

Wireless Networking: Addressing the Health Insurance Portability and Accountability Act Requirements

This white paper will address the concerns around wireless networking technologies within the context of the Health Insurance Portability and Accountability Act (HIPAA) and provide insights into how Cisco wireless solutions fit into the framework of HIPAA security. In order to do this effectively, the paper will first provide some background on HIPAA legislation, specifically focusing on the various pieces as they relate to security; discuss the common concerns and security challenges of wireless LAN technology; and finally conclude by demonstrating how Cisco's wireless solutions can be deployed to address security issues for HIPAA compliance.

What is HIPAA and how is WLAN technology relevant to HIPAA compliance?

The Health Insurance Portability and Accountability Act (HIPAA) passed in 1996, mandates that health care entities covered under the Act take appropriate minimum measures to ensure the protection of the personal information (PI) of their patients, customers, and partners. The impact of this legislation and the enforcement regulations developed under HIPAA by the Department of Health and Human Services (DHHS) will continue to grow in significance as the regulations become final and deadlines for compliance draw closer. Thus, health care industry professionals are increasingly assessing the ability of the solutions they deploy to enable HIPAA compliance.

Wireless LANs (WLANs) represent a networking technology growing in popularity within health care organizations. The security concerns identified in WLAN deployment, however, have caused concerns within these organizations when taking into account HIPAA security standards and guidelines. These concerns, if not properly addressed, could represent an inhibitor to adoption of wireless networking technologies in the health care sector. For health care entities that are deploying WLAN technologies, ensuring that the security challenges of wireless networking are addressed within the network will become necessary to successful HIPAA compliance strategies. Cisco wireless solutions provide health care entities covered under HIPAA with robust and flexible mechanisms for protecting the security and privacy of information in a WLAN environment, and can play an important part in both an organization's networking and HIPAA compliance strategies.



It should be noted that HIPAA and the associated DHHS regulations cover a variety of privacy issues surrounding personal health information, and represent fairly complex requirements that cover information management and protection strategies throughout the organization. Thus, no one technology affords complete compliance to all HIPAA guidelines, and no WLAN technologies currently available address all security requirements under the proposed standards. However deployments of wireless networking solutions, when combined with other security controls and mechanisms within the context of an effective risk management strategy and policy, can effectively meet the security standards as proposed under HIPAA. To that end this paper addresses the following topics:

- HIPAA and the proposed DHHS security regulations
- Security challenges in WLAN deployment
- Mapping Cisco wireless solutions to HIPAA security standards

Additionally, a quick summary of proposed HIPAA security standards and Cisco security solutions is available at the end of the document in an 'at-a-glance' table.

HIPAA and DHHS Proposed Security Regulations

The HIPAA legislation proposes a set of standards to regulate the electronic interchange of health information and to protect the confidentiality and security of electronic health information. It applies to virtually all segments of the health care industry that transmit any health information that is in electronic form and contains "identifiable" content that could compromise the confidentiality of a patient. The recommendations set forth within HIPAA are intended to assist the United States Congress and the DHHS in the development and enactment of regulations regarding the maintenance and transmission of health information pertaining to individual patients. The penalties for non-compliance can be significant. HIPAA states that the general penalty for "failure to comply" would range from \$100 to \$25,000 based on the number of violations, and the penalty for wrongful disclosure of individually identifiable health information would range from \$50,000 to \$250,000.

The DHHS regulations for implementing HIPAA are divided into four areas:

- Transaction and Code Sets
- Privacy
- Security
- Provider Identifiers

At the time of this writing, the Transaction and Code Sets and Privacy regulations were finalized, while regulations covering Security and Provider Identifiers remain in the proposal stage. However many covered health care entities have discovered that implementing the final privacy regulations is heavily dependent upon the proposed standards for security. As such, many organizations are seeking to implement security strategies based upon the proposed security regulations under the assumption that the final Security rules will not differ greatly from those proposed, and in an attempt to meet HIPAA deadlines in a timely fashion

Requirements for security under the proposed DHHS guidelines are encompassed in *45 CFR Part 142—Security and Electronic Signature Standards*. While the regulations are not yet finalized, many industry experts anticipate that the final regulations will not significantly differ from the proposed draft.



To ensure a comprehensive approach to HIPAA compliance for wireless deployments in health care, covered entities must take into consideration administrative, physical, and technical security mechanisms as outlined by 45 CFR Part 142. The 5 distinct areas of security implementations covered by this regulation are:

- Administrative Procedures
- Physical Safeguards.
- Technical Security Services
- Technical Security Mechanisms
- Electronic Signature Standard

Each area is described below and covered by a subsection of the regulation.

Administrative Procedures

The proposed HIPAA security standard requires that certain administrative and procedural controls be in place within a covered organization to protect data integrity, confidentiality, and availability. These provisions are non-technical in nature and define high-level policy and procedural infrastructures. However, deployments of WLANs should be considered in developing these policies and procedures, and such deployments should conform to these documented policy requirements. Administrative procedures proposed under HIPAA security standards include:

- Certification of the security of computer systems or network designs.
- Chain of trust partner agreements to protect data processed through third parties.
- Contingency plans for responding to system emergencies.
- Formal mechanism for processing records from receipt through disposal.
- Information access control for granting access to health care information.
- Internal audit of the records of system activity maintained by an entity.
- Personnel security policies and procedures for granting clearance to personnel.
- Security configuration management for information systems.
- Security incident procedures for responding to and reporting security incidents.
- Security management processes to address potential security breaches.
- Termination procedures for ending employee and user access.
- Security training for staff.

Detailed descriptions of the proposed Administrative Procedures requirements may be found at <http://aspe.hhs.gov/admsimp/nprm/sec06.htm>.



Physical Safeguards

In addition to administrative procedures for protecting data, the proposed security standard requires covered entities to undertake processes to ensure the physical protection of information systems. While these proposed requirements do not address technical controls, deployments of wireless networks should be undertaken to conform to these policies and procedures. In particular, the location of wireless access points (APs) as well as policies and training on the secure use of WLANs should be considered. Physical safeguards to information systems defined in the standard include:

- Assigned security responsibility for a specific individual or organization.
- Media controls to govern the receipt and removal of hardware and software.
- Physical access controls for limiting physical access to a covered entity.
- Policy/guideline on workstation use within a covered entity.
- Secure workstation location to eliminate the possibility of unauthorized access.
- Security awareness training for all employees, agents, and contractors.

Detailed descriptions of the proposed Physical Safeguards requirements may be found at <http://aspe.hhs.gov/admnsimp/nprm/sec07.htm>.

Technical Security Services

The proposed security standard mandates certain levels of technical control be built into a covered entity's information systems. These controls may include security inherent in individual security technologies and products, as well as larger infrastructure controls achieved through integrated security solutions. Technical security services include:

- *Access controls*—Technical controls to restrict access to resources and allow access only by privileged entities. Controls include emergency access procedures; context-, role-, or user-based access controls in information systems; and optional encryption controls.
- *Audit controls*—Audit control mechanisms to record and examine system activity.
- *Authorization controls*—Mechanisms to ensure that only properly authorized individuals are able to access or use health information.
- *Data integrity*—Corroboration that data has not been altered or destroyed in an unauthorized manner, including the use of check sums, double keying, message authentication codes, or digital signatures.
- *Entity authentication*—Corroboration that an entity is who it claims to be. Controls include unique user identification and automatic logoff mechanisms, passwords, personal identification numbers (PINs), tokens, automatic callback mechanisms, or biometric identification.

Detailed descriptions of the proposed Technical Services requirements may be found at <http://aspe.hhs.gov/admnsimp/nprm/sec08.htm>.



Technical Security Mechanisms

The proposed security standard requires that communications and network controls be put in place whenever information is transmitted over a public or private network. When deploying WLANs, the following mandatory and optional controls should be considered as part of any implementation:

- Integrity controls for all network communications over public or private networks utilized by a covered entity.
- Message authentication for all network communications over public or private networks utilized by a covered entity.
- Access controls or encryption to protect transmitted health information on public and private networks. Over a public network, encryption is required to protect transmitted health information.
- Alarm mechanisms
- Audit trails
- Entity authentication
- Event reporting

Detailed descriptions of the proposed Technical Security Mechanisms requirements may be found at <http://aspe.hhs.gov/admnsimp/nprm/sec09.htm>.

Electronic Signature Standard

Under the proposed security standard, electronic signatures are not required for any proposed standard transactions. However, in cases where a HIPAA specified transaction requires the use of an electronic signature, the following standard applies:

- Mandatory features for message integrity, non-repudiation, and user authentication.
- Optional features for the ability to add attributes, continuity of signature capability, countersignatures, independent verifiability, interoperability, multiple signatures, and transportability.

What are the security challenges associated with WLAN deployment?

A proliferation of client devices, and the low cost and ease of deployment of WLAN infrastructure coupled with the ability of wireless technology to reduce a number of administrative health care costs, and increase the productivity of clinical staff who are short in supply, is driving WLAN adoption at rates challenging to many IT departments. Security issues with these deployments, however, are not insignificant. Security weaknesses in the IEEE 802.11b wireless standard, specifically the Wired Equivalent Privacy (WEP) security model defined by the standard, have aroused the curiosity and interest of hackers and criminals, and have been widely documented and published. Under the proposed HIPAA security standards, these weaknesses in wireless security represent a fundamental challenge to implementing WLAN technologies in a health care environment. Many health care entities covered under HIPAA are concerned that such deployments may place them in a position of non-compliance to the DHHS security regulations when they are finalized.

The good news is that wireless networking technologies, when properly configured and deployed, can incorporate strong security as required under HIPAA. Cisco wireless solutions provide many of the explicit controls mandated or recommended by proposed HIPAA security regulations. When combined with interoperable network and security solutions to create an end-to-end approach to security, Cisco wireless solutions can assist an organization in deploying effective wireless infrastructures while still addressing the requirements under the proposed DHHS security standards.



General Security Concerns with Wireless LANs (WLANs)

Wireless networks have become one of the most interesting targets for hackers today. Because most WLAN devices ship with all security features disabled, this wide deployment attracted the attention of the hacker community. Several Web sites have now started documenting all the freely available wireless connections nationwide. Although most hackers are using these connections as a means to get free Internet access or to hide their identity, a smaller group sees this situation as an opportunity to break into networks that otherwise might have been difficult to attack from the Internet. Unlike a wired network, wireless networks send data over the air and usually extend beyond the physical boundary of an organization. In particular, when strong directional antennas are used, a WLAN can reach well outside the building in which it is deployed. This scenario creates an environment where traditional physical security controls are ineffective because the packets can be viewed by anyone within radio frequency range. For example, a person with a Linux laptop and a sniffer program such as TCPdump can take advantage of this concern and receive and store all packets circulating on a given WLAN.

In the hands of a determined attacker, a rogue wireless AP can be a valuable asset in the attempted compromise of network resources. The principal threat is installing an AP into a network after gaining unauthorized access to a building. A possible scenario involves the attacker gaining access to the building by “tailgating” behind a user with a valid access badge or by obtaining a guest badge for some other reason. Because APs are relatively small and can be purchased at many electronics outlets worldwide, it is easy for the attacker not only to obtain the AP but also to install it discreetly. Also consider the possibility of man-in-the-middle (MITM) attacks. Using a device that can masquerade as a trusted AP, a skilled attacker could manipulate wireless frames as they cross his or her device.

Concerns with 802.11b and the Wired Equivalent Privacy (WEP) Protocol

802.11b is the most widely deployed WLAN technology today. The foundation of the security of 802.11b is based on a frame encryption protocol called Wired Equivalent Privacy (WEP).

The 802.11 standards define WEP as a simple mechanism to protect the over-the-air transmission between WLAN access points and network interface cards (NICs). Working at the data link layer, WEP utilizes the RC4 encryption algorithm and requires the same secret key to be shared by all communicating parties. To avoid conflicting with U.S. export controls that were in effect at the time the standard was developed, 40-bit encryption keys were required by IEEE 802.11b, though many vendors now support the optional 128-bit standard.

There has been a great deal of research into the shortcomings of WEP security. Problems have been identified with insufficient key lengths (Walker), with the design of the WEP specification itself (Borisov, Goldberg, and Wagner), and with WEP's use of the RC4 encryption algorithm (Fluhrer, Shamir, and Mantin).

WEP can be easily cracked in both 40- and 128-bit variants by using off-the-shelf tools readily available on the Internet. The IEEE 802.11 standard describes the use of encryption and keys in WEP, but does not specify specific methods for key distribution. Without an automated method for key distribution, any encryption protocol will have implementation problems due to the potential for human error in key input, escrow, and management.

Several tools exist to leverage these vulnerabilities in the WEP specification including that developed by John Ioannidis and Avi Rubin of AT&T Research Labs and Adam Stubblefield of Rice University, as well as the independently developed and available AirSnort.



How do Cisco Wireless Solutions map to HIPAA Security Standards?

Given the security weaknesses inherent in existing WLAN technologies, entities covered by HIPAA and the proposed security standard must ensure that wireless deployments within their organizations meet HIPAA requirements and guidelines for the protection of health information traversing the network. Cisco provides a number of recommendations and solutions for securing WLANs deployed within an organization, and meeting the requirements of the proposed HIPAA security standard.

The Importance of Policies

The HIPAA security standard mandates that policy infrastructures exist in the form of administrative procedures and physical safeguards to protect health information on networked systems. Policies and procedures are two primary weapons an organization has to combat the threat to wireless network security. From a policy perspective, Cisco recommends that an organization have a complete wireless network policy in addition to its overall security policy. This wireless policy should, at a minimum, disallow the connection of non-IT supported APs into the network. On the procedures side, the IT department needs to conduct regular scans of its office space to check for rogue APs. This includes both physical searches and wireless scans. Several vendors offer tools designed to discover the presence of the wireless APs in a certain area, and Cisco provides similar services as part of a Cisco Security Posture Assessment (SPA). To meet specific HIPAA requirements, Cisco recommends that WLAN deployments conform to policies, procedures, and practices as defined by the appropriate subsections of the HIPAA security standard, and that regular testing of the WLAN be performed to maintain the security of the deployment.

Improving Security of WLANs with Cisco Solutions

Most WLAN devices ship with security features disabled, thus making default deployment of these devices unsuitable for an organization covered under the HIPAA security standard. It therefore becomes necessary in a HIPAA environment to build or enable additional security around a WLAN deployment in order to meet regulatory security requirements. Cisco wireless solutions provide a number of mechanisms for supporting required security standards in both the wireless device itself as well as within the rest of the network. These mechanisms provide a more robust alternative to WEP and may prove more suitable in HIPAA environments. No one solution can be said to be more or less compatible with proposed HIPAA security requirements. DHHS has deliberately created flexible and non-specific security guidelines so as to provide covered entities with the ability to choose appropriate security solutions based upon existing network designs, business models, and risk management strategies. The strategy of Cisco on wireless security is to provide maximum choice to customers in implementing secure WLAN infrastructures through the mechanisms discussed below.

Improving WLAN Security with 802.1X and TKIP

The IEEE 802.11 Task Group i (802.11i) is in the process of defining the new standard for WLAN security. The 802.11i draft standard includes the use of 802.1X for authentication and key management, the use of software-based Temporal Key Integrity Protocol (TKIP) algorithms to strengthen WEP keys, and the eventual replacement of RC4 with AES as the algorithm used to encrypt and decrypt WLAN data.



By using the framework defined by the IEEE 802.1X standard, a WLAN can support centralized authentication and dynamic key distribution. When 802.1X operates on a WLAN, a supplicant on a client device authenticates to an authenticator on the access point, which interacts with an authentication server, typically a RADIUS server, to complete the authentication. 802.1X specifies the use of the Extensible Authentication Protocol (EAP) as defined in RFC 2284, between the supplicant and the authenticator during the authentication process.

802.1X supports different EAP types, or authentication types that use EAP. With EAP-Cisco Wireless, or LEAP, a logon username and password is used to authenticate both the WLAN client and the authentication server. EAP-TLS requires the deployment of a Public Key Infrastructure (PKI) to support the use of digital certificates for authenticating both the wireless client and the authentication server. Because many customers were daunted by the large administrative effort required by EAP-TLS, Cisco, Microsoft, and RSA Security defined Protected EAP, or PEAP. In PEAP, the supplicant uses TLS to authenticate the server via a certificate and to create an encrypted tunnel to the authentication server in a manner similar to the use of SSL in a Web browser. Once the encrypted tunnel is established, the client authenticates to the server using a logon password, a one-time password, or whatever criteria is required by the EAP type that operates through the tunnel. PEAP supplicants are available both from Cisco and Microsoft; other vendors have announced plans to provide additional PEAP supplicants.

With 802.1X, a wireless client that associates with an AP cannot gain access to the network until the client performs a network logon. Based on the type of EAP authentication method used the user must either enter a username and password into a network logon dialog box or its equivalent or provide a passphrase for a certificate. The client and an authentication server perform a mutual authentication, with the client authenticated by the supplied credentials. This mutual authentication reduces the risk of wireless clients connecting into unauthorized, or rogue, wireless access points within the network. The authentication server and client then derive a client-specific WEP key to be used by the client for the current logon session. Sensitive information is never transmitted in the clear, over the wireless link.

TKIP includes several measures to make WEP keys significantly less vulnerable to the types of WEP attacks described earlier. One TKIP element is key hashing, or per-packet keying. When key hashing is used, the encryption key for a packet is formed by hashing the base WEP key with information that is unique to the packet, such as the Initialization Vector (IV). As a result, the key is not vulnerable to an attack that exploits weak IVs as described in the Fluhrer, Mantin, and Shamir paper. Another TKIP element is message integrity check, or MIC. The use of MIC renders unsuccessful an active, bit-flipping attack, whereby an attacker intercepts an encrypted packet, flips bits, and resends it to the AP in the hopes that the network will generate a predictable error message. With MIC, a corrupted packet is discarded with no message generated.

The Wi-Fi Alliance, which certifies WLAN products as interoperable or Wi-Fi compliant, has defined the Wi-Fi Protected Access (WPA) specification which includes the use of 802.1X and TKIP. Beginning in 2003 the Wi-Fi Alliance will require WPA for Wi-Fi compliance.

Cisco Aironet products have supported the 802.1X standard since December 2000. Support for a pre-standard implementation of TKIP has been available in Aironet products since December 2001 and support for the standard TKIP will be available in 2003. Furthermore, Cisco plans to introduce AES support in the Aironet product line in the second half of 2003.



Improving WLAN Security with IPsec

IPsec is a framework of open standards for ensuring secure private communications over IP networks. IPsec VPNs use the services defined within IPsec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. IPsec also has a practical application to secure WLANs by overlaying IPsec on top of clear text 802.11 wireless traffic.

When deploying IPsec in a WLAN environment, an IPsec client is placed on every PC connected to the wireless network and the user is required to establish an IPsec tunnel to route any traffic to the wired network. Filters are put in place to prevent any wireless traffic from reaching any destination other than the VPN gateway and Dynamic Host Configuration Protocol/Domain Name System (DHCP/DNS) server. IPsec provides for confidentiality of IP traffic, as well as authentication and anti-replay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), which encrypts the data three times with up to three different keys.

Though IPsec is used primarily for data confidentiality, extensions to the standard allow for user authentication and authorization to occur as part of the IPsec process. This scenario offers a potential solution to the user differentiation problem with WLANs, which are outlined in the SAFE wireless white paper described below. For more information on IPsec, refer to the VPN primer in the SAFE VPN paper at http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml

There are difficulties with deploying IPsec across the WLAN environment. One problem is that the deployment of IPsec across the WLAN environment makes traffic differentiation impossible. If traffic cannot be differentiated according to its content then network services such as QoS become impossible. Another problem stems from the fact that not all WLAN clients can support an IPsec client.

Supporting Security Technologies for End to End Network Security

WLAN technologies do not in and of themselves provide all controls mandated by the proposed HIPAA security standard. When deploying wireless network technologies in a HIPAA environment, organizations will need to utilize additional security technologies and solutions to ensure an end to end secure network meeting all technical security services and mechanisms to comply with HIPAA requirements. These solutions include:

- Firewalls and other access control mechanisms
- Intrusion detection mechanisms
- Management, monitoring, and logging mechanisms

The Cisco SAFE Blueprint: Matching Network Security with Security Policy and Risks

The SAFE Blueprint for Secure e-Business is a flexible, dynamic blueprint for security and virtual private networks (VPN). Based on the Cisco Architecture for Voice, Video, and Integrated Data (AVVID), SAFE enables organizations to deploy security solutions throughout a network via modules that simplify security design, rollout, and management. Each module includes the security and VPN components necessary to mitigate the specific threats found in each area of the network.



The proposed HIPAA security standard does not mandate any particular network or security design architecture for covered entities. However, the standard does identify basic controls that must be in place on any network that handles health information. Cisco has created the SAFE blueprint to help organizations build robust network security infrastructures. Through SAFE, Cisco can help health care entities address the requirement for layered technical security controls mandated in the proposed DHHS security regulations. More information on the SAFE Blueprint may be found at <http://www.cisco.com/go/safe>.

SAFE Wireless White Paper

As a component of the SAFE Blueprint, Cisco provides best practice information for designing and implementing WLAN security in networks utilizing elements of the SAFE blueprints. While not specific to HIPAA in its recommendations, the SAFE wireless white paper frames WLAN implementation within the context of overall security design and best practices, which are key to a successful overall HIPAA compliance effort. The SAFE wireless white paper may be found at http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml.

Comprehensive WLAN Security

When 802.1X and TKIP are used by all WLAN clients, or when IPSec is a mandatory WLAN overlay, then Cisco wireless devices not only provide adequate encryption to protect confidentiality and privacy of transmitted data, but also support robust authentication controls mandated by the proposed HIPAA security standard. When deployed as part of a SAFE-based infrastructure, including the use of firewalls and other access control mechanisms, network and host based intrusion detection technology, management, monitoring, and logging capabilities, a Cisco WLAN deployment takes an integrated approach to security that helps a health care entity to address the specific security requirements as proposed by DHHS. As previously stated in this paper, the importance and necessity of well designed administrative and policy infrastructures to support these implementations is also necessary, and Cisco technologies are easily incorporated and managed under such an infrastructure.

At A Glance: Proposed HIPAA Security Standard and Cisco Solutions

Table 1

HIPAA Security Standard	Requirements	Cisco Wireless Solutions
Administrative Procedures		Administrative requirements are of a policy and procedural nature and do not directly affect technical implementation of Cisco wireless technologies. However, administrative procedures should take into account technology issues and wireless deployments should conform to existing organizational administrative procedures.



Table 1 (Continued)

HIPAA Security Standard	Requirements	Cisco Wireless Solutions
Physical Safeguards		Physical safeguards, like administrative procedures, represent policy level controls rather than any direct requirement for Cisco wireless technologies. In this case those controls represent practices and procedures to protect physical devices from unauthorized access or exploitation, as well as to ensure adequate backup and recovery of systems and data. Wireless network deployment should take into account physical security issues surrounding wireless enabled workstations and systems, location of wireless access points, and access control to physical media, systems, and facilities.
Technical Security Services	<ul style="list-style-type: none"> • Access Control • Emergency Access • Context-based • Role-based • User-based 	Use of 802.1X authentication within Cisco wireless products provides for user-based access control by requiring users to authenticate prior to gaining access to the wireless network. Additional controls can be implemented, including hardware address (MAC) filtering at the wireless AP. Other access control mechanisms can be implemented at higher system levels (for example through RADIUS or PKI).
	<ul style="list-style-type: none"> • Audit Controls 	Every Cisco wireless AP provides logging, including hardware address as well as user names.
	<ul style="list-style-type: none"> • Authorization Control • Role-based • User-based 	Cisco wireless solutions are interoperable with higher level authorization control mechanisms including RADIUS, TACACS+, and PKI to provide role and user-based authorization controls.
	<ul style="list-style-type: none"> • Data Authentication/ Integrity 	Cisco wireless solutions support TKIP which strengthens WEP keys through such mechanisms as key hashing (or per-packet keying) and message integrity check, thereby ensuring the privacy of transmitted data.
	<ul style="list-style-type: none"> • Entity Authentication • Unique User ID • Automatic Logoff • Password • PIN • Token • Automatic callback • Biometric 	Use of 802.1X authentication types such as EAP-Cisco Wireless and PEAP within Cisco wireless products provides for entity authentication leveraging an existing user database. Several of the listed entity authentication models may be employed through the use of these higher level systems.

Table 1 (Continued)

HIPAA Security Standard	Requirements	Cisco Wireless Solutions
Technical Security Mechanisms	• Integrity Controls	Capabilities through TKIP, which includes key hashing and MIC.
	• Message Authentication	Capabilities through MIC.
	• Access Controls	Capabilities through 802.1X authentication types such as EAP-Cisco Wireless and PEAP, plus optional MAC filtering.
	• Alarm	Compatible with Cisco Secure NIDS and HIDS.
	• Audit Trail	Capabilities through wireless AP logging, syslog, Cisco Secure NIDS and HIDS compatibilities.
	• Entity Authentication	Interacts with a RADIUS server to leverage existing user database for authentication.
	• Event Reporting	Capabilities through wireless AP logging, syslog, Cisco Secure NIDS and HIDS compatibilities.
	• Encryption	Supports dynamic, per-user encryption keys, including WEP keys and TKIP keys; also supports 3DES encryption between an IPSec (VPN) client and a VPN concentrator.
Electronic Signatures		While not required for health transactions, Cisco wireless solutions interoperate with other systems including PKI to provide electronic signature services and capabilities.

References

United States Department of Health and Human Services, *Notice of Proposed Rule Making for the Security and Electronic Signature Standards*, <http://aspe.hhs.gov/admsimp/nprm/seclist.htm>, November 1999.

Nikita Borisov, Ian Goldberg, and David Wagner, *Intercepting Mobile Communications: The Insecurity of 802.11*,



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

THE INFORMATION HEREIN IS PROVIDED ON AN "AS IS" BASIS, WITHOUT ANY WARRANTIES OR REPRESENTATIONS, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)