of hospitals, increasing productivity by bringing the power of computing to the point of care. For example, personnel can move freely between hospital rooms without having to return to a fixed station to access up-to-date information, allowing them to make accurate decisions and operate efficiently. This reduces medical errors and hospital stays, and increases the quality of patient care. WLANs can be installed faster and cheaper than wired LANs, making them flexible and scalable to the changing needs of HCOs. Biomedical and IT systems can be integrated into a single network infrastructure. Such benefits prove that WLANs offer a higher return on investment than wired LANs.

Despite the plethora of advantages WLANs provide for the healthcare community, wireless LANs still come with strings attached. The tradeoff for mobility and lower costs is increased security threats compared to that of traditional LANs. This paper strives to inform current and potential WLAN managers and users of wireless network security challenges applicable to the healthcare industry. Although implementing the strongest security mechanisms still might not fully ensure a wireless network's protection,

---

2 John Pescatore, *Wireless Networks: Can security Catch Up With Business?* <http://csrc.nist.gov/wireless/S08_State%20of%20industry-jp.pdf> (20 February 2003), WLAN: Fastest Growing Technology.

3 Beau Fidler, *Mobile Medicine,* 21 August 2001, <http://www.sans.org/rr/wireless/medicine.php> (20 February 2003), Why Wireless?

awareness of the wireless security issues and proper deployment of the security countermeasures will nevertheless mitigate the threats wireless networks face.

## WLAN Technology

A WLAN serves as a flexible data communications system to act as an extension to or substitute for a wired LAN. Data is transmitted and received over the air from one point to another using Radio Frequency (RF) and Infrared (IR) technology, not relying on any physical connection. In the United States, the Federal Communications Commission (FCC) set aside the 900MHz, 2.4Ghz, and 5Ghz radio frequency ranges, known as the industrial, scientific, and medical (ISM) band, for unlicensed commercial use.

WLANs were originally based on the IEEE 802.11 standard, established in 1997 for the specification of 1 to 2Mbps wireless data transmission. 802.11a was then established in 1999, improving data transmission speeds to 54Mbps using the 5Ghz band. Currently, most HCO WLANs are operating in the IEEE 802.11b standard, also called Wi-Fi (Wireless Fidelity), which provides data transfer rates of up to 11Mbps using the 2.4Ghz band. Two other IEEE standards, 802.1x and 802.11i, play an important role in the advancement of WLAN security and will be discussed later on in this paper. [4]

In addition to the above-mentioned technologies, caregivers have implemented another form of wireless technology into hospital networks. Bluetooth-compatible devices can operate in conjunction with Wi-Fi to enhance WLAN capabilities. Bluetooth is a wireless specification that enables short-range and low-cost communication connectivity between personal devices like mobile computers, portable handheld devices, and mobile phones. This technology allows clinicians to beam patient information directly between devices or to connect to the medical network.

Wireless LANs have two typical configurations. The most basic WLAN setup is the peer-to-peer network, also known as the ad-hoc mode. Two network clients equipped with wireless adapter cards form an independent network by being within range of one another. The clients directly communicate with each other without the involvement of additional infrastructure. [5]

The other typical WLAN configuration is the client and access point (AP) architecture, also known as the infrastructure mode. It consists of one or more access points in a fixed location that connect to the wired LAN through an Ethernet cable. Each access point serves as a communication beacon, accommodating connections from many wireless clients simultaneously. Clients with wireless adapter cards can transmit and

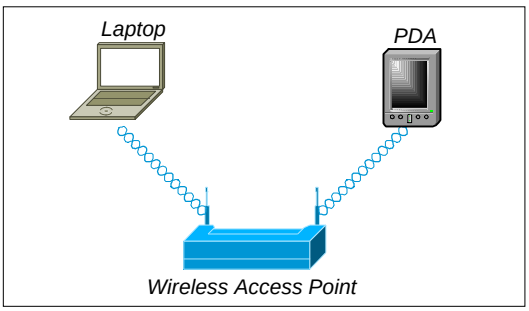
---

[4] Tom Karygiannis and Les Owens, *Wireless Network Security: 802.11, Bluetooth, and Portable Devices.* <http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf> (9 March 2003), Wireless Standards.

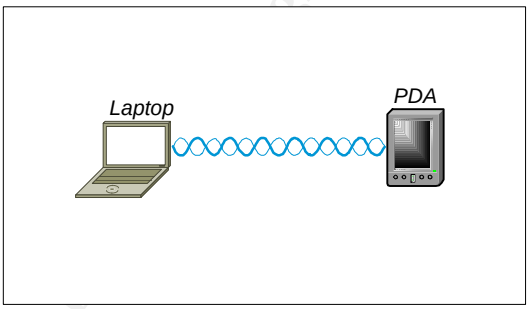
[5] Wireless LAN Association, *What is a Wireless LAN?* <http://www.wlana.org/learn/educate4.htm> (25 February 2003), Wireless LAN Configuration.

receive information through the AP if they are within transmission range, thus facilitating the client's communication with servers. [6]

**2 Types of Wireless Network Topologies:**




**Infrastructure Network Topology**




**Ad-hoc Network Topology**

According to Multi-Tech Systems Inc.'s *Wireless LAN Q&A,* "Access points have a finite transmission range, transmission -- around 100 meters (328 feet) indoors and 300 meters (984 feet) outdoors."[7] Overlapping more APs at the edges of the network range extends the WLAN's coverage area in a manner similar to cellular networks. Consequently, clients can roam throughout the network while maintaining connection, because when the client passes further beyond the boundaries of one AP's transmission range, another AP within closer range to the client will pick up the connection.

## Wireless security concerns

### Health Information Privacy

The use of airwaves instead of wires for data transmission increases WLAN's vulnerability to eavesdropping. In healthcare settings, this threat is paramount since it affects the privacy of patient data. When radio signals are sent from the wireless station to the AP, an anonymous attacker can passively listen to the signals and then decode the signals to gather the transmitted data. The passive nature of this attack complicates the detection of eavesdroppers. To eavesdrop, the attacker first obtains a computer system (usually a laptop or a PDA) equipped

---

[6] Multi-Tech Systems, Inc., *Wireless LANs Q&A*, 18 September 2001, <http://www.multitech.com/APPLICATIONS/WIRELESS/> (20 February 2003), What is a Wireless LAN?

[7] Ibid.

with a wireless networking card, the same type of hardware used by authorized wireless clients to communicate on their network. Using free software like NetStumbler, the attacker can detect available WLANs and record data about APs.

Next, the attacker needs to be within the communications range of the detected wireless transmitter. Radio signals can operate through walls, outside the physical confines of the network environment, and anything else not made of metal. Unfortunately, antennas and amplifiers, which were implemented to provide better coverage for the WLAN's authorized users, also propagate the radio signals so that someone with a listening device to eavesdrop from a further distance. In Merritt Maxim and David Pollino's book on wireless security, "recent tests of 802.11 wireless networking equipment show that an attacker can be nearly 20 miles away from a target and still receive a signal, thereby eavesdropping on wireless network communications."[8]

HCOs experience additional pressures to protect sensitive patient information due to government regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA was designed to help workers maintain insurance coverage by standardizing and simplifying healthcare-related information processing. In order to accomplish this, the US government included within HIPAA security and privacy rules for all protected health information.[9]

HIPAA's privacy rules mandate that all forms of health information (e.g. electronic, paper) be safeguarded from any intentional or unintentional use or disclosure. The security rules enforce this mandate by setting strict standards for how electronic health information will be protected -- such as access control, encryption, auditing, security management, and incident response.[10]

The technologically-neutral regulation puts caregivers who use WLANs in a predicament; patient data stored and transmitted 802.11b networks are inherently more vulnerable to security and privacy risks than wired networks. This means that HCOs with WLANs need to be more conscientious about HIPAA compliance. Healthcare providers who do not comply with HIPAA regulations will face penalties enforced by the Department of Health and Human Services (DHHS). The penalties range from "US$100 per worker per incident for unintentional HIPAA violations to $250,000 and 10 years in jail for intentional violations."[11]

---

[8] Merritt Maxim and David Pollino, *Wireless Security*, San Francisco: The McGraw-Hill Companies, 2002, p 49.

[9] Phoenix Health Systems, *HIPAA Primer*, <http://www.hipaadvisory.com/regs/HIPAAprimer1.htm> (15 March 2003), What is HIPAA?

[10] Phoenix Health Systems, "Security Standards", *HIPAAdvisory*, 20 February 2003, <http://www.hipaadvisory.com/regs/finalsecurity/comments.htm#general> (15 March 2003), General Issues.

[11] Christa L. Coleman, "Will Wireless Throw healthcare through a Loop?", Advisor Magazine, 7 January 2003, <http://securityadvisor.info/doc/11557> (9 March 2003).

**Controlling access to health network systems**

Data privacy becomes harder to protect once an intruder gains access to a WLAN. When inside the network, an intruder may be able to view, modify, and even forge the health care provider's medical and administrative information. The attacker may also be able to tamper with healthcare applications that run medical equipment.

Wireless networks provide new avenues for obtaining unauthorized access. The following are some examples:

- **Rogue Network Access Points** – An attacker may try to attain network access information by deploying rogue APs. These counterfeit APs may attract unsuspecting users and trick them into mistaking the APs for legitimate APs. If an unauthorized AP emitting a stronger signal than the original AP is placed closer to the wireless clients, the rogue AP could masquerade as a trusted network resource. As a result, users may unknowingly try to log into the attacker's honeypot server and give away authentication information like passwords and usernames.

  Networks are also susceptible to rogue access points set up by regular users. Driven by the need for convenience, users may inadvertently open up a backdoor to the network by setting up their own APs that have not been approved by those responsible for the network's security. It is incredibly easy to obtain and install rogue APs, since they can be purchased for as little as $50.

  The John's Hopkins Medical Campus *Wireless Bridge and Access Point Policy* makes several important points about the problems with user installed APs. [12] Those APs usually have "no security and are wide open for anyone to attach to and enter into our network." Their improper placement can also cause interference with other legitimate wireless installations and patient monitoring devices. The dangers of interference will be discussed later in this paper.

- **Rogue clients** - An intruder may mimic a client's identity and pretend to be an authorized user in order to enter the WLAN system. This is possible with a compromised access device such as a stolen laptop or another small device that is already linked to the network. The intruder can also use his or her own wireless device along with access information that was gathered from eavesdropping to log into the network. As a rogue client, the malicious entity can use the WLAN to connect to other organizations and launch attacks under a concealed identity.

---

[12] Johns Hopkins Networking and Telecommunications Services Web, *Wireless Bridge and Access Point Policy*, <http://nts.jhmi.edu/networking/wirelesspolicy.cfm> (15 March 2003).

### Network Reliability

Radio interference poses as another security concern for WLANs because it can decrease network bandwidth and throughput. Interference in a WLAN occurs when network traffic overlaps with signals emitted by entities that operate in infrared or the same unlicensed 2.4 GHz radio frequencies. Such entities include Bluetooth devices, cordless phones, microwave ovens, medical equipment, and other WLANs. Most of the time, interference happens unintentionally -- when both devices are located too close to each other.

Interference can be powerful enough to overwhelm weaker signals and cause jamming, where communications between parties may totally cease. This is also known as a Denial of Service (DoS) attack. Jamming can also be aimed towards a particular access point or client. After the targeted device is jammed, the attacker can impersonate the disabled device as a rogue client or AP.[13]

## Securing WLAN Transmissions with OSI (Open Systems Interconnect) Layer Controls

### MAC Address Filtering

Access points can filter MAC (Media Access Code) addresses, which are the hardware addresses for clients' network cards, to allow certain trusted wireless clients a connection to the network. APs contain an Access Control List (ACL), which includes all MAC addresses allowed on the WLAN. When a client station tries to associate with the AP, the AP's router reads the unique MAC address on the client's network card and then compares it against the AP's ACL. If the MAC address is included in the list, the client will be able to access the network.

MAC address filtering protects the network from unauthorized devices, but does not protect WLANs from intruders who could be operating authorized devices. Another limitation of this security feature is the extensive administrative effort needed to maintain and configure each AP's ACL for every trusted client.

### Wired Equivalent Privacy (WEP)

To address the privacy needed in WLAN systems, IEEE 802.11 offers the Wired Equivalent Privacy (WEP) protocol, which provides encryption and authentication methods that operate at the data link layer of the OSI model. WEP was intended to help WLANs match its privacy levels with wired LANs by encrypting radio signals with a shared key. Encryption with a shared key was supposed to protect

---

[13] Randall K. Nichols and Panos C. Lekkas, *Wireless Security: Models, Threats, and Solutions*, New York City: The McGraw-Hill Companies, 2002, p 336.

wireless communications from other devices that do not know the key. WEP was also intended to prevent unauthorized users.

Unfortunately, the current implementation of WEP and the RC4 encryption algorithm has rendered the protocol open to compromise and virtually useless. If the WEP keys are not updated often, freely available exploit tools like AirSnort and WEPCrack can crack a WEP-enabled network's encryption keys within a few hours of gathering and analyzing transmitted packets. After the static shared keys have been recovered, the attacker can join the network. Therefore, both the 40-bit and 128-bit versions of WEP cannot be relied upon for security. Nevertheless, because many 802.11-compliant WLAN products support WEP as a standard feature, it is better to protect a WLAN's privacy using WEP as a minimal form of security than not use any security measures at all.[14]

**802.1x**

While WEP is sufficient for protection against the casual snooper, it is without a doubt inadequate for securing sensitive information transmitted within healthcare networks against attackers with off-the-shelf tools. As a result, standards committees have sought to overcome WEP's shortcomings by introducing 802.1x, a stronger alternative to WEP. 802.1x is a link layer standard that defines port-based authentication and key distribution mechanisms that can be applied in Ethernet or wireless LANs. In a WLAN, before the wireless client can connect to the AP, the AP would verify that the client is a valid user by using an authentication server such as Remote Authentication Dial-In User Service (RADIUS) or Kerberos. Once verified, the AP will allow the client to send and receive transmissions through a port on the AP. The dynamic key exchange mechanism that is optional in 802.1x allows for encryption keys to be changed often, reducing an attacker's chances of recovering the current WEP key[15]. 802.1x's features reduce a WLAN's vulnerability towards eavesdropping, rogue clients, and effectively address HIPAA's privacy concerns.

**Wired Protected Access (WPA) and 802.11i**

Jim Geier of *802.11 Planet* concisely described WPA as "a snapshot of the current version of 802.11i."[16] 802.11i currently incorporates some of the data link layer protection offered by 802.1x with Temporal Key Integrity Protocol (TKIP).

As mentioned in the previous section, 802.1x requires a user to authenticate through the AP and a login server before he or she can access the WLAN. TKIP

---

[14] Jim Geier, "802.11 WEP: Concepts and Vulnerability", *802.11 Planet*, 20 June 2002, <http://www.80211-planet.com/tutorials/article.php/1368661> (10 March 2003), When WEP Makes Sense to Employ.

[15] Jim Geier, "802.1x Offers Authentication and Key Management", *802.11 Planet*, 7 May 2002 <http://www.80211-planet.com/tutorials/article.php/1041171> (20 March 2003), 802.1x in Action.

[16] Jim Geier, "WPA Security Enhancements", *802.11 Planet*, 20 March 2003, <http://www.80211-planet.com/tutorials/article.php/2148721> (23 March 2003) Inside WPA.

strengthens WEP's encryption system by supplying additional checks for message integrity and making the 802.11 frames harder to decrypt.

802.11i also provides greater security by replacing WEP's RC4 encryption algorithm with AES (Advanced Encryption Standard). It is unknown when the 802.11i standard will be ready for implementation.

### VPNs and IPSec, SSL and Terminal Services

To further ensure the confidentiality of the data being transmitted over a wireless network, additional encryption methods can be applied to the other layers of the OSI model. Virtual Private Networks (VPNs), commonly deployed using the IPSec protocol, create a virtual tunnel between two specific endpoints, such as a laptop and an access point. All traffic that travels within the virtual tunnel is protected by encryption and authentication. VPNs operate at the network layer – other encryption methods like SSL (Secured Sockets Layer) and terminal services operate at the application and session layer, respectively.

## Other Ways to Protect from Network Detection and Eavesdropping

### RF limiting

Lowering RF signals will limit the extent of the wireless network coverage to reduce a WLAN's vulnerability towards eavesdropping and unauthorized access. It becomes harder for war-drivers and other potential attackers to detect the WLAN if the network's transmission power is at the lowest setting needed to communicate. RF signals can be attenuated by lowering the transmit power configuration on the access points. Directional antennas can also be used to control where the wireless radio signals travel. An additional way to prevent excessive RF signal leakage is to incorporate materials like metallic paint and blinds into the design of building facilities. Metal's properties encourage signal attenuation.[17]

### Access Point Configuration

Some of the simplest steps that would reduce a WLAN's risk towards detection and eavesdropping can be done by properly configuring access points. The following are some configuration tips:

- Change the access point's Service Set Identifier (SSID), which is the wireless network's name, from the default factory setting to a name that is hard for an outsider to guess.
- Disable the access point's broadcast beacon. The broadcast beacon announces the presence of the AP to anyone within range.

[17] Maxim and Pollino, *Wireless Security*, p 194.

## Detecting Rogue Access Points

Rogue access points can be identified using 802.11b analyzers like NetStumbler or Cisco's AiroPeek.[18] These tools sniff wireless packets that travel within their range and can be used to detect access points and their vendor names, MAC addresses, and security configurations. Access points that have differing information than what is authorized on the WLAN may turn out to be rogue APs. An alternative way to identify rogue access points is to use Transmission Control Protocol (TCP) port scanners such as SuperScan 3.0. The scanning tool can detect all Port 80 (HTTP) connections to the network, which could include most access points. The access points usually respond with their vendor names and IP addresses, so one would be able to notice a rogue access point if its vendor name seems to be unauthorized.

Unfortunately, new rogue APs can appear on the WLAN right after other rogue APs have been discovered. Finding the rogues becomes more difficult if the WLAN spans across more buildings and wider geographical area. Ideally, centralized monitoring devices such as AirWave could ease their detection. These consoles use existing authorized access points to listen for rogue APs and alert personnel of their appearance.

## Reducing Vulnerabilities to Intentional Interference

Deploying a network using the 802.11a standard will eliminate issues with interference. This standard uses the 5GHz band for radio transmissions, completely different than other devices (microwaves, cordless phones, etc.) that would normally interfere with 802.11b WLANs. Less devices share the 5Ghz ISM band compared to the 2.4Ghz band, so for that reason an 802.11a network will not be as susceptible to interference.

To reduce the chances of jamming, deploy a WLAN with both the 802.11a and 802.11b standard – a network that uses two different bands is less likely to completely jam. Using both a wired network in addition to the WLAN will also mean that some of the network will still function if the WLAN ceases communications due to jamming.

## Conclusion

It is important to realize that the recommended security measures would only be useful in providing a substantial amount of security if implemented in layers. Additional research is recommended before deploying any solution because implementation mistakes and misconfiguration can significantly reduce the effectiveness of a WLAN's security.

---

[18] Air Defense Inc., *White Paper Summary – Enterprise Approaches to Detecting Rogue Wireless LANs*, <http://www.airdefense.net/eNewsletters/rogue_feature.shtm> 30 March 2003.

Hospitals, clinics, and private practices will face additional challenges as they strive to accommodate new wireless technologies and threats. For example, in December 2002, the Swedish Space Corporation achieved Wi-Fi broadband connectivity of almost 200 miles[19]. With increased convenience and capabilities comes increased risk to all the threats that were discussed in this paper. Nevertheless, awareness of those risks will aid and help bring a healthcare network one step closer to increased security.



19 Alvarion Ltd., Press Release: *World's Longest Wi-Fi Connection Made by The Swedish Space Corporation,* 12 December 2002 < http://www.alvarion.com/RunTime/CorpInf_30130.asp?fuf=281&type=item> (20 February 2003).

## References


Air Defense Inc. *White Paper Summary – Enterprise Approaches to Detecting Rogue Wireless LANs*, <http://www.airdefense.net/eNewsletters/rogue_feature.shtm>30 March 2003.

Alvarion Ltd. *Press Release: World's Longest Wi-Fi Connection Made by The Swedish Space Corporation.* 12 December 2002. <*http://www.alvarion.com/RunTime/CorpInf_30130.asp?fuf=281&type=item*> *(20 February 2003).*

Coleman, Christa L. "Will Wireless Throw healthcare through a Loop?" *Advisor Magazine*, 7 January 2003. <http://securityadvisor.info/doc/11557> (9 March 2003).

Fidler, Beau. *Mobile Medicine*. 21 August 2001. <http://www.sans.org/rr/wireless/medicine.php> (20 February 2003).

Geier, Jim. "802.11 WEP: Concepts and Vulnerability." *802.11 Planet*. 20 June 2002. <http://www.80211-planet.com/tutorials/article.php/1368661> (10 March 2003).

Geier, Jim. "802.1x Offers Authentication and Key Management." *802.11 Planet*. 7 May 2002 <http://www.80211-planet.com/tutorials/article.php/1041171> (20 March 2003).

Geier, Jim. "WPA Security Enhancements." *802.11 Planet*. 20 March 2003. <http://www.80211-planet.com/tutorials/article.php/2148721> (23 March 2003).

Joch, Alan. "Wireless Watchdogs." *Healthcare Informatics Online,* July 2002. <http://www.healthcare-informatics.com/issues/2002/07_02/wireless.htm> (2 February 2003).

Johns Hopkins Networking and Telecommunications Services Web. *Wireless Bridge and Access Point Policy*. <ttp://nts.jhmi.edu/networking/wirelesspolicy.cfm>(15 March 2003).

Karygiannis, Tom and Owens, Les. Wireless Network Security: 802.11, *Bluetooth, and Portable Devices*. <http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf> (9 March 2003).

Klaus, Christopher. *Wireless LAN 802.11b Security FAQ*. 6 October 2002. <http://www.iss.net/wireless/WLAN_FAQ.php> (25 February 2003).

Maxim, Merritt and Pollino, David. *Wireless Security.* San Francisco: The McGraw-Hill Companies, 2002.

Multi-Tech Systems, Inc. *Wireless LANs Q&A*. 18 September 2001. <http://www.multitech.com/APPLICATIONS/WIRELESS/> (20 February 2003).

Nichols, Randall K. and Lekkas, Panos. *Wireless Security: Models, Threats, and Solutions.* New York City: The McGraw-Hill Companies, 2002.

Pescatore, John. Wireless Networks: Can security Catch Up With Business? <http://csrc.nist.gov/wireless/S08_State%20of%20industry-jp.pdf> (20 February 2003).

Phoenix Health Systems. *HIPAA Primer*. <http://www.hipaadvisory.com/regs/HIPAAprimer1.htm> (15 March 2003).

Phoenix Health Systems. "Security Standards". *HIPAAdvisory*. 20 February 2003. <http://www.hipaadvisory.com/regs/finalsecurity/comments.htm#general> (15 March 2003).

Wireless LAN Association. *What is a Wireless LAN?* <http://www.wlana.org/learn/educate4.htm> (25 February 2003).