

Network Security Solutions for Health Care Making HIPAA SAFE



Introduction

The evolution of networking technologies has enabled businesses to provide enhanced services, greater access to information, and higher levels of availability, resulting in increased customer satisfaction. While many industries have easily adopted internetworking technologies, others have been unable to do so because of the inherent complexities of their specific businesses. The health care industry is a prime example. Health care, which is documentation-intensive, has faced significant challenges in migrating to the near “paperless” environments most industries strive to achieve utilizing networking technologies. Furthermore, health care organizations, dealing with such sensitive data as patients’ personal health information, have to be extremely wary of the potential privacy and security risks of converting to electronic information infrastructures.

In recent years, several factors have forced the health care industry to move towards the use of computer networking and the development of electronic health (e-health) strategies to improve the efficiency of their operations. For instance, health care has been undergoing massive consolidation resulting in the emergence of integrated delivery systems. Integrated delivery systems are large, regional providers that need to share clinical and other information among multiple hospitals, clinics, home-care agencies and other facilities. Also, the ability to provide physicians with the capabilities to practice medicine remotely and to assess patients in isolated locations via the Internet, often referred to as “telemedicine,” is becoming important to health care organizations to optimize effectiveness as well as to attract and retain the best physicians. According to a March 19, 2001 Fortune Magazine article, *Building a Virtual Infrastructure for Health Care* by Nancy Giges, “Web connectivity among hospitals, labs, pharmaceutical manufacturers, medical device companies, insurers, and managed care providers is reducing paperwork, phone calls, and redundant data entries. This flow of digital information is speeding up everything from claims to eligibility checks to orders of tests to reporting of test results.”

The health care industry’s steady move to electronic-based patient records and the delivery of health care information using computer networks has heightened concerns about the security of that information. With the proliferation of networking technology in health care, the need to implement safeguards to protect the privacy of patient data is paramount. However, many health care organizations have been reluctant to incorporate adequate security technology into their network infrastructures. According to observations made by Cisco Systems security consultants while conducting security posture assessments of health care organizations, the health care industry has the highest percentage of Internet vulnerabilities. For example, health care Web servers are found vulnerable 61.07 percent of the time, while the average throughout other industries is 27.37 percent. The Cisco consultants noted the common concern among health care organizations that security presents obstacles to sharing information.



While the health care industry has remained apprehensive about network security, the government has acknowledged the great importance of protecting patients' privacy and has developed health care privacy and security legislation. Although government intervention can elicit unplanned expenditures and administrative issues for some companies, these recently enacted and pending regulations should ultimately drive the health care industry to evaluate and optimize the efficiency of their networks, thereby improving customer relations and satisfaction.

Health Care and Legislation: HIPAA

On August 21, 1996, President Clinton signed into law, as US Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA 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 United States Department of Health and Human Services (DHHS) in the development and enactment of regulations regarding the maintenance and transmission of health information pertaining to individual patients. For example, HIPAA requires that by the completion of the 106th Congress, legislation be passed defining personal privacy as it applies to health care. Congress stated that once the final standards are adopted, small health plans have 36 months to comply, and other health care organizations must comply within 24 months. HIPAA also 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 Clinton administration reviewed HIPAA but did not enact any concrete health care privacy or security laws before the end of its term. More recently, the Bush administration has been reviewing HIPAA, and based on the recommendations within HIPAA, has enacted specific regulations by which health care organizations must abide. On April 12, 2001, President Bush agreed to move forward on the Patient Privacy Rule, which includes, among other items, regulations to prevent health care providers and insurers from disclosing patients' medical information without permission from the patients. The health care industry has until April 12, 2003 to comply with the new Patient Privacy Rules, however, the Bush administration will continue to consider changes to the rules regarding areas that have drawn considerable criticism. Health care organizations must comply with regulations, such as the Patient Privacy Rule, and take the proper steps in anticipation of further privacy and security regulations that may arise as a result of Congress' consideration of the HIPAA proposals.

HIPAA Proposed Security Standard

Recognizing that no single standard exists that integrates all the components of security (administrative procedures, physical safeguards, technical security services, and so forth), the legislators who developed HIPAA proposed a new security standard to define the security requirements. HIPAA states that the final health care security standard should be comprised with the following three conceptual guidelines as a basis:

- The standard should be *scalable*—All sizes of health care entities should be able to comply with the standard.
- The standard should be *comprehensive*—The required security solutions should act as a unified system, not a series of “piecemeal” products that do not communicate with each other.
- The standard should be *technology-neutral*—It should not reference or advocate specific security technology, because technology is constantly evolving. By not dictating specific system architectures and technologies, health care organizations can take advantage of state-of-the-art technologies and have the flexibility to choose the best solutions to fit their particular environments.



HIPAA recommends several requirements that should be included in the final health care security standard to protect the integrity, confidentiality, and availability of electronic health data. For the purposes of presentation only, the proposed requirements were divided within HIPAA into the following four categories:

- Administrative procedures—Documented formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data. Administrative procedures would include such items as formal termination procedures, security incident procedures, and security training.
- Physical safeguards—Relate to the protection of physical computer systems, buildings, and equipment from fire, environmental hazards, and physical intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures that control access to computer systems and facilities.
- Technical security services—Include the processes to protect, control, and monitor information access, such as access control and data authentication.
- Technical security mechanisms—Include the processes to prevent unauthorized access to data transmitted over a communications network, such as encryption, event reporting, integrity controls, and audit trails.

HIPAA Takes a General Approach

HIPAA recommends general requirements for the prospective security standard, rather than mandating specific security technologies for implementation in health care networks. HIPAA also suggests that organizations assess the potential security risks to the health information in their possession and determine which specific technologies will best meet their particular security and overall business needs. This approach was supported by one of many research reports consulted by the creators of HIPAA. The National Research Council's 1997 report, *For The Record: Protecting Electronic Health Information*, states, "It is therefore not possible to prescribe in detail specific practices for all organizations; rather, each organization must analyze its systems, vulnerabilities, risks, and resources to determine optimal security measures. Nevertheless, the committee believes that a set of practices can be articulated in a sufficiently general way that they can be adopted by all health care organizations in one form or another."

Cisco Solutions for Health Care Networks

Cisco, along with its extensive network of partners, provides a comprehensive array of security solutions designed to assist any size health care organization in complying with legislation that is enacted as a result of the recommendations set forth within HIPAA. Members of the Cisco AVVID (Architecture for Voice, Video, and Integrated Data) Partner Program support standards-based architectures and share a commitment to interoperate with Cisco market-leading products, technologies, and services. Certified Cisco AVVID technology and services partners offer interoperable security solutions for Cisco networks. Cisco and Cisco AVVID partner security solutions address all four areas of compliance outlined by the HIPAA requirements. These solutions include components to cover all aspects of privacy protection and network security improvement, including policies and procedures, business processes, identity, perimeter security, secure connectivity, monitoring, and policy and network management. These components, in conjunction with SAFE, a blueprint from Cisco describing how to design a practical security infrastructure to protect all areas of a network, enable organizations to create scalable, manageable, and reliable security infrastructures that should meet or be ready to meet the most stringent security regulations that come down the road.



Administrative Procedures

Cisco partners specializing in HIPAA compliance issues provide comprehensive services for the assessment and improvement of a health care entity's policies, procedures, and business processes. HIPAA compliance is as much about the "culture of privacy" within an organization as it is about technical safeguards. Cisco HIPAA partners provide reviews of an organization's privacy policies and procedures for the secure handling of sensitive patient information. They also review the organization's deployment of and existing controls over specific technologies that could affect the privacy posture. Using the results of these assessments, Cisco partners assist the organization in improving its posture through policy building, process improvement, and training and awareness efforts.

Physical Safeguards

Cisco security partners provide security reviews to assess the effectiveness of physical controls in place within a health care entity. In a physical security review, the security consultant evaluates such areas as the physical protection of hard copy and digital health care information, access to sensitive equipment and systems, and backup and recovery mechanisms.

Technical Security Services

As noted previously, HIPAA states that, "...the proposed standard requires that each health care entity engage in electronic maintenance or transmission of health information, assess potential risks and vulnerabilities to the individual health data in its possession in electronic form, and develop, implement, and maintain appropriate security measures." To that end, Cisco offers Security Posture Assessments (SPAs) conducted by highly experienced Network Security Engineers (NSEs) from the Cisco Secure Consulting Services team. Cisco SPAs include comprehensive security analyses of large-scale, distributed networks externally from the perspective of an outside hacker and internally from the perspective of a vindictive employee or contractor. The Cisco NSEs and security consultants then compile and analyze the security vulnerability information and present the customers with operational-level recommendations to make their corporate networks more secure and help them reach their full e-business, or e-health, potentials.

Cisco HIPAA partners provide a variety of additional security services to assist health care entities in assessing and mitigating potential risks and vulnerabilities to individual health data. These services include outsourced monitoring and management of security equipment, business impact and risk assessment services that measure the business risk of specific technical vulnerabilities, and application and configuration reviews of systems or software to determine vulnerabilities to exploitation or attacks at a host or code level.

Technical Security Mechanisms

Cisco provides a comprehensive suite of technical security solutions for building secure network infrastructures. Using the SAFE blueprint for secure networks, Cisco offers the security equipment necessary to protect and monitor health care entities' network data and data transmissions. Cisco solutions address secure authentication, perimeter protection, intrusion detection, encryption, and network monitoring and management. Cisco security solutions and mechanisms include:

SAFE Blueprint

SAFE is a comprehensive, robust security blueprint based on Cisco AVVID. The SAFE blueprint consists of modules that address the distinct requirements of each network area. By adopting a SAFE blueprint, network managers do not need to redesign their entire security architectures each time a new service is added to the network. With modular templates, securing each new service as it is needed and integrating it with the overall security architecture is easier and more cost-effective.

SAFE is the first industry blueprint that recommends exactly which security solutions should be included in which sections of the network and why they should be deployed. Each module in the SAFE blueprint specifically provides maximum performance for e-health while allowing enterprises to maintain security and integrity. By adopting a security infrastructure based on the SAFE blueprint, health care organizations can ensure the utmost protection for all areas of their networks and that they are prepared to meet government security regulations.



Access Control Servers

Access control servers validate users' identities, and determine which areas or information the users can access based on stored user profiles. The Cisco Secure Access Control Server (ACS) is a high-performance, highly scalable, centralized user access control framework. ACS offers centralized command and control for all user authentication, authorization, and accounting (AAA) from a Web-based, graphical interface and distributes those controls to hundreds or thousands of access points in a network. With ACS, network managers can control and administer user access for all Cisco IOS[®] routers, VPNs, firewalls, dial and broadband digital subscriber line (DSL) and cable access solutions, voice over IP (VoIP), and Cisco wireless solutions. The Cisco Secure ACS is one of many solutions in the Cisco suite of specialized security software solutions for AAA.

Firewalls

Firewalls provide barriers to traffic crossing network “perimeters” and permit only authorized traffic to pass, according to predefined security policies. Firewalls create protective layers between networks and the outside world. They also can log attempted intrusions and report them to network administrators.

The Cisco PIX[®] Firewall series is a high-performance, enterprise-class firewall product line that delivers high security without impacting network performance and scales to meet the requirements of any size health care company. The Cisco PIX Firewall series is a key element in the overall Cisco end-to-end security solution set and is the leading product line in the firewall market. Easy to install and manage, this purpose-built perimeter security device uses a hardened operating system focused solely on protecting both the security of the device and the security of the network in which it is deployed. The integrated hardware and software package delivers full stateful firewall protection and IP Security (IPsec) VPN capabilities allowing organizations to rigorously protect their internal networks from outside intrusions. The Cisco PIX Firewall also supports the new Cisco PIX Device Manager (PDM), a browser-based graphical user interface (GUI) for setup, configuration, and monitoring of PIX firewalls.

With the Cisco IOS Firewall, companies can embed advanced firewalling capabilities in their network operating systems. The Cisco IOS Firewall software is an add-on module to the Cisco IOS Software and is available for a wide range of Cisco routers.

Intrusion Detection

Network security is in many ways similar to physical security in that no one technology serves all needs—rather, a layered defense provides the best results. Organizations should implement complementary security technologies to counter risks and vulnerabilities that one mechanism alone cannot address. A network-based intrusion detection system (IDS) provides around-the-clock network surveillance. Unlike firewalls, an IDS monitors and analyzes packet data streams within a network, searching for unauthorized activity, such as attacks by hackers, and enabling users to respond to security breaches before systems are compromised. When unauthorized activity is detected, the IDS sends alarms to a management console with details of the activity and often orders other systems, such as routers, to cut off the unauthorized sessions. Cisco offers the widest array of sensing platforms in the industry, including dedicated network appliances, IDS line cards to incorporate into switches, and IDS functionality in Cisco IOS Software. This broad collection of devices fits the needs of any health care organization.

Network Scanning

Network scanners conduct detailed analyses of networked systems to compile electronic inventories of the assets and detect vulnerabilities that could result in security compromises. This technology allows network managers to identify and fix security weaknesses before intruders can exploit them. Cisco Secure Scanner is software that scans networks and compiles lists of all the networked systems within a specified address range, their operating systems, and active services. It then compares that information against an extensive network vulnerability database and determines which systems have security weaknesses. After non-intrusively confirming the presence of those vulnerabilities, Cisco Secure Scanner presents the information in a variety of formats from tables, charts, and text reports to detailed recommendations for corrective action. Cisco Secure Scanner allows users to measure security, manage risks, and eliminate security vulnerabilities on their networks.



Encryption and Virtual Private Networks

Health care companies must protect confidential patient information from eavesdropping or tampering during transmission. By implementing Virtual Private Networks (VPNs), companies can establish private, secure communications across a public network—usually the Internet—and extend their corporate networks to remote offices, mobile users, telecommuters, and partners. Encryption technology ensures that messages traveling across a VPN cannot be intercepted or read by anyone other than the authorized recipient by using advanced mathematical algorithms to “scramble” messages and their attachments. All Cisco VPN hardware and software devices support advanced encryption technology to provide the utmost protection for the data they transport.

The Cisco VPN 3000 Concentrator Series is a best-of-breed, remote-access VPN solution. Incorporating the most advanced, high-availability capabilities with a unique purpose-built architecture, the Cisco VPN 3000 concentrators allow any size corporation to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications. Remote users can utilize several devices to connect to the corporate network via VPN software clients loaded on PCs or laptops, hardware VPN routers, firewalls, and hardware clients. Cisco has solutions for all connectivity techniques using the Cisco VPN Unified Client Framework, Cisco routers, Cisco PIX firewalls, and the Cisco VPN 3002 Hardware Client.

Site-to-site VPNs—VPNs that connect branch offices and home offices to the central site—are best constructed using Cisco VPN-optimized routers, which include the Cisco 800, 1700, 2600, 3600, 7100, and 7200 router series. VPN-optimized routers provide scalability through optional hardware encryption acceleration. They also provide the wealth of routing, security, and quality-of-service (QoS) features resident in Cisco IOS Software required for secure, scalable, and reliable site-to-site VPN deployments.

Security Policy Management

A policy management system enables the simple and uniform deployment of network policies throughout a network. These policies may support various network services such as security, QoS, and voice. Security infrastructures, in particular, can include several technologies and products such as firewalls, VPN gateways, and IDS devices.

Cisco Secure Policy Manager (CSPM) centrally manages policies that support configurations of Cisco security products, such as the Cisco PIX Firewall, and Cisco routers running Cisco IOS firewalls. Using CSPM, network security personnel define the appropriate policies for their networks. CSPM then automatically translates these policies into the proper configuration files for the relevant network devices and securely distributes the configurations to the security devices.

Making HIPAA SAFE

HIPAA arguably impacts the health care industry more than any other recent legislation, causing major organizational and financial disruptions for many health care entities. The prospect of large new technology implementations or overhauling an entire network infrastructure to accommodate and anticipate government mandates can clearly be overwhelming. However, the benefits of a secure network extend far beyond government compliance and the avoidance of government-imposed penalties. Properly secured—SAFE—networks help companies avoid network attacks and breaches in privacy that have time-consuming and costly repercussions. Compromises to data integrity, availability, and confidentiality often take days of network downtime to repair, can elicit expensive civil lawsuits from customers, and can greatly decrease employee efficiency and customer satisfaction. Regardless of legislation, avoiding privacy and security breaches is pivotal to the success of a health care organization. Therefore, designing a network security architecture based on the SAFE blueprint and Cisco security mechanisms will enable organizations to run efficient, cost-effective, and competitive e-health operations.

Additional Information

For further information on Cisco security solutions, visit www.cisco.com/go/security.

For additional information on HIPAA and the Cisco "Making HIPAA SAFE" program, visit www.cisco.com/go/HIPAA.

For more information on Cisco AVVID partners, visit www.cisco.com/go/avvidpartners.



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.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 Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • 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

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX 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. (0105R)