# Cisco PCI Solution for Healthcare

## Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) was designed to protect customer privacy and credit card information. Meeting PCI requirements, however, can be challenging for many healthcare customers. The Cisco® PCI Solution for Healthcare provides guidance for healthcare institutions working to reach PCI compliance. This solution is a set of PCI audited architectures for remote locations, Internet edge, hospital campus, and data center networks, created to help with the design and implementation of network security for PCI compliance in the healthcare environment. In addition, Cisco PCI Compliance Services help healthcare institutions move toward achieving PCI compliance and then maintain a compliant state.

## Introduction

PCI was designed to ensure the security of cardholder data and information while in motion or at rest. PCI applies to any company that stores, processes, or transmits credit card information; in other words, the PCI standard affects most industries, including healthcare. Healthcare institutions may process credit card information in several locations, including registration and admittance areas, pharmacies, gift shops, cafeterias, in-room services, and in online billing and payment processes. And wherever credit card data is stored, those locations become part of the PCI scope. Areas such as the data center, remote clinics, or different departments that may store credit card data are all affected by the PCI Data Security Standard. PCI is an industry-regulated, global standard. Five major card brands—Visa, MasterCard, American Express, Discover, and JCB—control deadlines and enforcement of the PCI standard. The PCI Security Standards Council maintains and updates the standard, and provides training and certification of the Qualified Security Assessors (QSAs) and Approved Scan Vendors (ASVs)—companies that perform PCI audits and assessments. Healthcare organizations must have at a minimum quarterly scans performed by an ASV, and some healthcare organizations must have an annual onsite audit performed by a QSA.

## Deadlines and the Risks of Noncompliance

In the United States, the deadline for merchants to become PCI-compliant was September 30, 2007, for Level 1 merchants and December 31, 2007, for Level 2 and Level 3 merchants. Companies that missed this deadline may receive fines between US$5,000 and $25,000

per month, with some companies receiving $100,000 fine per month. These fines are for noncompliance—not for security breaches. Several companies did receive extensions to the September 30 and December 31, 2008, dates. European merchants (non-Level 1 merchants) have until December 31, 2008. Dates for other countries range from November 2008 through December 2009. Visa can provide specific deadline dates for each country and merchant level.

Merchant levels differ for each geographic region of the world. In general, however, Level 1 merchants are identified as organizations that process more than 6 million transactions annually of one card brand—for example, 6 million Visa transactions or 6 million MasterCard transactions, etc. It is not the aggregate transaction volume. Level 2 and lower merchants process fewer than 6 million transactions of any one card brand. This number varies significantly among regions of the world.

Security breaches have resulted in lawsuits, government investigations, expensive damage cleanup, reduced revenue, and brand reputation damage. Industry analysts state that damage from credit card security breaches can range from $82 per record to more than $300 per record. It is difficult to assess an actual number, because the damage costs depend directly upon the number of records stolen or lost, the amount of additional security that must be implemented into the network, processes and documentation that must be created, the time that investigation and forensics analysis takes, and lawsuits associated with the breach.

### The Challenge of Meeting Requirements

PCI compliance requirements are comprehensive, but they are built upon security best practices and provide more detailed information than most compliance regulations. Table 1 lists the 12 PCI requirements.

Table 1 PCI Requirements

| PCI Data Security Standard Requirements | |
|---|---|
| Build and maintain a secure network. | 1. Install and maintain a firewall configuration to protect data.<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters. |
| Protect cardholder data. | 3. Protect stored data.<br>4. Encrypt transmission of cardholder data and sensitive information across public networks. |
| Maintain a vulnerability management program. | 5. Use and regularly update antivirus software.<br>6. Develop and maintain secure systems and applications. |
| Implement strong access control measures. | 7. Restrict access to data by business need-to-know.<br>8. Assign a unique ID to each person with computer access.<br>9. Restrict physical access to cardholder data. |
| Regularly monitor and test networks. | 10. Track and monitor all access to network resources and cardholder data.<br>11. Regularly test security systems and processes. |
| Maintain an information security policy. | 12. Maintain a policy that addresses information security. |

Most industry experts agree that the best way to achieve and maintain PCI compliance is to adopt a strategic, holistic approach to network security risk management and compliance that includes policies, procedures, and technology. Cisco PCI Solution for Healthcare provides guidance on the technology aspect of PCI, as well as a set of PCI Compliance Services to facilitate achieving and maintaining compliance.

## Cisco PCI Solution for Healthcare

Cisco PCI Solution for Healthcare is a set of architectures (including remote locations, main hospital campus, the Internet edge, and the data center) in a lab environment to address PCI requirements. Cisco invited a global PCI Qualified Security Assessor (QSA), Verizon Business, to evaluate these architectures. The auditors found that the technology, if properly deployed and maintained, helps customers achieve PCI compliance. Customers can use these network architectures as a guideline as they work toward PCI compliance.

Figures 1 through 3 show healthcare environments that the Cisco PCI Solution for Healthcare includes as part of the audited architectures. Figure 1 covers a doctor's office with fewer than 25 devices on the network, Figure 2 shows a medical clinic that supports 25 to 100 devices, and Figure 3 is the hospital environment that has more than 100 devices connected to the network.

Figure 1 Doctor's Office with Fewer than 25 devices

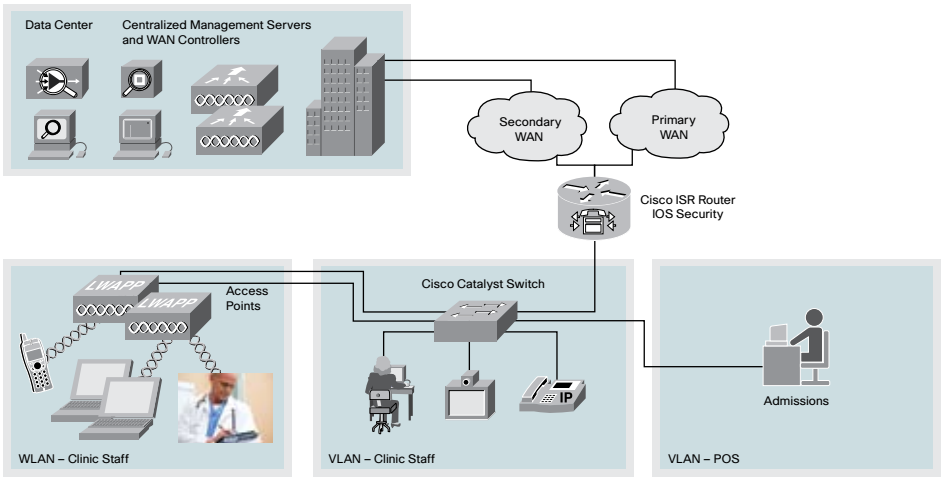



Figure 2 Medical Clinic with 25 to 100 Devices

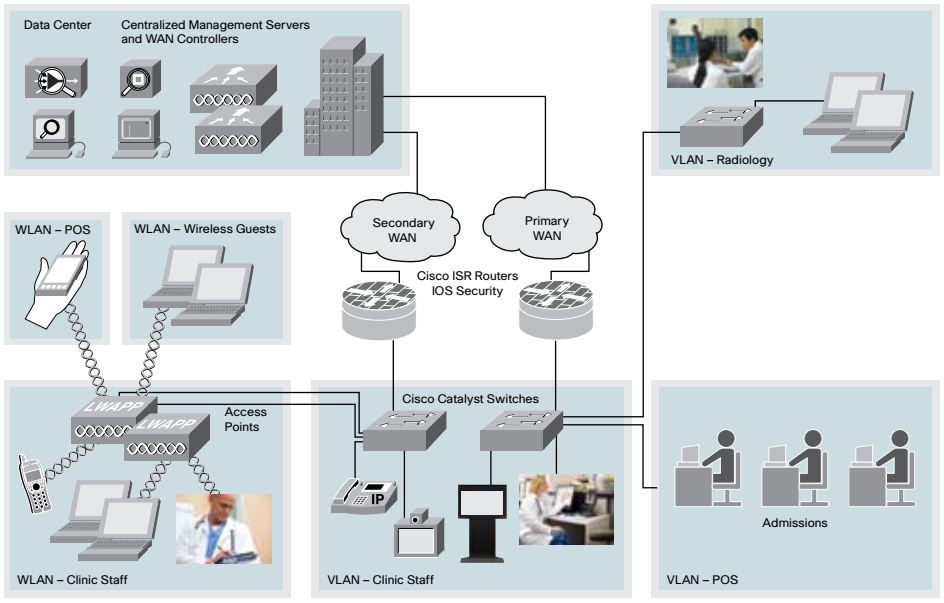
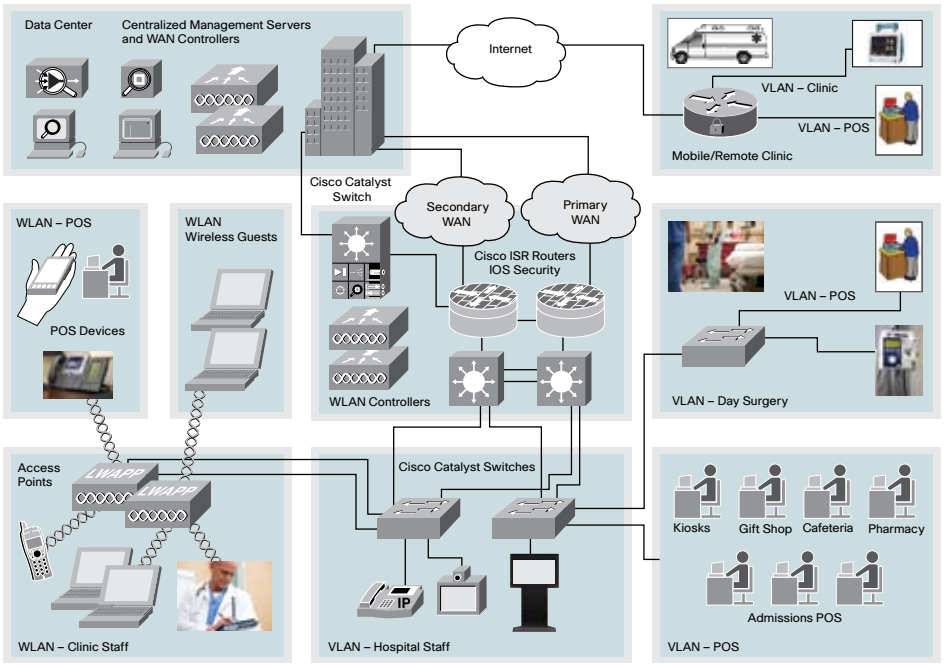


Figure 3 Hospital with More than 100 Devices




## Cisco PCI Compliance Services

PCI compliance services from Cisco and Cisco Security Specialized Partners support efforts of healthcare institutions to achieve PCI compliance and to stay compliant by helping identify and resolve compliance gaps.

## The Cisco PCI Compliance Service consists of four services

- **Cisco PCI Gap Analysis Service:** This service assesses your network relative to the PCI Data Security Standard and helps you to:
  - Accelerate the identification of gaps relative to the PCI Data Security Standard
  - Prevent additional, time-consuming planning cycles by proactively identifying potential gaps and risks
- **Cisco PCI Remediation Service:** This service addresses and closes compliance gaps as needed. The scope of this service varies, depending on the results of the Cisco PCI Gap Analysis Service and your decisions about which remediation activities you prefer to do yourself. The Cisco PCI Remediation Service helps you to:
  - Increase network security by aligning hardware and software releases, features, and functions with PCI Data Security Standard specifications
  - Improve deployment team and operations staff proficiency by providing continuous knowledge exchange throughout service delivery
  - Mitigate the risk of network downtime and costs from potential rework by accelerating the implementation and migration of new security solutions and technologies
  - Prioritize your remediation strategy and more effectively budget by providing a detailed PCI solution implementation plan
- **Cisco PCI Remote Monitoring and Management Service:** This service rapidly identifies threats and helps you to:
  - Protect assets, proactively, against new and existing threats through rapid incident identification

- **Cisco PCI Periodic Gap Analysis Service:** This service proactively identifies potential gaps and risks, helping you prevent additional, time-consuming planning cycles.

## Learn More Today

Cisco PCI Solution for Healthcare can help your healthcare organization achieve its compliance goals and simultaneously enable new strategic business initiatives. Call your local Cisco account executive to learn more. For additional information, visit www.cisco.com/go/healthcare, www.cisco.com/go/compliance, and for Cisco PCI Compliance Services, visit www.cisco.com/go/services/security.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**



DDM08CS1648 08/08