CHAPTER 1

Solution Overview

Introduction

Cisco customers have stated that the Health Insurance Portability and Accounting Act (HIPAA) is vague, and they are not sure how it directly applies to their enterprise networks. Many do not understand how HIPAA relates to technology and infrastructure. They have asked Cisco to provide guidance that shows this relationship. This Cisco Compliance Solution for HIPAA Security Rule provides a reference architecture designed to help covered entities and business associates simplify compliance with the HIPAA Security Rule. The guidance in this document maps architectures and products to the HIPAA Security Rule technical safeguards, standards, and implementation specifications.

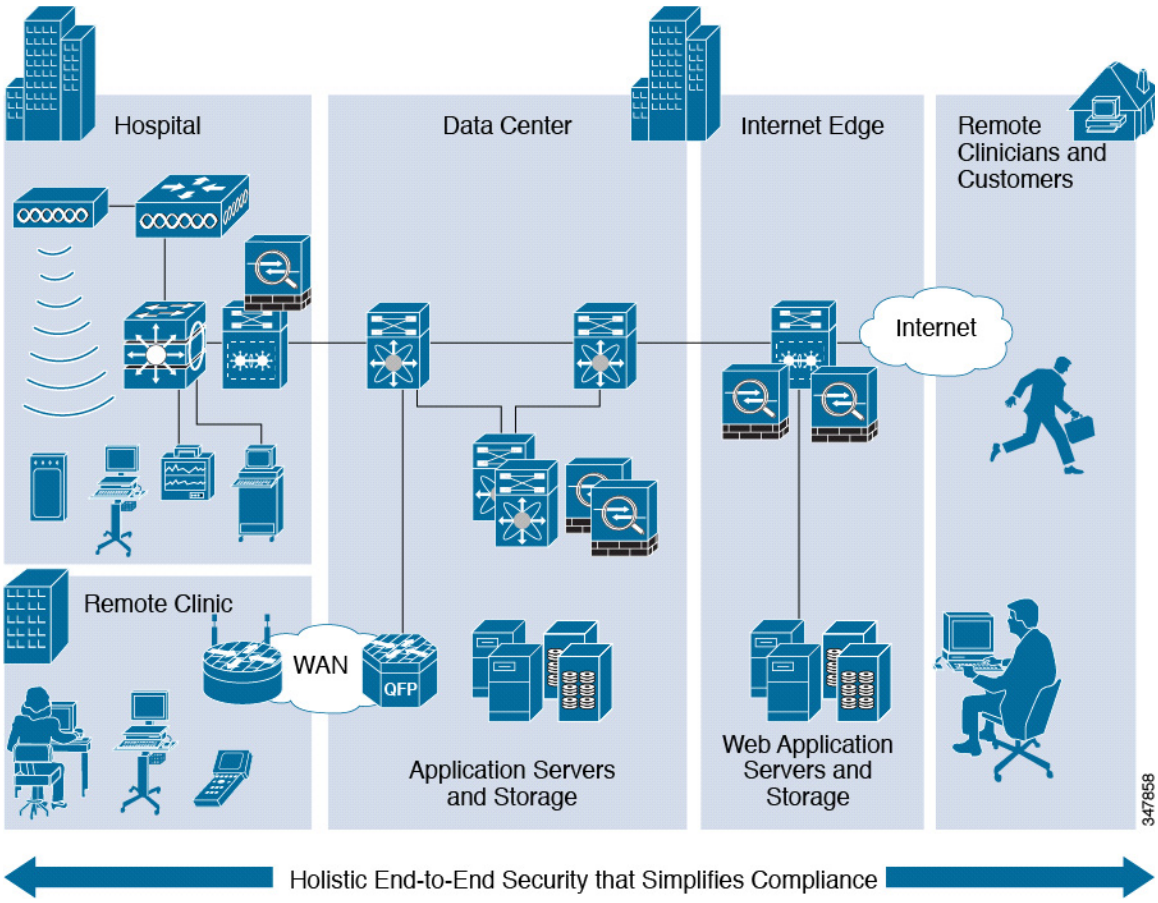
Chapter 2, "HIPAA and the Solution Framework," describes the elements that make up the solution framework. The solution framework organizes the scope of the Protected Health Information (PHI) data environment for contextual reference. Chapter 3, "Solution Architecture," discusses what IT should consider when designing their network to best align with HIPAA Security Rule implementation specifications. For specific designs referencing these architectures, read Chapter 4, "Solution Implementation." In Chapter 5, "Component Assessment," each component is individually assessed for its capabilities, and configuration examples are given to demonstrate this utility. The complete assessment report authored by Verizon is located in Appendix C, "Reference Architecture Assessment Report—Cisco Healthcare Solution."

The Cisco Compliance Solution for HIPAA Security Rule was built and tested using a holistic enterprise perspective including the following:

- Endpoint consideration—PHI systems and devices, including wireless devices
- Administrative concerns within scope of HIPAA
- Cisco, RSA, EMC, and Hytrust network infrastructure and architectures comprising data center, Internet edge, and healthcare facilities that simplify the process of meeting the HIPAA Security Rule implementation specifications.

Figure 1-1 shows an example of the enterprise architecture.

Figure 1-1 Enterprise Architecture



Solution Methodology

Cisco customers have asked for clarification on how HIPAA relates to Cisco architectures and individual components within the architecture. To address this challenge, Cisco contracted Verizon Business to "reassess" an existing compliance solution that protects credit card data; Cisco Compliance Solution for PCI DSS 2.0. The strategy is to use a common control structure that addresses multiple compliance standards using a "unified compliance" mindset. The intent is that regardless of the type of sensitive electronic data (payment or healthcare), a single security strategy should meet the needs of an organization to protect it from a compliance perspective.

Target Market/Audience

The audience for this solution includes compliance managers, as well as technical teams seeking guidance on how to design, configure, and maintain their IT architecture and components for HIPAA Security Rule compliance. Although the diagrams and references relate to healthcare institutions, the reference architecture also applies for other covered entities and business associate networks in relation to the HIPAA Security Rule.

Solution Benefits

The solution demonstrates how to design end-to-end enterprise systems that conform to the HIPAA Security Rule safeguards and provides the following benefits:

- Insight into the Cisco enterprise architecture and the controls used to address HIPAA Security Rule technical safeguards
- A detailed analysis and mapping of Cisco and partner components and their relationship with HIPAA Security Rule controls
- A scalable set of reference designs that can be used to establish the security controls necessary to achieve compliance with the HIPAA Security Rule
- A centralized management "tool kit" simplifying the operational challenges of an enterprise network
- The central focus of this design guide is the implementation of an architecture that meets the HIPAA safeguards; in addition, using the recommended segmentation strategies and additional quality of service (QoS) parameters can increase performance.

HIPAA Solution Summary Results

Table 1-1 lists the HIPAA citations that were addressed within the solution.

Table 1-1 HIPAA Citations Addressed

Citation	Title
164.308(a)(1)(i)	Security Management Process
164.308(a)(1)(ii)(D)	Information System Activity Review
164.308(a)(3)(ii)(A)	Authorization and/or Supervision
164.308(a)(3)(ii)(C)	Termination Procedures
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Function
164.308(a)(4)(ii)(B)	Access Authorization
164.308(a)(4)(ii)(C)	Access Establishment and Modification
164.308(a)(5)(ii)(B)	Protection from Malicious Software
164.308(a)(5)(ii)(C)	Log-in Monitoring
164.308(a)(5)(ii)(D)	Password Management
164.308(a)(6)(ii)	Response and Reporting
164.308(a)(7)(i)	Contingency Plan
164.308(a)(8)	Evaluation
164.310(a)(2)(iii)	Facility Access Control and Validation Procedures
164.312(a)(2)(i)	Unique User Identification
164.312(a)(2)(ii)	Emergency Access Procedure
164.312(a)(2)(iii)	Automatic Logoff
164.312(a)(2)(iv)	Encryption and Decryption
164.312(b)	Audit Controls

Table 1-1 HIPAA Citations Addressed

164.312(c)(1)	Data Integrity
164.312(d)	Person or Entity Authentication
164.312(e)(2)(i)	Transmission Integrity Controls
164.312(e)(2)(ii)	Transmission Encryption

Compliance with the HIPAA Security Rule was assessed by an external auditor, Verizon Global Services Group.

Note This document does not guarantee compliance with the HIPAA Security Rule.