**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 Europe
11 Rue Camille Desmoulins
92782 Issy-Les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

**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: +65 317 7777
Fax: +65 317 7799

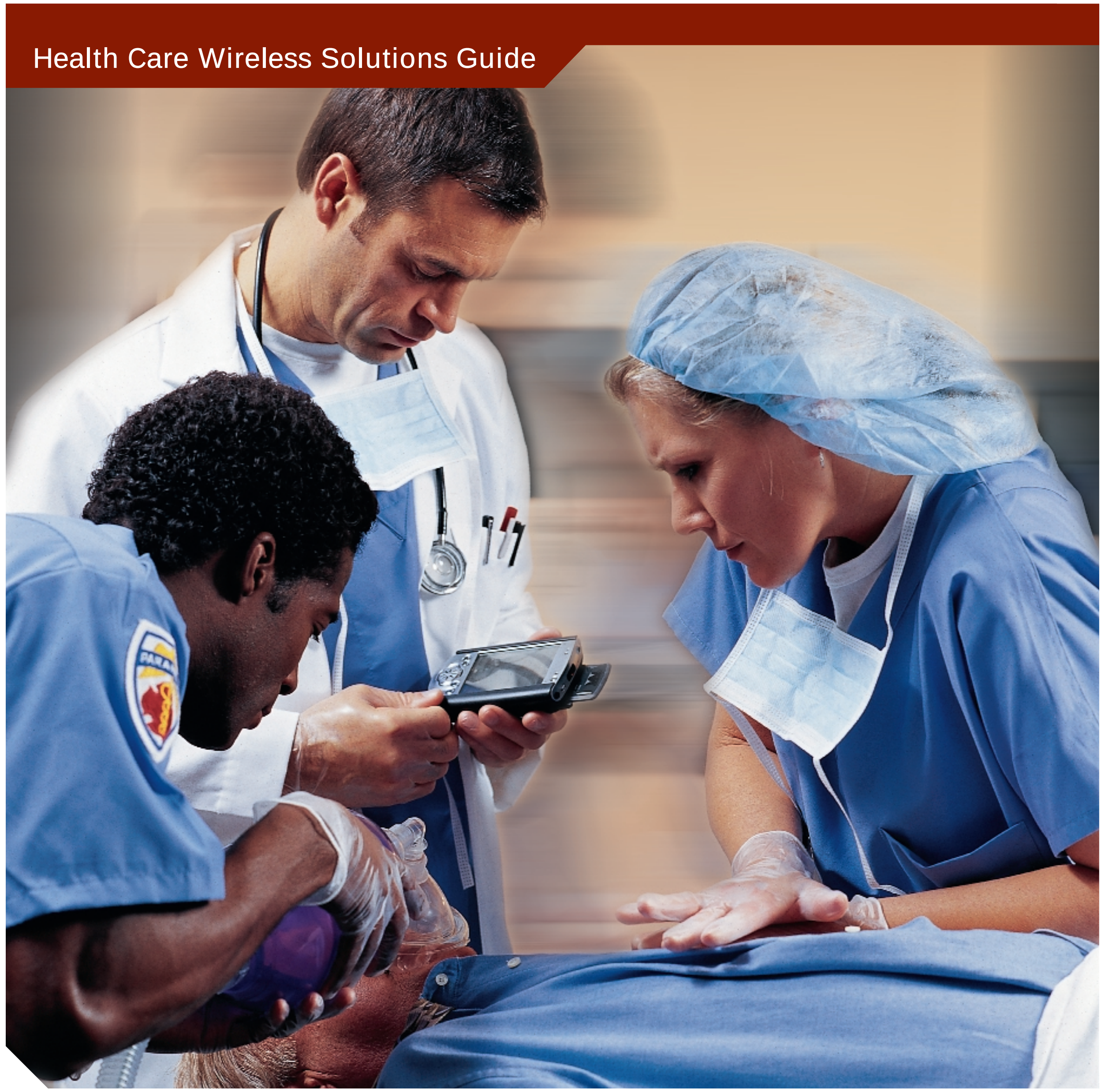
**Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.**

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

Printed in the USA

AIR01-707/AP/GLL/05-02
Lit # 956184

# Health Care Wireless Solutions Guide



Emergencies happen
in real time. Shouldn't your
information system work the same way?

TABLE OF CONTENTS

The Siemens Medical Solutions Health Services/Cisco Partnership

Best Practices

Case Studies

# Why Wireless LANs are being adopted in health-care systems globally.

Reduced reimbursement, capitation, government regulations, and staffing shortages are forcing health-care systems to search for new ways to increase efficiency, improve accuracy, increase revenue, and lower costs—all while maintaining quality care.

As a result, health-care systems around the world are exploiting the mobility, flexibility, and speed of Wireless LAN (WLAN) technologies to access real-time patient information or research for decision support *at the point of care*. This setup allows caregivers to make decisions and act with greater accuracy, speed, and efficiency.

Cisco Systems and its business partners are offering integrated WLAN-based solutions to support health-care systems with clinical and administrative applications that increase the competitiveness of their organizations by enhancing patient care at reduced cost.

Key WLAN-based health-care solutions that are being deployed include patient-facing applications such as:

- Electronic medical record access/review
- Physician order entry and medication matching
- Claims processing and charge capture
- Nurse call systems
- Patient bedside care
- Vital statistics monitoring

Inside, you'll learn about the benefits you'll derive from enabling wireless solutions at the point of care. You'll also learn of the challenges associated with operating radio frequency wireless devices in a medical environment and how proper network design can help mitigate those risks. And you'll find case studies of several health-care institutions that currently employ wireless LANs.

## Siemens Medical Solutions Health Services Relies on Cisco for Wireless

With over 5000 hospital customers worldwide, Siemens Medical Solutions Health Services Corporation (Siemens Health Services) is one of the largest providers of information systems to the health-care market. Siemens Health Services' strategic partnership with Cisco helps provide the network hardware and software it takes to operate Siemens Health Services' Health Information Network.

This state-of-the-art network connects over 1000 health-care institutions to Siemens Health Services' Information Services Center, which processes over 107 million health-care transactions each day. And it does so with an average network availability of 99.998 percent. That would not be possible without Cisco.

It's estimated that for every hour of care given, another hour of documentation is required. If documentation can be added in real time at the point of care, which is possible using Cisco Aironet 350 Series WLAN solutions, the customer's personnel can be more productive and the quality of care more effective.

Siemens Health Services has found that one of the biggest challenges its customers face is shortages—shortages of skilled medical personnel, shortages of qualified IT personnel, and shortages of funds to provide those personnel with adequate equipment to do their jobs. With the help of Cisco, Siemens Health Services addresses these shortages by giving its customers reliable information systems that work as efficiently and as effectively as possible.

Siemens Health Services uses Cisco technology to support not only its current applications, but also emerging solutions, such as the company's Soarian™ solution. This advanced Web-based solution delivers integrated clinical, financial, and administrative information directly to the acute-care institution, to the physician's office, or across the entire continuum of care using Cisco technology.

Cisco and Siemens Health Services work together successfully because the two companies share like philosophies—to provide solutions that meet the needs of customers. A solution that combines the strengths of two major corporations is extremely valuable in the health-care marketplace, where issues such as availability, reliability, performance, and security are paramount to the end users.

## The Cisco Aironet 350 Series—Advanced Wireless Solutions for Health Care

Advancements in medical technology have made it possible to enhance the quality of patient care at reduced cost while complying with federal mandates for security and confidentiality of patient data. The innovations that have given patients a better chance of recovery have been as simple as a new procedure or as complex as the new breed of medical imaging equipment. Among those innovations is one that eliminates preventable medical errors; improves daily workflow; and allows caregivers to collect more detailed, accurate information for demonstrating outcomes. That innovation is the wireless LAN-based mobile solution.

Cisco Aironet® 350 Series WLAN products add value that network components have not previously provided. Health systems using wireless report a 47 percent increase in the accuracy of patient information (source: *NOP World*, November 2001). By helping maintain accurate, up-to-date patient records, the Cisco Aironet 350 Series can lower costs and minimize costly malpractice litigation. Additionally, the Cisco Aironet 350 Series gives clinical staff a level of mobility that current wired networks fail to provide. Moreover, the ability of caregivers to get real-time, point-of-care charts, records, and test results greatly improves patient care.

Because the Cisco Aironet 350 Series is both flexible and scalable, a health-care system can take a modular approach to deployment rather than committing to location-wide coverage immediately. For instance, deployment can be made in areas requiring immediate network connectivity, such as emergency departments, and coverage for additional areas can be added later. All Cisco wireless solutions seamlessly integrate with existing networks, so your network can grow as your practice or health system grows, staying up to date and up and running. Moreover, wireless technology enables network connectivity for older buildings where installing a traditional wired network is either impossible or prohibitively expensive.

Installing the Cisco Aironet 350 Series enables your practice to improve patient outcomes, improve clinical workflow, and maintain compliance with health-care legislation.

Able to withstand extended operating-temperature ranges, plenum-ratable Cisco access points are the center points in an all-wireless network or the connection points between a wired and wireless network.

Cisco access points can be placed throughout a building or the entire health campus and provide users equipped with client adapters the ability to move freely about covered areas, while maintaining fully secure, uninterrupted access to all network resources.

Cisco wireless bridges can also be added to create wireless links between buildings in point-to-point and multi-point configurations, extending up to 25 miles in range and eliminating leased line costs.

## A Wireless System that Offers Great Return on Investment

Measuring business value in IT investments is often difficult, but the Cisco Aironet 350 Series was designed with immediate business value in mind. As an extension of existing enterprise-wide information systems, WLAN-based mobile computing technology increases the reach of current IT investments and health-care information systems by bringing decision support data to the point of activity throughout the care continuum. Advanced in-building wireless systems can integrate with existing nurse call systems and can double as alphanumeric pagers. Alternatives to traditional communication devices also exist through Voice over IP (VoIP), enabling voice and data to operate on the same network and offering two-way voice communication that allows staff to accept patient calls on handheld devices, speak to the patient directly, and immediately assess patient needs from any location in the system. Wireless LANs bring the network to your staff, saving time and reducing expenses.

Wireless costs less than traditional wired LANs. Hospitals attribute to wireless networks average annual savings of nearly $120,000 (source: *NOP World*, November 2001). The savings are made possible by eliminating the cost of room reconfiguration, building changes, and other hurdles that IT departments encounter every day. As network needs change, simply bringing another workstation into the room and installing a Cisco Aironet 350 Series client card is all it takes to increase the size of the network—no costly wire drops. With the ever-changing face of health care, it makes more sense to employ the flexibility that a wireless system provides than to install individual ports.

## Best Practices: Cisco Aironet and Siemens Health Services Help You Comply with HIPAA

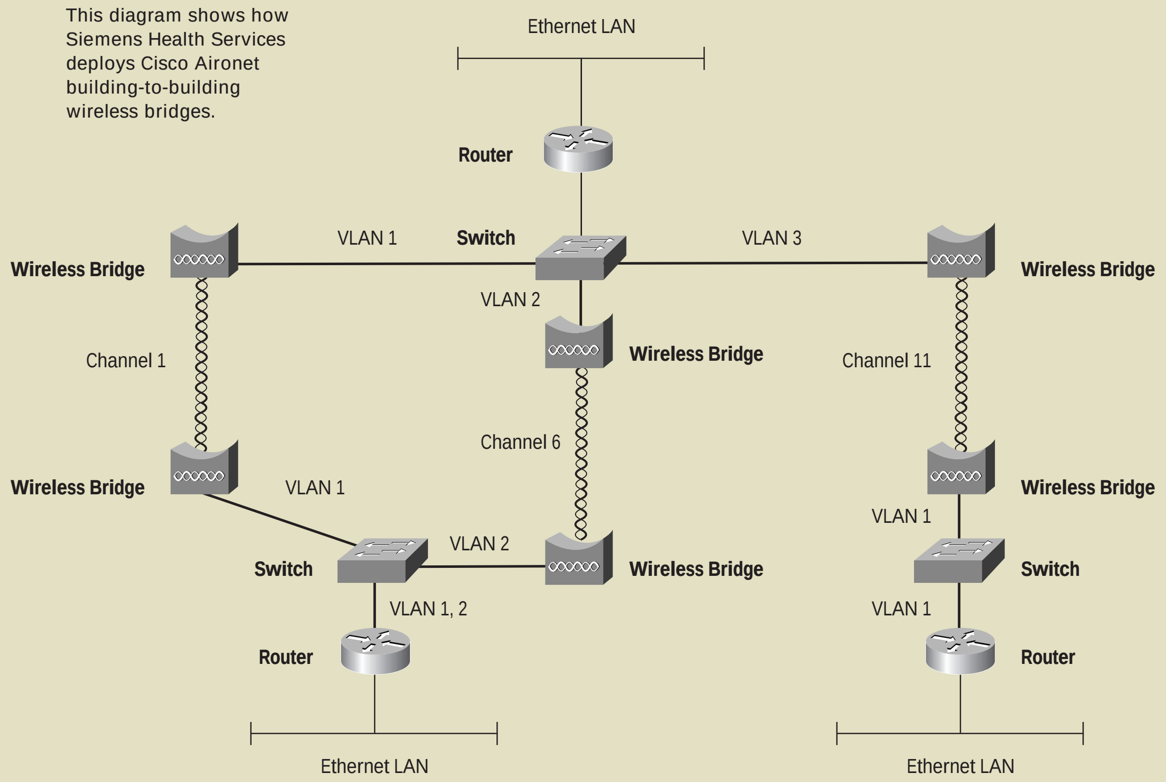
In July 1996, President Clinton signed the Health Insurance Portability and Accountability Act into law. One of the most important objectives of HIPAA was to protect patients' health information against unauthorized access.

Failure to secure identifiable health information on the WLAN can have costly consequences. Organizations can be penalized both for failure to adhere to HIPAA standards and for wrongful disclosure of health information. *HIPAA violations and abuse of patient information can result in severe penalties or even imprisonment.*

HIPAA should not only be considered but also strictly followed when working to deploy a wireless network on which patient information can be accessed. Two things must be accounted for: patients, caregivers, and insurance companies must be confident that "identifiable health information" is protected from outside interests, and there must be reliable and appropriate access to health information stored in information systems.

*continued on page 4*

## Building-to-Building Wireless Design


This diagram shows how Siemens Health Services deploys Cisco Aironet building-to-building wireless bridges.

## Best Practices: HIPAA, continued

### Ensuring the Protection of Patient Information

To ensure that identifiable health information is protected, security, privacy, and confidentiality measures must be in place.

*Security* relates to the safeguards that protect the management of such information and ensure appropriate access to it. Combining the use of the Cisco Aironet 350 Series with Virtual Private Networking (VPN) is the best way to ensure that hackers cannot access patient information.

*Privacy* pertains to the rights of individuals to understand how their identifiable health information is secured and how that information is shared with others. The wireless policies and procedures must be reviewed and approved by the health system's chief security officer, not the IS or networking manager.

*Confidentiality* ties security and privacy together to ensure that the security measures that have been established do indeed protect privacy as it has been defined. Therefore, the health-care organization must decide who has access to the WLAN, from what device(s), and what information can be obtained via the WLAN. These decisions will form the core of your organization's security program.

### Things to Remember about Wireless Networking and HIPAA

Some guidelines should be followed when considering an upgrade to a WLAN system. First, you should operate under the assumption that a WLAN "out of the box" is as unsecured as the public Internet. You will need to take advantage of the Cisco enhanced security solution to fully realize the security features available to you with the Cisco Aironet 350 Series. Also, conducting a site survey is necessary to ensure that the WLAN does not "leak" out of your intended coverage area, either inside or outside the building.

All wireless devices should be authenticated before being assigned an IP address on the network. The mutual authentication required by the Cisco Aironet 350 Series ensures that no rogue client adapters are being used. Only legitimate devices can connect to the network. VPN logs should be reviewed to make sure that no unauthorized access is being granted through the wireless system.

In cases where VPN is not utilized, all health information should be encrypted across the wireless link. This keeps patient records private—the key component of HIPAA compliance.

*continued on page 7*

According to the *NOP World* study, employees in health-care settings report average time savings of 1.16 hours a day when using WLANs rather than traditional wired LANs. Given the staffing shortages in health-care settings, this can add up to significant productivity gains. Based on an average annual salary of $64,000, these gains translate into cost savings of as much as $9000 per user each year.

Installing a Cisco wireless LAN system can help save money in other significant ways. The Cisco Aironet 350 Series makes it possible to capture and easily code physicians' activities. Therefore, patient records are more accurate and up to date, so drug interactions can be checked prior to prescribing, improving compliance and medication utilization as well. All of which helps reduce clinical and administrative costs, along with medical errors and associated legal fees and malpractice insurance.

Using the Cisco Aironet 350 Series as the keystone in a wireless network gives medical staff real-time, point-of-care access to medical records, test results, and even research. Such a system would make it possible for you to improve the care patients receive on every floor, ward, and wing.

If your health system includes buildings that are not on the main campus, such as emergency medical centers, you can seamlessly connect them to the network using Cisco Aironet 350 Series wireless bridges. They provide high-speed, long-range building-to-building wireless connections between Ethernet networks, saving the enormous time and cost of installing dedicated lines or renting telecom lines.

A WLAN system that provides return on investment (ROI) must provide radio frequency sensitivity, security, disaster recovery functions, and scalability. The Cisco Aironet 350 Series is fourth-generation technology that has been thoroughly field tested and proven, making it a better and safer investment than wireless products that are still first or second generation. Cisco is a name you can trust, ensuring operational support, maintenance, and system performance metrics that meet the needs of your health-care system. And Cisco wireless systems are used globally, from small businesses to the enterprise level.

### Cisco Aironet Gives Siemens Health Services Customers the Benefits They Need

Siemens Medical Solutions Health Services Corporation provides an end-to-end solution by bringing applications and networks together. Part of that solution is providing the Cisco Aironet 350 Series with the Cisco Wireless Security Suite for enhanced security. Combined with VPN solutions, there is no better way to go wireless while remaining HIPAA compliant.

HIPAA compliance was an important factor in Siemens Health Services' decision to use and recommend the Cisco Aironet solution. Single-user, single-session, 128-bit dynamic WEP keys and mutual authentication are utilized to ensure that anyone who is on the network belongs on the network. This login-based security architecture requires both wireless devices and users to be authenticated before any information can be transferred over a secure VPN. This scenario keeps patient information private, the key to HIPAA compliance.

When authentication is successfully completed, the Cisco Aironet 350 Series enables Siemens Health Services customers to deliver state-of-the-art applications to their caregivers at the point of care. This is done by using Cisco Aironet solutions installed in wireless devices, whether they are wireless-based laptops being rolled around on carts, wireless tablets such as the Siemens SIMpad, or handheld PC devices. The wireless devices communicate with the network via Cisco Aironet 350 Series access points installed throughout the facility. Physicians can carry wireless devices on their rounds, enabling them to check results, view patient histories, and even prescribe medication without ever leaving the bedside.

Siemens Health Services selected Cisco and Cisco Aironet access points not just because it is a Cisco Powered Network provider and Cisco Gold Certified Partner. "That doesn't automatically mean that Cisco gets our business," says Michael Alban, a strategic alliance manager for Siemens Health Services. "We scout the industry and make sure that we're offering products that best meet our customers' needs and expectations."

Siemens Health Services has shown that it truly trusts and relies on Cisco Aironet products. The company has deployed Cisco VPN and the Cisco Aironet 350 Series solutions internally as well as for its customers. "We're using it to enhance employee productivity, whereby employees can get up and move around," Alban says. "They're mobile. They can collaborate with each other by taking their laptop or PDA with them and not having to worry about where the network is."

Alban continues, "Another way I like to look at it is that employees do not have to seek out the network; now the network is wherever they are within the campus."

### The Cisco Aironet 350 Series Works for Siemens Health Services

Siemens Medical Solutions Health Services Corporation recognizes the need in health care for accurate information 24 hours a day, 7 days a week—because patients don't choose to have emergencies during regular business hours. Siemens Health Services realized that Cisco was the clear choice when it comes to delivering reliable networking products that are always on call.

Much of the information that is passed from the bedside to Siemens Health Services' Information Services Center and back is critical to providing the patient with quality care. Thus, it has to be successfully transmitted around the clock. That's why Siemens Health Services relies on the Cisco Aironet 350 Series to accurately deliver that information whenever and wherever it's needed.

But round-the-clock information exchange is only part of what hospitals need in an information system. Russ Miller, Siemens Health Services' vice president of network services, says, "Siemens Health Services found that the Cisco Aironet product works right out of the box and is very easy to use. It is so key with everything that's going on to find partners that will provide us products that are well documented, easy to use, easily implemented, and that work the way that they're advertised."

Before installing any Cisco Aironet system, Siemens Health Services conducts a site survey to avoid interference with medical and other devices. Miller explains, "With a site survey, we can meet all the requirements of a hospital environment so that interference does not occur, still have full deployment and full coverage within a hospital, and meet all the hospital's availability needs."

Providing network solutions to the health-care market is challenging. Regulations change, needs change, even the type and amount of information necessary change. But in every case, one thing remains—the goal of improved quality of care. Cisco Aironet 350 Series solutions enable health-care institutions to provide excellent care while maintaining the security that patients and HIPAA need.

Siemens Health Services found that Cisco Aironet 350 Series solutions are easy to install, save costs by providing excellent ROI, perform as promised, and provide enhanced security in an end-to-end solution. This partnership between Cisco Systems and Siemens Health Services ensures that these industry leaders together will be providing the highest-quality information technology to hospital customers for a long time to come.

### Enhanced Security for HIPAA Compliance

The Cisco Aironet 350 Series has best-in-class security for compliance with the Health Insurance Portability and Accountability Act (HIPAA). It's the first product line to use a standards-based security measure for hassle-free administration that still manages to mitigate known security attacks against the standard wireless security protocol, Wired Equivalent Privacy (WEP). It has a user-based privacy mechanism that can scale to thousands of users. The IEEE 802.1x-based Extensible Authentication Protocol (EAP) solution provides scalable, centralized security management and supports dynamic single-session, single-user encryption keys integrated with network logon. Because it's a standards-based security mechanism, it supports a variety of authentication types, including digital certificates, biometrics, and two- and three-factor authentication services.

User access to the wired network is completely blocked until the successful completion of mutual authentication between the client device and the authentication server, such as a Remote Access Dial-In User Service (RADIUS) server. At this point, the client and the authentication server determine a WEP key, which is distinct to the client and provides the appropriate level of network access. This gives the client on a wireless network the same level of security as the user on a wired connection. Users can employ 128-bit strong encryption to ensure that proprietary information does not get into unauthorized hands. Additionally, the user's key can be changed as frequently as the IT staff deems necessary to prevent the compromise of security, with little performance overhead and complete transparency to the user. And finally, security mechanisms exist to detect attempts to tamper with transmissions through a message integrity check, in concert with comprehensive auditing of user access to the network.

The Cisco security solution was created with HIPAA compliance in mind. Information is secured so patients, physicians, and insurance providers can take advantage of the many benefits of electronic patient medical records and health-care point-of-care applications without jeopardizing the security and privacy of that data.

### Mobility that Brings Information to the Point of Care

What good is freedom of use without freedom of movement? That's why the Cisco Aironet 350 Series allows users to roam from access point to access point without interruption in connection and workflow. That means freedom to move around the wireless covered area without worrying about having to log back on to the network. Users can attend staff meetings and complete rounds with tablets, Personal Digital Assistants (PDAs), or even laptops on carts, remaining connected all the while. And users never have to worry about finding a connection to the wired network. The Cisco Aironet 350 Series wireless infrastructure allows users to do their work just about anywhere. A recent study by the Federation of Nurses and Health Professionals revealed that the shortage of nurses has finally reached a crisis point; 20 percent now plan to leave the field within five years, primarily citing "unsatisfactory work conditions" (source: *Health Management Technology,* "Talk Before You Walk," January 2002). Alleviating their workload with tools such as advanced wireless integrated systems may lead to a more satisfied workforce.

In addition to enhancing patient care, the mobility provided by the Cisco Aironet 350 Series system will help your staff work more efficiently. In fact, a recent study showed an average increase in productivity of 22 percent (source: *NOP World,* September 2001).

### Protecting Wireless Devices Protects Patients

Because wireless devices are portable by their very nature, they are susceptible to theft. Thus, precautions should be taken to ensure that patient information remains private. Users must understand both their obligations to protect the information stored on the devices and what the devices are capable of accessing. Also, personnel with such devices must agree to comply with the organization's wireless policies and procedures. Most important, all patient information stored on these devices should be encrypted and the devices themselves should be password protected.

Installing a Cisco Aironet 350 Series WLAN and following the suggestions here can get you on the right track to establishing an effective and efficient wireless network while remaining HIPAA compliant. For more information about how the Cisco Aironet solution can help you remain HIPAA compliant, contact your Cisco representative or sales partner.

## Best Practices: Addressing Radio Interference

Before installing any wireless system in a health-care environment, Cisco Systems and Siemens Health Services recommend that several issues be taken into consideration. Because wireless networking systems emit and receive radio frequencies in the 2.4-GHz range, some interference with monitoring and lifesaving devices may occur if the network is not properly designed. A site survey should be conducted before beginning the installation, along with a non-mission-critical test of all components in the system, to minimize the possibility of harmful radio interference in your network. Some interference can be avoided simply by locating the access point just a few feet from where it was originally planned. Consult your Cisco representative for more information regarding site surveys and properly designed networks.

Cisco recommends that you have your wireless network designed and installed by a Cisco trained professional installer. This will help you avoid unforeseen problems. Although some interference is relatively benign, causing no serious effects or producing only low-grade interference, such as snow on a monitor, more severe interference can cause a device to produce erroneous readings, reset, or jam its communications. In a medical environment, where mission-critical decisions are being made all the time, avoiding such problems is worth the cost of hiring a professional installer whose products, services, and expertise can help you throughout the process.

## Surveying for Sources of Radio Interference

The first step in preparing to launch the Cisco Aironet 350 Series at your facility is to determine whether there is any potential interference with medical equipment. Some medical devices are not properly hardened for certain radio frequency levels and frequencies common to wireless networking. This is particularly true of older devices that were manufactured prior to the adoption of certain certifications and standards. These determinations can be made by checking the standards and certification labels carried by the equipment and by designing around the associated limitations.

You should involve the health system's biomedical engineering department when testing the WLAN in a controlled environment with other sources of electromagnetic interference. It is the responsibility of this department to test devices and to define the policies and procedures relating to these devices and their usage. Most biomedical engineering departments have a standard test set that is based on known industry issues and the electromagnetic devices that the health system has already installed. Knowing the location of these other devices is extremely important, because proximity to such devices must be considered during the site survey.

*continued on page 10*

## The Flexibility to Grow Your Network at Your Own Pace

The Cisco Aironet 350 Series of equipment offers great flexibility and scalability—critical characteristics when budgets must be considered. Because individual units in the system can be used alone or in tandem with others, you can install wireless in a single room. As network use increases, you can grow the system to cover a ward, a wing, or even whole buildings. And with wireless, it's possible to extend your network across every square foot of the medical campus.

Deploying wireless in a single defined public space and expanding from there is not unusual, because the Cisco Aironet 350 Series easily integrates with your existing network. Although seamless coverage throughout the health-care facility can be maintained through location-wide deployment, many facilities start by installing the Cisco Aironet 350 Series in the trauma center or emergency room, places where immediate response and instantaneous information are crucial. Most institutions that start with small or limited deployments are able to quickly increase the size of their wireless networks because of their ease of use, ease of installation, and ease of maintenance.

## Speed and High Availability for Reliable Mission-Critical Care

The Cisco Aironet 350 Series supports an Ethernet-like data rate of 11 Mbps and delivers industry-leading performance. The throughput of Cisco IEEE 802.11b products is up to 20 percent faster than that of similar products—a difference that can be critical in life-and-death situations.

High availability through hot standby and fault tolerance means that the system is always ready and always available. When redundant access points are used, the system remains covered in the unlikely event that one access point fails.

Beyond automatic failover, there are other advantages to having multiple access points in a single location. If greater speed is needed in a certain area, that area can be serviced by up to three access points, enabling an aggregate data rate of up to 33 Mbps. This load-balancing technology increases the flexibility as well as the speed. More users can enjoy faster data rates wherever additional access points are used.

## Enterprise Wireless Design

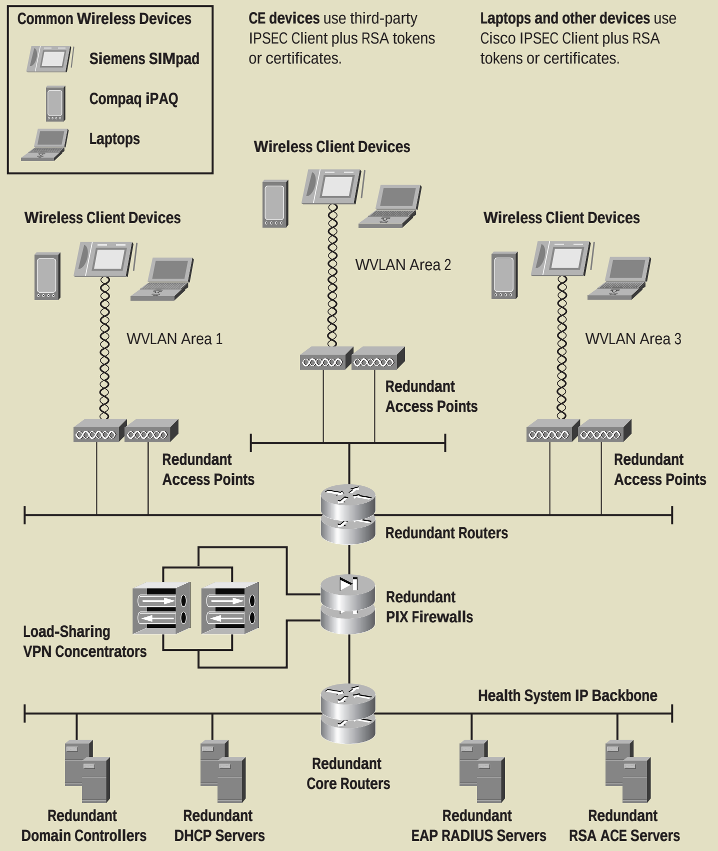
This diagram is an example of how Siemens Health Services utilizes Cisco Aironet wireless LAN solutions in an enterprise setting.

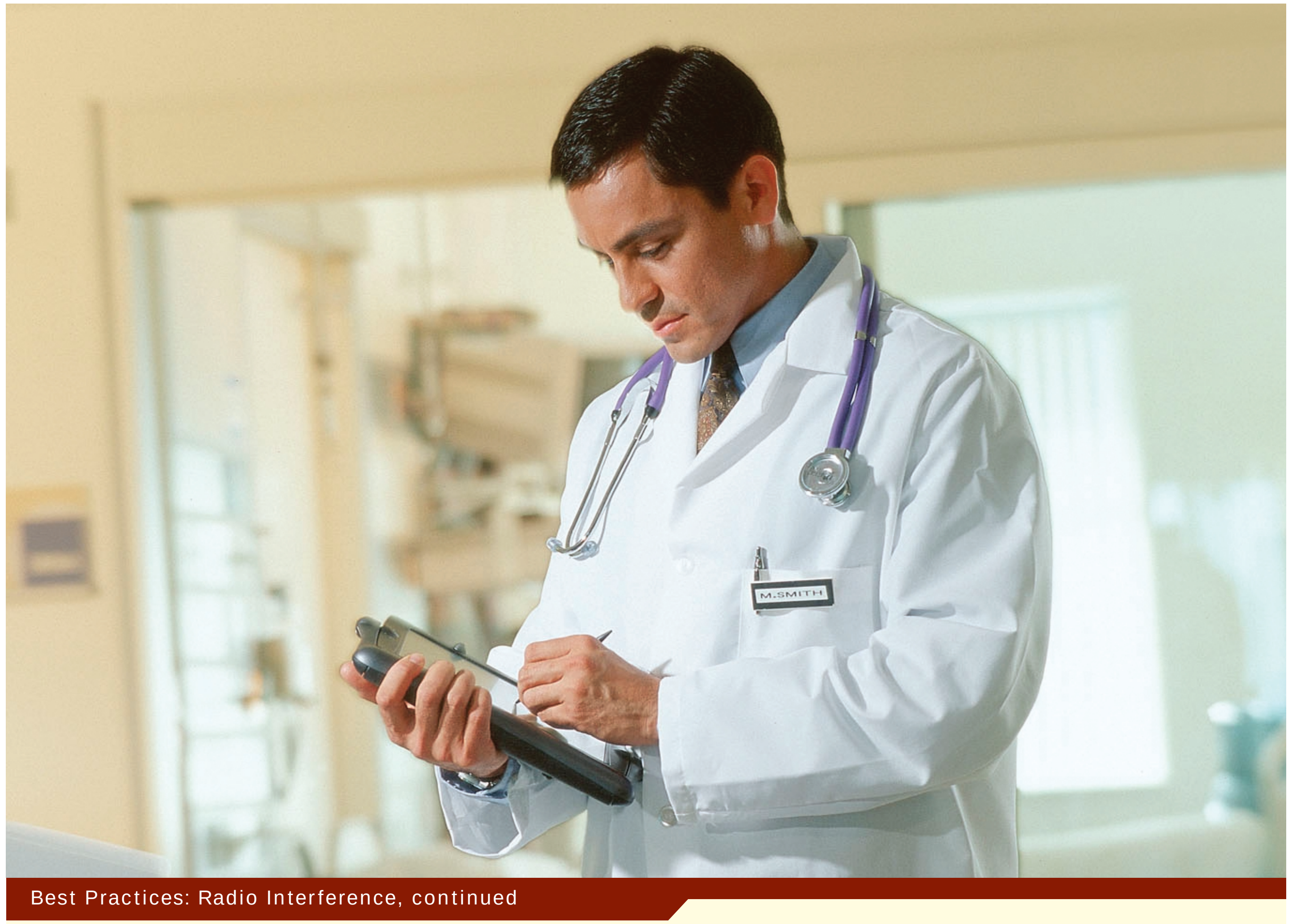
### Enhanced Security Features

- Centralized, scalable, user-based authentication.
- Mutual authentication of client devices and RADIUS server to protect against rogue access points.
- Supports various authentication types.
- Dynamic WEP key support.
- User-configurable WEP key refresh timeouts to match key-rotation times with security risk data loads of network.

### Wireless Security in a Nutshell

- User associates with access point. Access point prevents network access.
- Encrypted credentials are sent to authentication server.
- Authentication server validates user, grants access rights.
- Access point port is enabled and dynamic WEP keys are assigned to client (encrypted).
- Wireless client can now access general network services securely.





### Checking Equipment for Medical Electromagnetic Compatibility Standards

As another part of the preparation process, you should check to see if the medical equipment needs to meet the Electromagnetic Compatibility (EMC) and safety requirements of medical devices used to provide direct patient care or peripheral support. Electromagnetic compatibility means that any equipment used in proximity to such devices should not cause harmful interference, but must be able to accept harmful interference, including that which disrupts service. To adhere to EMC standards, Cisco Aironet 350 Series components operate on a noninterference basis.

Some of those devices the Cisco Aironet 350 Series is designed not to interfere with are other wireless services (telemetry patient-monitoring services); nonwireless, non-mission-critical medical devices and other digital devices; and nonwireless, mission-critical medical devices (heart monitors, defibrillators). An EMC-compliant device must also be able to accept harmful radio emissions from other devices, even if that means interruption in service.

A device must also be compliant with IEC 601-1-2 standards, established by the International Electrotechnical Commission to determine acceptable levels of emissions. Compliance requires that the device be tested to the emission requirements as delineated in CISPR 11. There are two levels of compliance for CISPR 11: Class A and Class B emissions. In compliance with the requirements of IEC 601-1-2, if the digital device has been tested to the requirements of CISPR 22, then the product does not need to be tested to CISPR 11.

The emission levels set forth in CISPR 11 address only the unintentional spurious emissions from the device and do not cover any of the transmitter emission parameters. Compliance with the transmitter parameters would be to the appropriate radio standard.

It should be noted that a piece of medical equipment that has been tested and certified to IEC 601-1-2 standards is still subject to interference. However, despite the fact that Cisco Aironet 350 Series components are transmitters, they will not necessarily cause interference. In fact, in some cases, medical equipment is more likely to be affected by nearby computers or other digital devices than by the Cisco Aironet 350 Series access points.

continued on page 11

### Ensuring Equipment Meets International Certifications

Prior to being placed on the market, the components of the Cisco Aironet 350 Series were thoroughly tested and certified for international regulatory standards for 802.11a, 802.11b, and HyperLAN devices and are labeled accordingly. Some installations may require further tests based on emission and immunity requirements specific to that environment.

*Note:* 802.11a, 802.11b, and HyperLAN are *not* regulatory standards. Compliance to 802.11 and HyperLAN is not mandatory for products to be placed on markets, nor is it a requirement for certification, so conducting additional certification checks is imperative.

The following table shows the international regulatory standards that 802.11a, 802.11b, and HyperLAN devices, including the Cisco Aironet 350 Series, must adhere to.

### Regulatory Standards

| Country | WLAN | UNII |
|---|---|---|
| Australia | AS/NZS 4771 | AS/NZS 4771 |
| Canada | RSS-210 | RSS-210 |
| European Union | EN 301.328 | EN 301.893 |
| Japan | Std 33A & Std 66 | |
| New Zealand | AS/NZS 4771 | AS/NZS 4771 |
| United States | FCC Part 15.247 | FCC Part 15.401 |

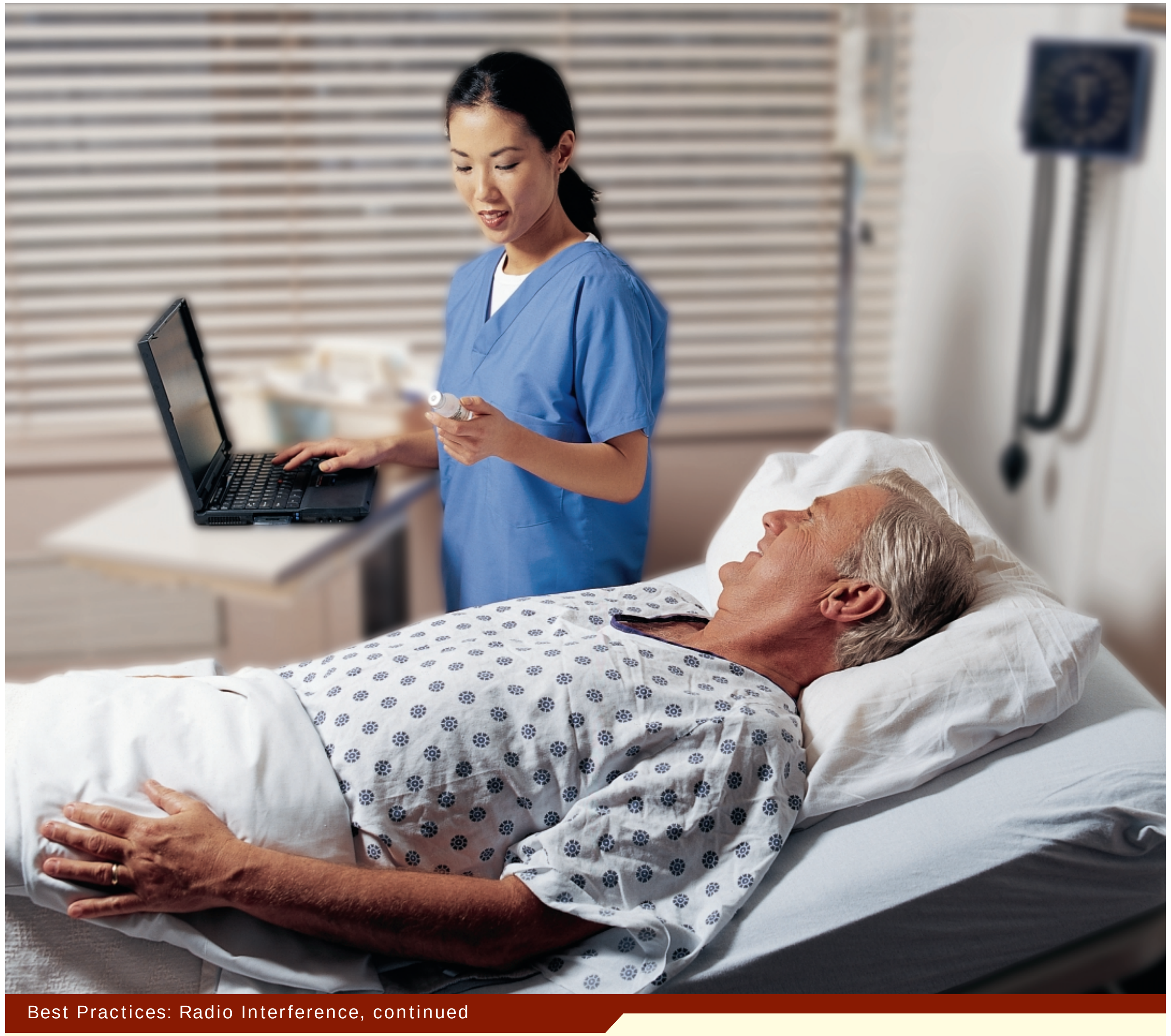
continued on page 12

### Seamless Integration with Both Legacy and Future Equipment

Cisco was careful to ensure that the Cisco Aironet 350 Series easily integrates with legacy networks. The IEEE 802.11b standard for wireless technology, which Cisco helped develop and the Cisco Aironet 350 Series adheres to, also simplifies the implementation process for network administrative and technical support staff by ensuring interoperability with other IEEE-based wireless products. Cisco Aironet products are also Wi-Fi certified for interoperability with other Wi-Fi (IEEE 802.11b) products by the Wireless Ethernet Compatibility Alliance (WECA).

Because it’s standards based, the Cisco Aironet 350 Series connects to the wired networks of any vendor. Although there are advantages to getting your network components from one vendor, Cisco wireless components work as well in third-party network environments as they do in networks with only Cisco products.

The key to understanding how wireless components integrate into existing wired networks is to think of wireless and wired network sections as a whole, not as separate entities. This reinforces the concept that the wireless connections work and act in a manner that is consistent with wired connections. Each client on the wireless portion of the network appears on the network equivalent to one on the wired portion of the network. In fact, installing the Cisco Aironet 350 Series can actually increase the effectiveness of the whole network by providing more freedom and safety for medical staff, for administrators, and for you.



## Best Practices: Radio Interference, continued

### Handling Specific Medical Concerns

One concern that has been raised in the past is the possibility that a WLAN device may interfere with hearing aids or pacemakers. The possibility is remote, and the tests that have shown interference have been conducted with cordless and cellular phones held up to the ear, not access points, which are generally nowhere near a person's hearing aid.

Another concern that's been voiced is the possibility of interference with devices operating in the same frequencies as microwave ovens. It should be noted that most pacemakers that are subject to interference are older models, and the interference comes from systems operating in bands of 900 MHz or lower. Changes and improvements in pacemaker design have helped eliminate some of these problems.

In 1996, tests were conducted by Greater Chicago's Ingalls Memorial Hospital to verify that no problems would occur between Cisco 2.4-GHz radios and pacemakers. The summary report is available upon request from Cisco. In November 2001, the Ohio State University Medical Center tested Cisco Aironet 350 Series components in its MRI facility and found no interference to the Cisco radios or the MRI unit.

To ensure safe operation of your WLAN system, you should verify noninterference through a qualified Cisco installation specialist.

### Implementing the System in Your Facility

The Cisco Aironet 350 Series easily integrates with your existing network, makes real-time information exchange possible at the point of care, and saves money in the long run while improving the quality of care. Its mobility and flexibility make it the best solution for wireless networking needs. Moreover, it's easy to install. Call your Cisco account manager or sales partner for more information.

After being tested for product quality, ease of use, and security, the Cisco Aironet 350 Series was named a Network World® Blue Ribbon Winner in 2001.

### St. Luke's Episcopal Hospital of Houston Uses Cisco Aironet to Improve Patient Data Privacy

"Improved security was one of our primary goals," says Don McGovern, St. Luke's project manager, who uses the Cisco Aironet 350 Series to facilitate the secure downloading of data from mobile units into the hospital network. Because the Cisco Aironet 350 Series supports dynamic WEP keys, the IEEE 802.1x standards framework, EAP, and EAP authentication types such as Transport Layer Security (TLS), Message Digest Algorithm 5 (MD5), biometrics, and EAP Cisco Wireless, St. Luke's found it to be the perfect choice for a wireless system that would help the hospital achieve HIPAA compliance. "The Cisco Aironet solution offered us the level of protection that we needed to meet HIPAA standards."

### Antelope Valley Hospital Adds Wireless to Improve Efficiency of Care and Maintain HIPAA Compliance

To test the Cisco Aironet 350 Series system before full deployment, Antelope Valley conducted a pilot program in a 40-bed unit, and the program was very successful. "This pilot group presented a wrinkle in that medical charting isn't always uniform—charts might be kept at bedside on one floor and with the charge nurse on another," says Ash Shehata, director of information systems and telecommunications. Shehata says his nurses are quite pleased with the system. "Wireless has made chart-keeping more convenient. All the nurses have adopted it very well," he explains. As a result, efficiency and productivity have greatly increased.

Antelope Valley Hospital also uses its WLAN with FRED—its Friendly Robotic Electronic Druggist—which takes orders from the hospital information system via the Cisco Aironet 350 Series, fills the order, barcodes it, and seals it so that pharmacy technicians can pick it up.

Antelope maintains HIPAA compliance while improving efficiency of care. "On the wide area network, we will use EAP Cisco Wireless plus VPN and, to complement this system, we are evaluating additional security products from three third-party providers. It's the same for the local area network—we are checking into additional security products that will interoperate well with EAP Cisco Wireless," Shehata said. "We use RSA tokens as well as BioconX biometric solutions for two-factor authentication in conjunction with EAP Cisco Wireless and VPN technology to ensure that we as an organization have done our due diligence to protect our patients' data across our networks."

### Sharp HealthCare System of San Diego County Uses Wireless to Enhance Patient Care

The Cisco Aironet 350 Series helps Sharp improve the bedside experience for both the caregiver and the patient. Sharp uses its WLAN to give its caregivers access to its Electronic Medical Record system through computers mounted on rolling carts—providing point-of-care data on tests, health history, and admissions information. "The mobility that the wirelessly enabled Electronic Medical Record system provides our staff is priceless," says Mark Wiesenberg, Sharp's director of network services. "It not only makes the bedside visit more convenient and efficient for the caregiver, but it also enhances the visit from the patient's standpoint, because the clinician remains at the bedside throughout the visit."