

MEDICAL-GRADE NETWORKS—WHAT YOU NEED TO IMPLEMENT PROTECTED HEALTHCARE SOLUTIONS FOR PHYSICIAN GROUPS AND CLINICS

INTELLIGENT NETWORKS. SMART MEDICINE.

ABSTRACT

As physician groups and clinics move from paper-based to digital healthcare, protecting network-based applications and records is a top priority. A Cisco Systems® Medical-Grade Network meets the rigorous security and performance requirements of healthcare organizations. Cisco® Protected Healthcare Solutions for Physician Groups and Clinics enable practices of all sizes to reap the full benefits of modern healthcare tools. This implementation roadmap provides an overview of drivers and network security requirements for healthcare practices, including:

- An overview of the healthcare trends and challenges driving network security requirements
- Cisco network security capabilities, tools, and benefits for physician groups and clinics
- Strategic business and deployment considerations for implementing a network security solution

INTRODUCTION—HEALTHCARE TRENDS AND CHALLENGES

Healthcare organizations face mounting pressure from rising costs, staff shortages, increasing regulatory requirements, and growing expectations for the highest quality patient care. To respond to these needs, many healthcare practices are looking to transition from paper-based, manual processes to digital, automated, and networked healthcare. Electronic medical records (EMRs) and wireless networks can enhance a caregiver's ability to record and communicate information, reduce errors, and improve the quality of patient care. Network-enabled tools such as practice management solutions manage paperwork electronically, reducing costs and increasing profitability. In the past, only the largest hospitals and healthcare organizations were able to deploy these tools. But today, Cisco Medical-Grade Networks make these healthcare solutions available to even the smallest healthcare practice.

For practices to realize these benefits, however, the network must be secure. And as healthcare practices move away from paper-based systems to a network- and Internet-enabled environment, they face new security threats. With real dangers to healthcare networks such as hackers, computer viruses, disaffected employees, and even human error, a locked file cabinet or office door is no longer sufficient to protect confidential patient information. As a result of these threats—and increasing regulatory mandates—smaller practices with limited IT budgets

and expertise have been squeezed between growing needs and financial realities. These practices need network and security solutions that are powerful and affordable, and that scale to match their requirements.

Cisco network security solutions address healthcare security needs for small, midsize, and large physician practices. Cisco Protected Healthcare Solutions for Physicians Groups and Clinics range from secure wireless technologies to Internet VPNs, with capabilities for intrusion protection, access control, encryption, and other advanced security management features to protect confidential patient information. These solutions are easy to deploy and use, and have been designed specifically for smaller organizations like physician groups. This implementation roadmap provides an overview of how you can use a Cisco Medical-Grade Network, based on proven security expertise, to protect your healthcare practice and help ensure that the data traveling across your network is safe.

The Need for Network Security in Healthcare

While information security is a top priority for any organization, healthcare practices must be especially diligent about protecting confidential patient data. The drivers for implementing strong security in healthcare practices include:

- *Security and privacy requirements*—As smaller healthcare organizations digitize systems and records, they need to pay greater attention than ever before to network security. Government regulations, such as the U.S. Healthcare Insurance Portability and Accountability Act (HIPAA), mandate strict privacy measures and guidelines for securing healthcare information. Simply deploying a firewall in the network is not sufficient—you need to take a comprehensive approach to protecting patient information at every potential point of access inside and outside the medical facility. Cisco Protected Healthcare Solutions for Physician Groups and Clinics enable staff to use healthcare applications securely and to protect the confidentiality of patient data accessed via wired and wireless devices such as pocket, tablet, and touchscreen PCs.
- *Evolution of security threats*—Threats to information security grow daily. For many of today's paper-based practices, the threats range from inappropriate storage and handling to loss of patient information due to fire or floods. But as practices move toward digital records and sharing information over a network, the network must also be secure. That means deploying encryption and access-control tools to protect sensitive data from unauthorized use.

As practices begin to harness the power of the Internet, they also must take precautions to ensure that intrusions cannot disrupt the workflow of the practice. Communicating over the Internet can enable substantial efficiencies and cost savings, but only if a practice's network and servers are protected from hackers' growing arsenals of viruses, worms, and other attacks.

Practices also must guard against unintentional internal security breaches. According to a 2003 study by the U.S. Federal Bureau of Investigation (FBI), internal security breaches are the most common and can cost 10 times as much as external threats to correct.

- *Costs of poor security*—The most immediate damage that can be caused by a security breach is interrupting caregiver access to healthcare applications, impeding the ability to provide the most timely and effective care. Practices must not only ensure that applications are dependable, but that the network supporting the applications also delivers the highest level of security and reliability. The costs in legal liability for compromised patient data or fines for lack of compliance can be substantial. And, most importantly, a healthcare practice that cannot protect confidential data risks losing the confidence of its patients.

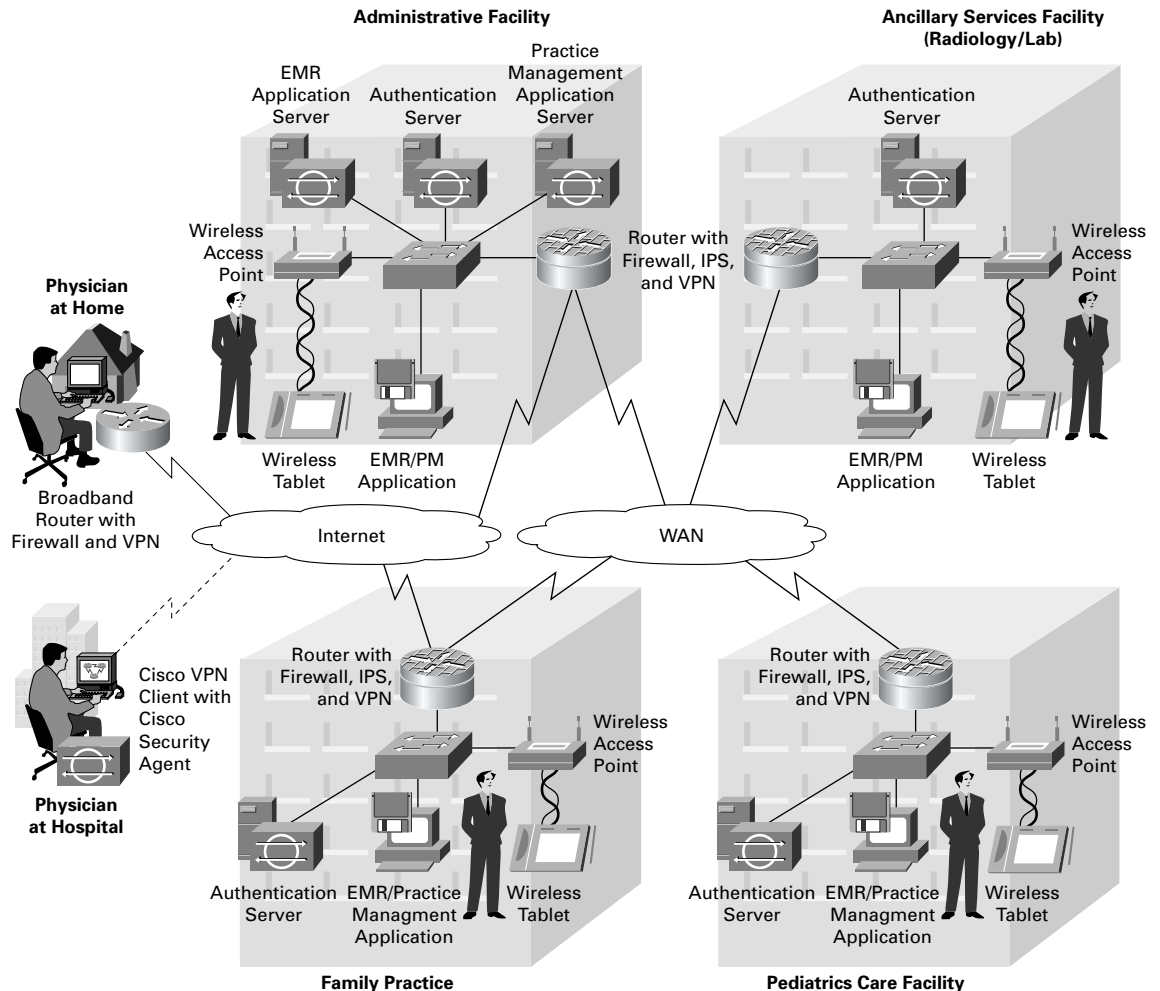
Protected Healthcare Solutions for Physician Groups and Clinics

While the threats to healthcare practices are very real, protecting against those threats is a straightforward process—even for organizations without a large IT staff. Cisco Protected Healthcare Solutions for Physician Groups and Clinics are based on the industry's most comprehensive security portfolio. These solutions meet the requirements of healthcare organizations of all sizes—from practices with one or two physicians, to large clinics with several hundred employees (Figure 1).

Cisco Protected Healthcare Solutions for Physician Groups and Clinics include:

- *Access control*—Practices need to protect patient records and networked healthcare applications. Network-based access control and identity services enable the network to identify different applications, devices, and users and to control their access to the network. These capabilities range from standard passwords to digital certificates and authentication keys, to more sophisticated capabilities. For example, using guest virtual LANs (VLANs), practices can make part of a network or the Internet available to patients and guests, while protecting confidential resources behind a secure partition.
- *Secure WLANs*—Practices are rapidly adopting wireless tools to give caregivers greater mobility and to deliver patient information at the point of care. Cisco security solutions provide strong protection for sharing sensitive information in a wireless environment. Cisco Aironet® wireless access points, for example, offer integrated access control and encryption features that supplement and strengthen network-based security services.
- *Intrusion protection*—Intrusion protection systems (IPSs) defend against worms and viruses, protecting healthcare application clients and servers, and helping to ensure network availability and performance. Cisco has teamed with industry-leading security software organizations, including Symantec, Network Associates, and Trend Micro, to bring the latest and most-effective threat protection to healthcare networks.
- *Internet security*—Firewalls and Internet security capabilities enable practices to safely use the Internet without exposing sensitive resources to potential external threats.
- *VPNs*—Secure IP VPNs enable practices to safely extend healthcare applications and information to remote facilities, hospitals, medical conferences, and even caregivers' homes. This technology protects data in an encrypted tunnel, allowing physicians to securely connect to the network over the Internet from virtually anywhere. With IP VPN encryption, healthcare information cannot be compromised, intercepted, or read by anyone other than the authorized recipient.
- *Secure core networking products*—Cisco Ethernet switches and routers support secure networking and provide a robust foundation for Cisco Protected Healthcare Solutions for Physician Groups and Clinics.
- *Network management*—Cisco security management products give practices the tools to monitor and maintain comprehensive information security. These tools offer simple yet powerful interfaces and the flexibility to manage all security and access policies across the network as a single, integrated system.

Figure 1
Network Security of Cisco Protected Healthcare Solutions for Physician Groups and Clinics



The security threats facing practices today are real, and must be addressed. Using scalable Cisco Protected Healthcare Solutions for Physician Groups and Clinics, practices of all sizes can protect confidential patient information from attacks and security threats.

BENEFITS OF CISCO PROTECTED HEALTHCARE SOLUTIONS FOR PHYSICIAN GROUPS AND CLINICS

Ensuring security and privacy of healthcare information is more than just a regulatory requirement. When practices can safely use network-based healthcare applications and access information at the point of care, the benefits are significant.

Providers implementing Cisco Protected Healthcare Solutions for Physician Groups and Clinics can deliver the best possible patient care and service, while increasing profitability and reducing costs. Secure, network-based applications can help practices lower costs per transaction, reduce staff time per claim, and reduce or eliminate lost and “undercoded” claims.

Cisco Protected Healthcare Solutions for Physician Groups and Clinics can enable:

- *Prevention of a damaging security breach*—The costs of even a single security breach can be substantial, including lost data, lost productivity, diminished patient confidence, and large fines and penalties. A strong, well-planned security solution can help healthcare practices avoid these pitfalls.
- *Access to information at the point of care*—A protected wired or wireless network allows physicians to access and update clinical records directly from an examination room or lab, providing a more up-to-date, comprehensive view of the patient where caregivers need it most.
- *Increased mobility*—Secure wireless networks and VPNs allow physicians to access patient information, lab results, and medical libraries from tablet computers, PDAs, mobile phones, and remote and home offices.
- *Enhanced productivity and reduced costs*—Once a protected, reliable network is in place, healthcare practices can deploy applications that streamline resource-intensive back-office processes. Solutions include practice management applications, claims processing systems, and systems for finance and human resources processes. These applications help increase staff productivity and reduce operating costs by automating routine tasks such as multiple form completion, patient record location, transcription, and billing.
- *Improved patient care and safety*—Digital clinical applications and real-time information sharing enabled by a protected network result in a more unified, up-to-date view of the patient and faster, more accurate care. When physicians can securely update records and write prescriptions digitally and at the point of care, they can substantially reduce the errors associated with hand-written, paper-based systems.

STRATEGIC CONSIDERATIONS FOR PHYSICIAN GROUPS AND CLINICS

The following strategic considerations are helpful in assessing your requirements for a Cisco protected healthcare solution:

- *Government regulations*—Is your current or planned healthcare system in compliance with privacy regulations? Can you protect patient data at every point within your network?
- *Level of risk*—What is an acceptable level of risk for your practice? What are the most critical applications for your caregivers, and what are the costs if those applications are disrupted?
- *Security expertise*—Do you have the internal expertise to effectively protect your network and confidential patient information? Would you benefit from working with a technology partner that has extensive experience deploying healthcare security systems?
- *Adoption of new technologies*—Do you plan to deploy new tools such as wireless or EMR applications? Do you have an integrated solution for both wired and wireless network-based applications? Do you have a security plan to address the new points of network access that those tools create?
- *Access to clinical systems*—How many people will have access to confidential patient information? Do you have tools in place to monitor and restrict access throughout your organization?
- *Using the Internet*—Are you using or planning to use electronic claims submission, e-prescription, and other healthcare applications that connect with external labs and clinics over the Internet? Do you have systems in place to protect against viruses, worms, and other widespread Internet threats?

DEPLOYMENT CONSIDERATIONS AND QUESTIONS

While large practices may have an experienced IT staff to manage deployment, smaller practices should strongly consider working with a technology partner. Cisco certified resellers and partners have a wealth of experience, both with Cisco network security technologies and the threats facing healthcare networks. These partners can manage all aspects of planning and with deploying Cisco Protected Healthcare Solutions for Physician Groups and Clinics, allowing practices to focus on medicine.

Practices should consider the following four areas before deploying a network security solution:

- *Strategy*—Understand your network security needs and objectives, and make sure you have the support of senior clinical and administrative staff. Work with an experienced security partner to identify your most critical applications, the most likely threats to your network, and your acceptable level of risk.
- *Process*—Work with a security partner to clearly define the methods for implementing a network security solution. What security solutions does your practice currently have in place? What are your organizational security policies? Will policy changes be required?
- *People*—Training, organizational culture, and organizational structure must support your security strategy and goals. Does your IT staff have the skills, equipment, and access to support the security solution on an ongoing basis? Will you need to outsource service and support?
- *Technology*—Reliable, scalable, and manageable computer networks, applications, and tools are essential to an effective security implementation, as is interoperability with your existing IT environment. Will you need to upgrade your network to help ensure effective security?

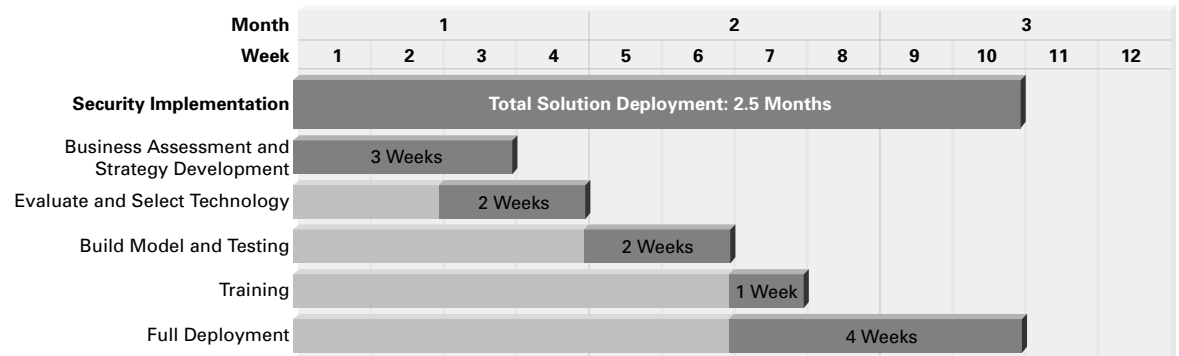
TIMELINE

Deployment timing depends on your network security needs. A typical deployment timeline includes the following basic elements:

- *Organizational assessment and strategy development*—Work with your technology partner to determine the current state of your practice's security infrastructure, obtain the support of senior stakeholders, and develop a strategic vision for your organization's network security.
- *Evaluate and select technology*—Let your partner help you determine the best software and hardware to support your needs and strategic vision. Prioritize your criteria (interoperability, scalability, and performance, for example).
- *Build and test your model*—Your technology partner and IT staff will connect organizational processes to technology features (a process known as “mapping”), customize configurations, and conduct testing.
- *Train*—Familiarize users with new technology, tools, processes, and operating activities.
- *Full deployment*—Implement full solution to the entire organization and network.

Figure 2 illustrates a sample security implementation timeline for a healthcare practice with up to 100 physicians.

Figure 2



SUCCESS MEASUREMENTS

Cisco Protected Healthcare Solutions for Physician Groups and Clinics provide many benefits for healthcare organizations. The most significant benefit is the increased level of confidence among patients and partners that confidential healthcare information is protected and secure.

Cisco Protected Healthcare Solutions for Physician Groups and Clinics—and the healthcare applications they enable—have other measurable benefits, including:

- Improved patient care through greater access to information
- Increased flexibility in where and how clinicians work
- Reduced errors by eliminating paper-based systems
- Reduced costs through streamlining manual processes
- Enhanced ability to collaborate and share information between physicians and organizations
- Faster claims processing
- Increased reliability and resilience of clinical systems

SUMMARY

Whether your organization is a large clinic or a small practice, you need to address healthcare privacy and security requirements. The threats to healthcare information and applications are growing. Today, even smaller organizations can deploy powerful, comprehensive solutions to protect and secure both critical healthcare applications and wired and wireless networks. The strong security provided by Cisco Protected Healthcare Solutions for Physician Groups and Clinics helps healthcare practices to ensure that they continue to have all the tools they need to effectively communicate with and care for patients.

Cisco offers numerous security solutions for small and midsize healthcare practices. These tools are specifically designed for easy deployment and use—even by organizations without a large IT staff.

Too much is at stake to risk compromising patient privacy or losing access to networked applications. Using Cisco solutions, you can draw on the industry-leading security expertise and hands-on experience Cisco and Cisco Channel Partners have gained from working with healthcare organizations around the world. Let us help you build a security foundation that serves the unique needs of your organization, and delivers comprehensive protection for your systems and your patients.



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

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Aironet 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. (0304R) N2/JB/LW5648 02/04