CHAPTER 2

HIPAA and the Solution Framework

The Health Insurance Portability and Accounting Act (HIPAA) was signed into law in 1996 (Public Law 104-191). The HIPAA Omnibus Final Rule was released January 2013, and included updates from the Health Information Technology for Economic and Clinical Health (HITECH) Act, breach notification, penalty tiers, and extended HIPAA compliance obligations to include both covered entities and business associates. Covered entities and business associates that create, receive, transmit, or maintain protected health information (PHI) in electronic form must make a good faith effort to protect the corporate computing environment from reasonably anticipated threats and vulnerabilities; and take reasonable and appropriate measures to protect the integrity, confidentiality, and security of such electronic data.

The HIPAA Omnibus Final Rule consists of three main parts (sections) that put in place security and privacy requirements for the protection of PHI:

- Part 160—General Administrative Requirements. Deals mostly with the legal, compliance, and penalty aspects of HIPAA
- Part 162—Administrative Requirements. Deals with unique identifiers for covered entities in healthcare, provisions for transactions, and many other administrative issues in healthcare
- Part 164—Security and Privacy. Deals with the safeguards for protecting PHI in electronic and paper media. Part 164 consists of the following:
  - Subpart A—General Provisions §164.1xx
  - Subpart B—Reserved
  - Subpart C—Security Standards for the Protection of Electronic Protected Health Information §164.3xx
  - Subpart D—Notification in Case of Breach of Unsecured Protected Health Information §164.4xx
  - Subpart E—Privacy of Individually Identifiable Health Information §164.5xx

  The Cisco solution described in this document relates primarily to Part 164 Security and Privacy Subpart C.

The HIPAA Security Rule requires covered entities and business associates to perform an analysis of the potential risks to the electronic PHI for which they are responsible; and to then develop, implement, and maintain appropriate security measures to safeguard the integrity, confidentiality, and availability of that data. The HIPAA Security Rule incorporates recognized security objectives and protections, but is intentionally technology-neutral. It provides standards and, in some cases, implementation specifications with which covered entities and business associates must comply. The scope and nature

of HIPAA compliance activities for each covered entity or business associate vary according to the specific environment and associated vulnerabilities as determined through risk assessment. Although the standard is objective, a covered entity or business associate's specific security controls may vary, because the HIPAA Omnibus Final Rule permits flexibility in the approach to compliance.

Cisco and Verizon have provided clarity to the HIPAA Security Rule by providing a reference use case common to an enterprise. This use case identifies specific risks as well as the appropriate technology and configurations that can be used to satisfy the respective controls for these risks. Combining Cisco's technology portfolio, reference architectures, and Verizon's HIPAA assessment expertise, Cisco customers can benefit from using this document as an illustrative example of how to apply the same technology, configurations, and architectures within their own organizations to satisfy the security safeguards of HIPAA.

Safeguard Applicability and Exclusions

HIPAA Part 164 Subpart C is made up of nine sections. Three of the sections are administrative and are not part of this assessment. The remaining six sections (Security Standards: General Rules; Administrative Safeguards; Physical Safeguards; Technical Safeguards; Organizational Requirements; and Policies and Procedures and Documentation Requirements) consist of 52 security safeguards. Verizon performed an initial assessment to determine whether the safeguards could be met by using specific technology components provided by Cisco.

Of the 52 safeguards in the current healthcare requirements, Verizon identified 29 safeguards as not applicable in the context of this assessment, because the safeguard was either explicit and demanding direct (non-technology related) controls; or general, but not allowing for the reasonable use of technology as a compensating control in the fulfillment of the safeguard. Table 2-1 lists the remaining 23 applicable safeguards.

Table 2-1 Applicable Safeguards

	Citation	Title
1.	164.308(a)(1)(i)	Security Management Process
2.	164.308(a)(1)(ii)(D)	Information System Activity Review
3.	164.308(a)(3)(ii)(A)	Authorization and/or Supervision
4.	164.308(a)(3)(ii)(C)	Termination Procedures
5.	164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Function
6.	164.308(a)(4)(ii)(B)	Access Authorization
7.	164.308(a)(4)(ii)(C)	Access Establishment and Modification
8.	164.308(a)(5)(ii)(B)	Protection from Malicious Software
9.	164.308(a)(5)(ii)(C)	Log-in Monitoring
10.	164.308(a)(5)(ii)(D)	Password Management
11.	164.308(a)(6)(ii)	Response and Reporting
12.	164.308(a)(7)(i)	Contingency Plan
13.	164.308(a)(8)	Evaluation
14.	164.310(a)(2)(iii)	Facility Access Control and Validation Procedures
15.	164.312(a)(2)(i)	Unique User Identification

Table 2-1 Applicable Safeguards (continued)

16.	164.312(a)(2)(ii)	Emergency Access Procedure
17.	164.312(a)(2)(iii)	Automatic Logoff
18.	164.312(a)(2)(iv)	Encryption and Decryption
19.	164.312(b)	Audit Controls
20.	164.312(c)(1)	Data Integrity
21.	164.312(d)	Person or Entity Authentication
22.	164.312(e)(2)(i)	Transmission Integrity Controls
23.	164.312(e)(2)(ii)	Transmission Encryption

See Appendix C, "Reference Architecture Assessment Report—Cisco Healthcare Solution," for the complete rationale of how HIPAA controls are divided between technology and policy.

Industry Standards

Although HIPAA is flexible and technology-neutral, industry standards are often used to meet the requirements. Among the standards often used are the NIST Special Publications, ISO 27002 and the HiTrust Common Security Framework (CSF). These standards provide more detail for the design and implementation of the infrastructure to meet the requirements.

The HiTrust alliance was formed by organizations in the healthcare industry to create a detailed framework to meet the vague HIPAA safeguards. Cisco's Solution Framework is closely aligned with the HiTrust CSF and can be used to address many of the detailed security controls in the CSF.

This document addresses HIPAA safeguards directly.

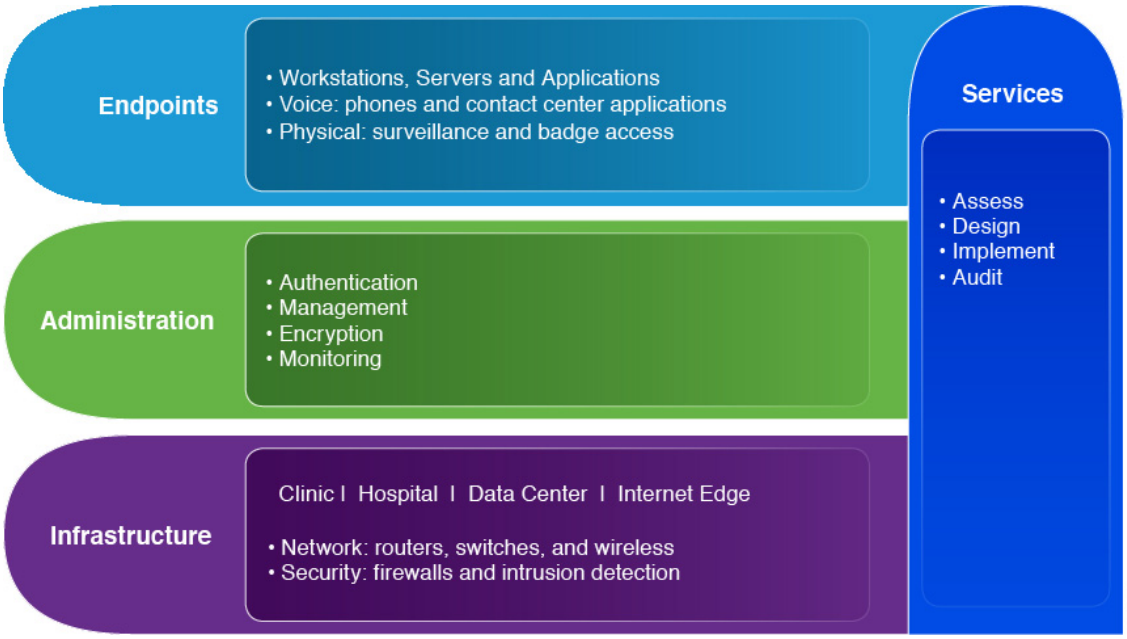
Control Mapping to the Cisco Reference Architecture

Verizon found that Cisco's solution architecture can directly address HIPAA safeguard requirements for technical controls to protect healthcare data. Any device that transmits or stores PHI data needs to be secured. An enterprise network can be conceptualized into several layers, creating a framework that ensures that these devices are properly handled.

HIPAA Solution Framework

Figure 2-1 shows how covered entities and business associates can be organized into a solution framework. By using this framework, healthcare security requirements and their associated control options can be simplified into three overarching layers that allow a simple way of discussing the complexity of the topic. The rest of this manual presents healthcare solution components within this context.

Figure 2-1 Cisco HIPAA Solution Framework



The HIPAA solution framework is used throughout this guide as a model for simplification.

Endpoints/Applications

The top layer of the solution framework takes into account applications or endpoints (workstations, clinical systems, medical devices, mobile carts, and doctors' laptops/tablets/phones) that are involved in the presentation of ePHI for use by/with clinicians, patients, and other member of the workforce. This layer includes the individual applications that may store and process ePHI, including:

- Clinical management and electronic records management systems
- Billing and payment systems
- Image management subsystems
- Voice transcription subsystems
- Video conferencing subsystems

This layer also includes the individual applications that may otherwise provide technical controls that fulfill some element of the HIPAA Security Rule safeguards, including:

- Physical security subsystems
- Emergency voice and data systems
- Data backup subsystems
- Facilities management subsystems

Administration

The middle layer of the framework shows the services used to support administration of the other layers. Example controls include:

- Identity management, authorization, authentication, and access management controls
- Logging and log management controls
- Auditing capabilities
- Monitoring and event management controls
- Data encryption/decryption controls and key management controls
- Physical access, intrusion detection, and surveillance controls

HIPAA is highly focused on Administrative safeguards. 29 of the 52 HIPAA safeguards (9 standards and 20 implementation specifications) are Administrative. To create an environment that is aligned with HIPAA safeguards requires the capability to meet these safeguards. Cisco addresses 13 of the administrative controls.

Infrastructure

The bottom layer of the framework addresses infrastructure components such as routers, switches, firewalls, and security components that support the common and advanced security controls managed at the layers above. The HIPAA Solution framework leverages the inherent strengths of the Cisco network and systems building blocks to allow the customer to build and configure robust architectures that support and align with the HIPAA Security Rule safeguards. The Cisco solution is a set of architectures, strategic principles, and tactical designs meant to provide the reader with a clarifying understanding of how the safeguards (and associated security control implementation requirements) are identified in the HIPAA Security Rule, and how real-world implementations of today's best-practice architecture can be efficiently deployed.

Services

The right-hand element that spans Endpoint, Administration, and Infrastructure layers includes services to plan, build, and manage the network to address the HIPAA Security Rule. These can be provided by Cisco, Cisco partners, and Verizon Business. Sample services can include the following:

- Strategy and analysis
- Assessments
- Design
- Validation
- Deployment
- Migration
- Product and solution support
- Optimization and operation services