CHAPTER 6

Summary

HIPAA is flexible and open to interpretation based on the type of healthcare entity. Cisco customers have asked for clarification in relation to the common architectures and security products that might be utilized. In response, Cisco contracted Verizon Business to assess Cisco's enterprise reference architectures and components. Verizon provides design guidance and explains the rationale that they used for assessing healthcare entities in the context of Cisco's enterprise solution set.

This Cisco Compliance Solution for HIPAA Security Rule provides a reference architecture designed to help covered entities and business associates clarify compliance with the HIPAA Security Rule by mapping architectures and products to the HIPAA Security Rule Technical Safeguards, standards, and implementation specifications.

Compliance is a journey, not a destination. It requires continual attention to maintain. It is a journey that cannot be traveled alone. Trusted advisors such as auditors and vendors simplify the goal of maintaining compliance. The following provides a summary of the assessment results.

HIPAA Solution Summary Results

Table 6-1 lists the HIPAA citations that were addressed within the solution.

Table 6-1 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

Table 6-1 HIPAA Citations Addressed (continued)

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
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

Lessons Learned

Addressing the individual HIPAA safeguards without an encompassing security framework is difficult; there are many grey areas that are contested by auditors and interpretations that can be made for corner cases. The best 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 data, a single security strategy should meet the needs of an organization to protect it from a compliance perspective.

As an example, there is no specific mention of firewall technology in the HIPAA standard because HIPAA is written to be flexible enough to address all types of healthcare entities. However, when considering the common risks that are associated with enterprise organizations, such as the Internet and partner connections that share ePHI, Verizon cites the following controls that inductively requires the use of a firewall:

- 164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
- 164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

The word *procedures* requires the use of a technology to address the commensurate risk. In organizations that are represented in the Cisco solution, the Internet is a tremendous threat that can be addressed only through the use of a stateful firewall.

In HIPAA, regardless of inconsistencies and specifics from interpretation, the resonant idea is that reasonable controls must be in place to mitigate existing risks that threaten the integrity and ownership of sensitive Healthcare data. By implementing a broader and often more specific common industry

security framework such as HiTrust's Common Security Framework (CSF), ISO 27002, or NIST Security Publications, as well as other industry-based standards, a comprehensive policy can be tailored to address the risk and governance needs specific to the enterprise organization.