APPENDIX C

Reference Architecture Assessment Report—Cisco Healthcare Solution

Based on: Healthcare Information Portability and Accountability Act of 1996 (HIPAA Security Rule)

November 27, 2013

Contact Information

Verizon Business **Kenneth Luberto** *Sr. Security Consultant* kenneth.luberto@one.verizon.com **Larry Bickner** *Principal Security Consultant* larry.k.bickner@one.verizon.com	
Cisco Systems, Inc. **Christian Janoff** *Compliance Solutions Architect* christian.janoff@cisco.com **Bart McGlothin** *Compliance Solutions Architect* bart.mcglothin@cisco.com	

Table of Contents

1. Executive Summary

Cisco Systems, Inc. (Cisco) engaged Verizon's Global Consulting and Integration Services (GCIS) to conduct a security controls assessment (Assessment) of Cisco's "Healthcare Solution" designed architecture, based on maximizing the alignment of Cisco's available security controls with the Healthcare Information Portability and Accountability Act (HIPAA) Security Rule safeguards. This Assessment reviewed how Cisco's "reference security architecture" provided either direct security controls or compensating security controls, which are capable of meeting or exceeding the security "safeguards" as identified in HIPAA. This Assessment included the review of Cisco's reference security architecture and the user, data, network, and system controls provided therein.

Cisco markets the assessed reference architecture solution to their customers looking to meet their healthcare security requirements, specifically within their IT environment and within their data center infrastructure. Cisco will use the findings from this assessment to design a solution that aligns with the security requirements that are generally accepted to fulfill security controls, with respect to the HIPAA security safeguards (requirements), and plan to provide the results of this Assessment to Cisco Sales Engineers interfacing with their enterprise Customers.

Verizon's Assessment covered Cisco's enterprise architectures including: datacenter; Internet edge; WAN; small, medium, and large clinic architectures; clinics/out-patient facilities; and small hospitals, among others.

The Cisco reference architecture is not designed or envisioned to directly fulfill the HIPAA Safeguards that are purely operational or organizational (for example, the assignment of the HIPAA Security Officer), or purely documentation oriented (for example, the assurance that documents are regularly reviewed). Verizon has found that Cisco's reference architecture for Healthcare does provide a strong technology foundation for managing technical risks that meet the healthcare customer's need to manage risks, specifically around the protection of electronic Patient Health Information (ePHI).

The Healthcare Security Requirements revolve around HIPAA Part 164 Part C. 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.

Of the remaining 23 Safeguard Areas in the current healthcare requirements, Verizon has further identified **8 Safeguards that call for universal security control requirements** that are foundational across Cisco's products and present in all network devices and systems that make up Cisco's Healthcare Reference Architecture.

Safeguard Areas where Cisco Security Controls are Not-Applicable	Safeguard Areas where Cisco Security Controls are Universally Applicable	Safeguard Areas where Cisco Security Controls are Specifically Applicable
29	8	15

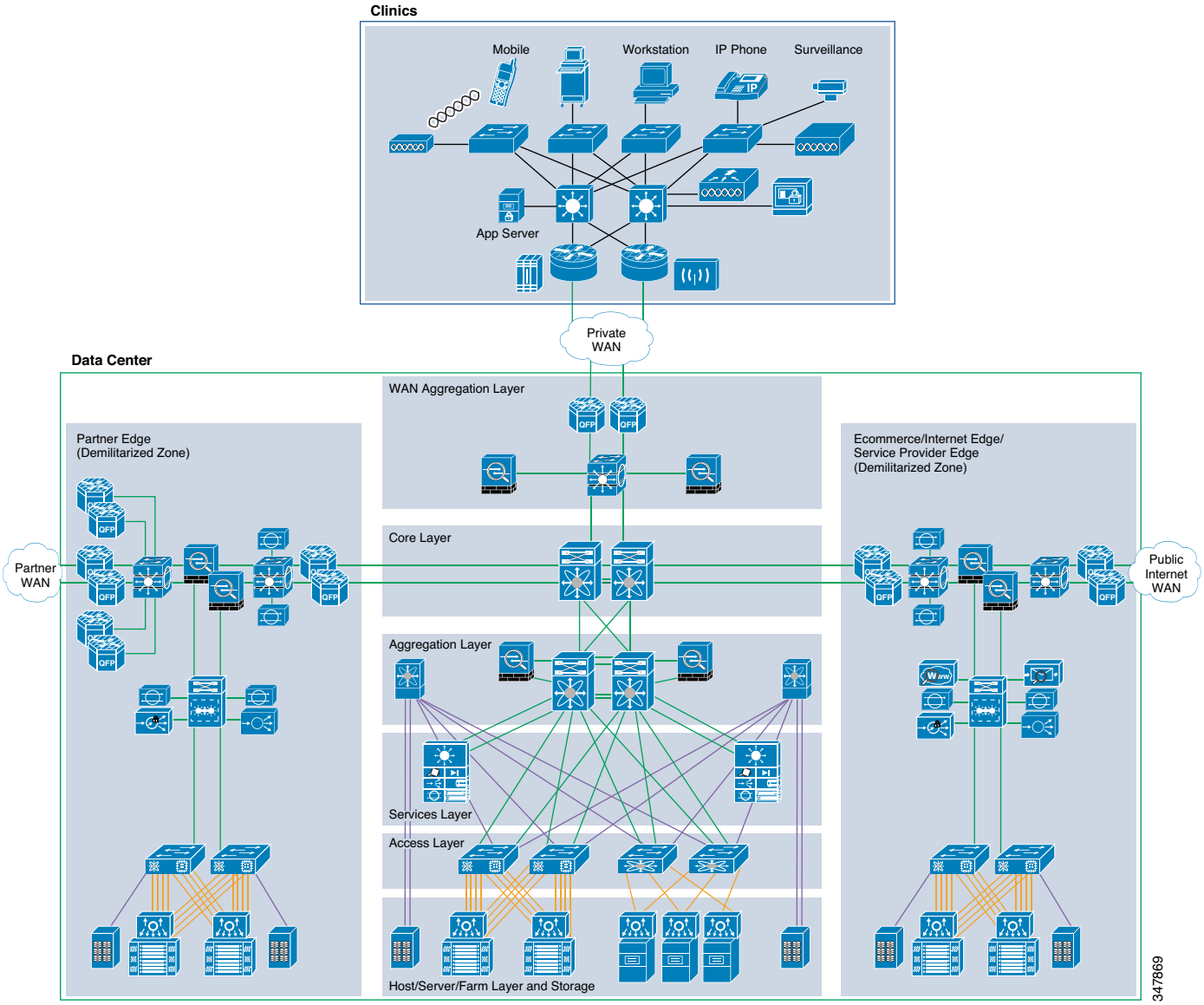
In the remaining 15 Safeguard Areas in the current healthcare requirements, Verizon assessed the capability and capacity for Cisco's Healthcare Reference Model to support technically Direct Control that meet the intent of the Safeguard, or to provide Compensating Controls that, when implemented in conjunction with layered controls, the Healthcare Reference Model could support the fulfillment of the Safeguard; as a technology implementation that would in turn allow for a less complex operating procedure or management process to meet this Safeguard. Verizon has identified the primary security controls that could be used to form a technical foundation of direct and compensating controls, for complying with the healthcare requirements.

Based on our assessment, Verizon believes that Cisco's Healthcare Reference Architecture provides a robust networking core and infrastructure that can support a customer's implementation of network security controls and system security controls as part of their security program and as a required HIPAA-Required Risk Management process. The architecture also provides both strong common security controls through network devices and security control and management systems that are highly capable to support data security, and specific security management components that are directly applicable to meet HIPAA safeguard control requirements. The fact that Cisco devices universally support the core security controls outlined in HIPAA Safeguards allows a customer to implement the reference architecture with the confidence that their resulting infrastructure will support HIPAA compliance from the outset, and with the knowledge that any additional use of Cisco's security management tools will only enhance the protection of ePHI and further support Healthcare compliance.

Cisco's Healthcare Reference Architecture also provides directly applicable security control features and capabilities owing to the depth of security management tools provided in this model. Directly Applicable controls include: Physical Access Control, Intrusion Detection, and Visual Surveillance;

Network Access and Authentication Controls for wired, wireless, and remote networks; Network Segmentation, Segregation, and Isolation Capabilities; Logging, Auditing, and Monitoring Capabilities; and Encryption.

Figure C-1 Enterprise-wide Healthcare Reference Architecture



2. Introduction

Reference Documentation

HIPAA (the "Act") was signed into law in 1996 (Public Law 104-191). Title II (Fraud, Simplification, and Abuse) of the Act contains the Administrative Simplification provisions with which Covered Entities (CEs) must comply in order to facilitate the exchange of electronic Protected Health Information (ePHI) and to ensure the security and confidentiality of consumer information. The Act asserts that CEs that collect, store, and/or process 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 security protections selected may be examined in the event that the CE and its associated business partners and service providers are the subjects of a compliance audit.

The HIPAA Security Final Rule that implements the Act requires CEs to perform an analysis of the potential risks to the electronic PHI for which they are responsible; and then develop, implement, and maintain appropriate security measures to safeguard the integrity, confidentiality, and availability of that data. Security plans must fully document the security measures implemented by the organization and should reflect the management of risk to acceptable levels. Periodic evaluation of the risks to the corporate computing environment and ePHI is also a requirement.

The HIPAA Security Final Rule is a regulatory framework that incorporates recognized security objectives and protections, but which is intentionally technology-neutral. The Final Rule provides standards and, in some cases, implementation specifications, that require CEs to implement predetermined controls. To achieve a baseline level of compliance, a covered entity must have a comprehensive information security program. The scope and nature of each covered entity's security program will vary according to its specific environment and associated vulnerabilities as determined through its risk analytical processes. Although the standard is objective, a covered entity's specific security controls may vary, as the Final Rule permits flexibility in approach to compliance. The Final Rule permits CEs to select "reasonable and appropriate" control measures according to level of risk and potential tolerance within the environment. For example, CEs can achieve compliance with authentication requirements by using strong passwords or through biometric technology. The choice to implement one authentication tool over another must be based in large part on the likelihood a security breach will occur and the potential damage that could result from such a breach.

HIPAA consists of three main Parts (sections) that are designed to put in place security and privacy requirements for protection of Protected Health Information (PHI). Each Part has multiple subparts that provide detail for the section.

- 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. This section is generally broken down into General Provisions §164.1xx, Security Standards for the Protection of Electronic Protected Health Information §164.3xx, Notification in Case of Breach of Unsecured Protected Health Information §164.4xx and Privacy of Individually Identifiable Health Information §164.5xx. This report deals mainly with the Security Standards for the Protection of Electronic Protected Health Information Subpart C.

There have been multiple discussions surrounding the required security components an organization needs to implement in order to meet HIPAA guidelines. Specific technologies such as intrusion detection and firewalls are not mandated and implementing appropriate security controls to address the requirements are determined by the covered entity.

HIPAA as written includes a flexibility rule in the security standards for determining the appropriate security controls based on a covered entities size, technical infrastructure, and hardware and software capabilities. Under §164.306 Security Standards: General Rules it states:

> (b) Flexibility of approach.
>
> (1) Covered entities and business associates may use any security that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
>
> (2) In deciding which security to use, a covered entity or business associate must take into account the following factors:
>
> (i) The size, complexity, and capabilities of the covered entity or business associate.
>
> (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
>
> (iii) The costs of security measures.
>
> (iv) The probability and criticality of potential risks to electronic protected health information.

This flexibility has led to confusion on occasion as covered entities attempt to identify appropriate security controls for their organization. Assessors have used current industry-accepted security practices to assess the security controls to determine the level of compliance with the safeguards. Typical infrastructure components such as firewalls, intrusion detection/ prevention, and network segmentation are among the technical controls that are industry-accepted security practices assessors typically review.

Business Associate

While HIPAA was written for CEs, consideration was taken into account for partners or Business Associates (BAs) that provide services to the CEs. The U.S. Department of Health and Human Services description of a business associate is: A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Further the American Reinvestment and Recovery Act (ARRA) of 2009 and the recent Omnibus Ruling in 2013 placed additional requirements on BAs to implement controls to meet HIPAA Security requirements. This significantly expands the HIPAA security requirements to organizations outside of the healthcare field. Organizations failing to meet the requirements are subject to substantial financial penalties.

Timeframe

Verizon performed this assessment in Q1 and Q2 of 2013. The previous PCI assessment which was performed in 2012 was used as a reference to gather knowledge about Cisco product offerings and to review the reference architecture.

Cisco's Healthcare Reference Architecture

Cisco's Healthcare reference architecture supports the networking infrastructure commonly seen in national-level healthcare organizations down to individual clinics operating as part of a regional health group. The architecture supports the centralization of ePHI into regional data centers (i.e. in hospitals or regional data center facilities) or into a central (national data center with regional backups).

The Architecture supports data, system, and application segmentation, segregation, and isolation at the data center level to allow for structuring of systems/network segments containing ePHI (for example, clinical systems) from networks/workstations/systems not intended for ePHI processing or storage (for example, administrative systems). The architecture addresses Internet isolation and patient access, remote secure access into the infrastructure by authenticated users, and the stratification of clinics, administrative offices, hospitals, and out-patient facilities that each have a variable need for ePHI access.

Reference Model Components

The architecture assessment included the following components:

CISCO COMPONENT	SPECIFIC CISCO DEVICES INCLUDED IN THE REFERENCE MODEL
Cisco Routers (ISR)	891w-AGN, 1941w, ISR G2, 2921/51 ISR G2, 3945 ISR G2, ASR1002, ISRs are configured with Firewall and IDS feature set.
Cisco Firewalls (ASA)	Network Firewall device, ASA-5585-x, ASA-5555-x, ASA-5500, ASA-5515-x
Cisco Switches	2960 PD-8TT-L, 2960- 8TC-L, 2960 S, 2960 C, 3560 C, 3560 X, 3750 X, 4507-Sup 7, 6500, Nexus1000v, Nexus5000, Nexus7000, MDS 9500, Catalyst-2000, Catalyst-3000, Catalyst-4000, Catalyst-6000
MDS Switch Fabric	
Cisco Wireless	1262N Access Points, 3502E Access Points, 3502I Access Points, CT5508 Controller, WLC2125 Controller, Mobility Service Engine, WCS-Wireless Manager, AIR-XXX, 891W, 1941W
Cisco Security devices	ASA 5585, ASA 5555, ASA 5515-x, NAC, IOS Firewall, AnyConnect - VPN. Catalyst ASA Services Module, Catalyst Intrusion Detection Service Module
Server Vitalization	Servers - ISR SRE 900, UCS Express server ESXi
VBlock	UCS - MDS - EMC SAN, EMC-Clarion,
Cisco Security Manager	Central provisioning of device configuration and security policies, including: ASAs, Cisco ASA Services Modules, IDS, ISRs, and switches
Cisco Secure Access Control Server (ACS)	AAA server
Cisco Prime LAN Management Solution (LMS)	Configuration Management / Configuration Enforcement and monitoring (Pari Compliance Module)
Cisco Physical Access Manager (PAM)	Configuration and central management of Cisco physical access control devices
Cisco Physical Access Gateway	Primary controlling device for physical access
Cisco Identity Services Engine (ISE)	Central Authentication, Policy / Configuration enforcement
RSA Access Manager	Used for central authentication/logging for access to RSA Data Protection Manager within the assessed environment.
RSA Authentication Manager	Central management/logging of RSA SecurID (two-factor) authentication for remote access into the data center environment.
RSA Data Protection Manager	formerly RSA Key Manager
RSA enVision	RSA's solution for compliance and security information management. RSA enVision was used to centrally collect RSA SecurID authentication logs on the RSA Authentication Manager server, using a batch process that runs several times a day.
HyTrust	Network-based virtual infrastructure policy enforcement. Administrative access control, enforcement of policy across virtual infrastructure, hypervisor hardening, and audit logging. Access and User administration, change and configuration, and operations

Network Segmentation and Management

Cisco has designed several network architectures to account for small, medium, and large healthcare IT environments. Cisco chose Integrated Services Routers (ISRs) to provide firewall, IDS, and routing functionality. Access-lists are applied through firewall policies, which are pushed to the ISRs in each architecture. Access-lists implicitly deny all inbound and outbound traffic across the network; Approved traffic must be explicitly allowed to the IP address, port and service level thereby creating access control granularity. Additionally, Cisco has incorporated wireless into the design, using WPA2, WPA-TKIP for secure wireless networking to support seamless control strategies for both wireless and wired networks.

The data center environment is segmented into multiple VLANs, including Internet Edge, WAN aggregation, and Core service aggregation. Multiple layers of network security are included in each data center segment, including Cisco ASA Services Module and ASA stateful firewall filtering and integrated IDS/ detection/prevention, access lists, secure VPN (WAN aggregation and remote VPN), and two-factor authentication. These devices allow for fine-grained control of network and system access between systems, and support isolating ePHI-containing systems/servers from IT resources that need not be exposed to ePHI. (e.g. Administrative systems) Network devices are centrally managed through the following:

- Cisco Security Manager (CSM)—(Central security management for ISRs and switches (e.g., firewall policy, IDS/signatures)
- Cisco Wireless Control System (WCS)—Central wireless management
- Cisco ACS—Central TACACS+ (central authentication) server for ASA firewall, Cisco ASA Services Module, ISR, ASR router, switch, wireless controller (RSA enVision and WCS).
- RSA enVision—Central logging/Correlation/Analysis/Alerting server. Alerts from IDS/alerts and firewall logs.
- Cisco ASDM—configuration for ASA firewalls.
- Cisco Device Manager (IDM)—IDS/configuration management.
- Cisco Prime LAN Management Solution (LMS)—Central configuration management, monitoring, and troubleshooting.
- Cisco Identity Services Engine (ISE) – Central Authentication, Policy / Configuration enforcement for ASA firewall, Cisco ASASM, ISR / VXR routers, Cisco switch, and wireless controllers

Wireless LANs and/or Wireless Applications

Wireless networks within the reference environment are configured to use WPA2, WPA-TKIP authentication for secure wireless networking. Wireless traffic must pass through the ISRs and IOS firewall access-lists to traverse any part of the network, thereby controlling wireless access to network segments and devices containing ePHI. Best practice security parameters have been applied to wireless networks, including: HTTPS access for wireless management, default SSID has been changed, SNMPv3 used (default strings changed), and HTTP access has been disabled.

Wireless technology in the PHI environment is a growing concern for organizations in the healthcare field. Implementing wireless requires that appropriate security controls are in place to prevent, detect, and respond to security violations. Appropriate controls include implementing a firewall to segment and protect the PHI data environment and intrusion detection services to identify potential intrusion attempts to the secured network. Encryption must be configured to adequately protect PHI transmitted over the wireless medium.

3. Assessment Findings and Conclusions

The Healthcare Security Requirements revolve around HIPAA Part 164 Part C. 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 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.

3.1 Safeguard Exclusions

Of the 52 Safeguard Areas 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. The Safeguards deemed as non-applicable under this assessment, and thereby removed for further consideration, include. the following.

Citation	Safeguard Title	Safeguard Description	Applicability of Technical Solutions to this Safeguard
§164.308(a)(1)(ii)(C)	Risk Analysis	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to ePHI held by the covered entity or business associate.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This Safeguard calls for a risk assessment to identify all areas of risk to ePHI. All infrastructure components that process, store or transmit ePHI must be addressed.
§164.308(a)(1)(ii)(C)	Risk Management	Implement security measures to sufficiently reduce the risks and vulnerabilities to a reasonable and appropriate level.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This Safeguard calls for the implementation of appropriate controls to address the risks identified in the risk assessment. Technological controls for each infrastructure component need to be evaluated to determine if they can appropriately protect ePHI.
§164.308(a)(1)(ii)(C)	Sanction Policy (1)(ii)(C)	Ensure that sanctions are in place to discipline workforce members of the covered entity or business associate who fail to comply with the security policies and procedures for protecting ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This Safeguard calls for the implementation of an operating Policy with the Customer's environment, and while a strong technical security baseline can support implementation of the Policy, it cannot substitute for a written policy that is distributed across the workforce.

§164.308(a)(2)	Assigned security responsibility	Assign responsibility for the development and implementation of the policies and procedures for protecting ePHI required by the covered entity and business associates.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This safeguard calls for the covered entity to formally assign an individual who is responsibility for the security program development and implementation of appropriate policies and procedures to protect ePHI. This is a personnel issue only and there is no technology requirements directly affiliated with this safeguard.
§164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Implement policies and procedures to determine that access of workforce members to ePHI is appropriate.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking for a policy and procedure to ensure that access to ePHI is appropriate. While technical controls may be used implement the policy, it Is not the direct intent of this safeguard.
§164.308(a)(5)(ii)(A)	Security Reminders	Identify and distribute periodic security updates to all members of the workforce including management.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are in place for the occasional distribution of security reminders to reinforce or update all staff on new threats and vulnerabilities.
§164.308(a)(7)(ii)(A)	Data Backup Plan	Establish and implement procedures to create and maintain retrievable copies of ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. -This Safeguard calls for backing up data and storing copies off-site that can be retrieved in response to an emergency that damages systems that contain ePHI.
§164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Establish and implement procedures to restore any loss of ePHI data.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This Safeguard calls for a documented plan to restore any loss of ePHI data.
§164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Implement procedures for periodic testing and revision of contingency plans.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This Safeguard calls for the periodic testing and revision of the disaster recovery plan.

§164.308(a)(7)(ii)(E)	Applications and Data Criticality	Assess the relative criticality of specific applications and data in support of other contingency plan components.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This Safeguard calls for the criticality of each application to be assessed to determine the priority required to restore applications in an emergency.
§164.308(b)(1)	Business Associate Contracts	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.
§164.310(a)(2)(i)	Contingency Operation	Establish and implement procedures that allow for facility access in support of restoration of lost data under disaster recovery plan and emergency access mode operations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This Safeguard calls for policies and procedures that allow for access to the facilities to restore lost data during a disaster or emergency.
§164.310(a)(2)(ii)	Facility Security Plan	Implement policies and procedures to safeguard the facility and the equipment inside from physical access, tampering and theft.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This safeguard is looking to ensure that physical access is available to authorized personnel to support the restoration of lost data in contingency operations
§164.310(a)(2)(iv)	Facility Access Controls - Maintenance Records	Description: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that devices providing physical security are maintained to prevent failure and allow unauthorized physical access to the facilities that process, store or transmit ePHI.

§164.310(b)	Workstation Use-Workstation Use	Description: Implement policies and procedures that specify the proper functions and the physical attributes for workstations that can access ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that all employees or contractors that have access to a workstation that has or may have access to ePHI is aware of the appropriate use of the workstation.
§164.310(c)	Workstation Security-Workstation Security	Description: Implement physical safeguards for all workstations that access ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that all workstations that have or may have access to ePHI are appropriately secured to prevent unauthorized access.
164.310(d)(2)(i)	Device and Media Controls- Device and Media Disposal	Description: Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are in place remove ePHI from devices and media before disposal.
§164.310(d)(2)(ii)	Device and Media Controls- Media Re-Use	Description: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are in place remove ePHI from devices and media before they are re-used.
§164.310(d)(2)(iii)	Accountability - Asset Ownership and Location	Assign responsibility for recording and maintaining the movement of hardware and electronic media that contain ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - Solution requires Asset and device ownership to identify where assets containing ePHI are located. Designed to ensure that data is not exposed unintentionally.
§164.310(d)(2)(iv)	Device and Media Controls -Data Backup and Storage	Description: Create a retrievable exact copy of ePHI when needed before movement of equipment.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that an exact backup copy of ePHI is made before a device is moved.

§164.314(a)(1)	Business Associate Non-Compliance	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.
§164.314(a)(2)(i)	BA Information Security Controls	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.
§164.314(a)(2)(i)	BA Handling of ePHI	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.

§164.314(a)(2)(i)	BA Contracts and Statutory Obligations	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.
§164.314(b)(1)	Requirements for Group Health Plans	The Group Health Plan is required to ensure that the plan sponsor will reasonably and appropriately Safeguard ePHI created, received, maintained or transmitted.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that the plan sponsor has policies and procedures in place to appropriately protect ePHI received, maintained or transmitted to or by the plan.
§164.316(a)	Policy and Procedures	Implement policies and procedures to comply with the HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that reasonable and appropriate policies and procedures are in place to comply with the HIPAA Security Standard.
§164.316(b)(2)	Documentation Time Limit	Retain policies and procedures for 6 years from the data of its creation or the last date it was in effect.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are retained for 6 years from the date of its creation or the date it was last in effect.

§164.316(b)(2)	Documentation Availability	Ensure that documentation is available to the persons responsible for implementing the procedures.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are available to the person(s) responsible for implementing the procedures to which the documentation pertains.
§164.316(b)(2)	Documentation Updates	Review documentation periodically and update as needed in response to environmental or operational changes affecting the security of ePHI.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are reviewed and periodically updated as needed in response to environmental or operational changes that could affect the security of ePHI.

3.2 Safeguards Provided throughout the Reference Model

Of the remaining 23 Safeguard Areas in the current healthcare requirements, Verizon has further identified 8 Safeguards that call for universal security control requirements that are foundational across Cisco's products and present in all network devices and systems that make up Cisco's Healthcare Reference Architecture. The Safeguards deemed as universally applicable under this assessment are explained here and removed for additional detailed consideration.

Citation	Safeguard Title	Safeguard Description	Applicability of Technical Solutions to this Safeguard
164.308(a)(1)(i)	Security Management Process	Implement policies and procedures to prevent, detect, contain and correct security violations.	Cisco devices provide security to help an organization prevent, detect and contain security violations. When combining multiple devices in the design guide, multiple levels of security can be put in place to help an organization meet the security requirements of HIPAA.

§164.308(a)(5)(i)	Protection from Malicious Software (5)(ii)(B)	Ensure that appropriate protections against malicious software are in place.	Patch management and protection from malicious software is a hallmark of Cisco's vulnerability management process and services provided around all Cisco products. Cisco continually reviews potential network, systems and applications threat, attack vectors being used to attempt to penetrate network and systems services, assesses the applicability of these attacks to Cisco products, and, as warranted, issues software patches and improvements to continually stay in front of the impact of malicious software or attacks. Additionally, Cisco firewalls and routers provide network segmentation that can help contain malicious software to a network segment.
§164.308(a)(5)(i)	Password Management (5)(ii)(D)	Ensure that appropriate policies and procedures are in place to manage passwords for network access and access to sensitive data to ensure that passwords are strong enough to prevent them from being guessed or exposed to brute force attacks and processes are in place to manage and protect passwords from compromise or exposure.	Cisco systems and devices all use strong passwords in support of this requirement. Passwords can be configured for AES encryption during transit and in storage providing a higher layer of security and preventing password theft by physical compromise of the device. Administrator passwords can be set to match current industry accepted practices for length, complexity, history, lifetime, failed login attempts and can be authenticated using TACACS or Active Directory.
§164.308(a)(8)	Periodic Technical and Non-Technical Evaluation	Ensure that periodic technical (pen/vulnerability tests, etc.) and non-technical (policy/procedural, etc.) evaluations are occurring to continue to meet the regulatory security requirements and any changes in the environmental and operational that may affect sensitive (ePHI) data. To ensure that systems and networks are tested periodically to ensure that protections are still in place and working effectively.	Most Cisco systems and network devices included in the Healthcare Reference Model comply with generally accepted industry practices in the support of network and system testing and validation. Cisco routers and switches support SPAN and RSPAN for analyzing network traffic.
§164.312(a)(1)	Unique User Identification (a)(2)(i)	Ensure that each user who has access to sensitive (ePHI) data has a unique user id. Solution requires Identification controls.	Most Cisco applications, systems and devices support assigning unique user identifiers in support of this requirement. Unique Ids can be assigned to network users to access systems and applications and to network administrators to monitor and update the network infrastructure.

§164.312(a)(1)	Automatic Logoff (a)(2)(iii)	Ensure that policies, procedures and technical controls are in place to automatically logoff (terminate) a session after a predetermined period of inactivity.	Most Cisco applications, systems and devices support automatic logoff in support of this requirement. The time for session timeout can be configured based on policy requirements. Session timeout can vary by device or be configured for a universal timeout for all devices.
§164.312(d)	Person or Entity Authentication	Ensure that policies and procedures are in place to identify person or entity seeking access to sensitive (ePHI) data. Solution requires Authentication mechanisms.	Most Cisco applications, systems and devices support authentication in support of this requirement. Authentication can be Role-based authentication or Unique User Id accounts depending on the organizations policies, regulatory and business requirements.
§164.312(e)(1)	Integrity Controls (e)(2)(i)	Ensure that policies and procedures are in place to verify that data has not been altered or destroyed in an unauthorized manner during transmission. Solution requires signing of data or other integrity controls.	Cisco systems and devices use multiple forms of integrity monitoring to protect information from improper alteration or destruction of data at rest or in transit. Cisco devices support File-integrity monitoring or change- detection software on logs to ensure that existing log data cannot be changed without generating alerts. Integrity during transmission

4. Safeguard Mapping to Security Control Areas

In the remaining 15 Safeguard Areas in the current healthcare requirements, Verizon assessed the capability and capacity for Cisco's Healthcare Reference Model to support technically Direct Control that meet the intent of the Safeguard, or to provide Compensating Controls that, when implemented together in the Healthcare Reference Model, could support the fulfillment of the Safeguard; as a technology implementation that would in turn allow for a less complex operating procedure or management process to meet this Safeguard.

Verizon has identified the primary Physical, Network, System, and Application layer security controls that could be used to form a technical foundation of direct and compensating controls, for complying with the healthcare requirements. The breakdown of the remaining Safeguards into major control groups is as follows.

Control Group	Physical Security Controls	Network Security Controls	System Security Controls	Application Security Controls
PHY: Physical access, intrusion detection, and surveillance of users attempting to access or accessing physical network devices of systems containing or transporting ePHI. §164.310(a)(1) Access Control	• Electronic Access Controls • Intrusion Detection • Visual Surveillance			

IAM: Identification, Authentication, and Access Management controls for users and systems seeking access to ePHI across networks, systems, or applications. §164.308(a)(3)(i) Authorization and/or Supervision §164.308(a)(3)(i) Termination Procedures §164.308(a)(4)(i) Access Authorization §164.308(a)(4)(i) Access Est./ Modification	• Electronic Access Controls	• Network Access/ Authorization • Remote/ Wireless Access • Firewall/ • Segmentation • Encryption	• System Access/ • Authentication • Encryption • Backups	• Application Access/ Authentication • Logging/auditing • Encryption
LAM: Logging, Auditing, and Monitoring of users and systems attempting to access or accessing ePHI across networks, systems, or applications. §164.308(a)(1)(i) Information System Activity Review §164.308(a)(5)(i) Log-in Monitoring §164.308(a)(6)(i) Response and Reporting §164.312(b) Audit Controls	• Intrusion Detection • Visual Surveillance	• Network Access/ Authorization • Remote/ Wireless Access • Firewall Controls • Event Management • Activity Logging/Auditing • IDS/IPS	• System Access/ Authentication • Logging/Auditing • Encryption • IDS/IPS • Backups	• Application Access/ Authentication • Logging/auditing • Encryption

Control Group	Physical Security Controls	Network Security Controls	System Security Controls	Application Security Controls
E/D: Encryption/Decryption of data to protect ePHI while stored or in transit. §164.312(a)(1) Encryption / Decryption §164.312(c)(1) Data Integrity §164.312(e)(1) Encryption	•	• Network Layer Encryption	• System Layer Encryption	• Application Layer Encryption
EMO: Emergency Mode Operation control to allow granting of access to ePHI when need during emergency situations. §164.312(a)(2)(ii) Emergency Access	• Electronic Access Controls • Intrusion Detection • Visual Surveillance	• Network Access/ Authorization • Remote/ Wireless Access • Firewall • Segmentation • Event Management • Activity Logging/Auditing • IDS/IPS • Configuration Management	• System Access/ Authentication • Logging/Auditing • Encryption • IDS/IPS • Backups	• Application Access/ Authentication • Logging/auditing • Encryption

The table below provides a mapping of Safeguard into Physical, Network, System, and Application controls that, when used in combination, can fulfill the remaining 15 Safeguards and implementation of a low risk program to manage the protection of ePHI.

Type	Area	Citation	Title	Description	Direct Controls	Comp. Controls	Control Domain			
							Physical	Network	System	Application
	Security Management Process	§164.308(a)(1)(ii)(D)	Information System Activity Review	Implement procedures to regularly review records of information	Yes	Yes		Network, Remote, Wireless Access, network authentication,	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
	Workforce Security	§164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Implement procedures for the authorization	Yes	Yes	Electronic Access	Network, Remote, Wireless Access,	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
		§164.308(a)(3)(i)(C)	Termination Procedures	Implement procedures to terminate access to ePHI upon	No	Yes	Electronic Access	Network, Remote, Wireless Access, network	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
	Information Access Management	§164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions	If a health care clearinghouse is part of a larger organization, the clearinghouse	Yes	Yes		Network, Remote, Wireless Access, network authentication,	Access Control, Authentication	
		§164.308(a)(4)(i)(B)	Access Authorization	Implement policies and procedures for granting access to ePHI (for example, through access to a workstation, Transaction, program, or other mechanism).	Yes	Yes	Electronic Access	Network, Remote, Wireless Access, network authentication, FW	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
		§164.308(a)(4)(i)(C)	Access Establishment and Modification	Implement policies and procedures that authorize access to ePHI and modify or delete access when it is no longer needed.	Yes	Yes	Electronic Access	Network, Remote, Wireless Access, network authentication, FW	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
	Awareness and Training	§164.308(a)(5)(ii)(C)	Log-in Monitoring	Implement procedures for monitoring log-in attempts to ePHI and report	Yes	Yes		Network, Remote, Wireless Access, network authentication,	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
	Incident Procedures	§164.308(a)(6)(ii)	Response and Reporting	Establish and implement policies and procedures for responding to suspected or	No	Yes	Intrusion Detection, Visual Surveillance	Network, Remote, Wireless Access, network authentication, Event Mgt.,	Access Control, Authentication, Logging/Auditing, IDS/IPS	
Administrative	Contingency Plan	§164.308(a)(7)(i)(C)	Emergency Mode Operations	Establish and implement procedures to enable continuation of critical business processed for the protection of the security of ePHI in emergency mode.	No	Yes	Electronic Access, Intrusion Detection, Visual Surveillance	Network, Remote, Wireless Access, network authentication, FW, Segmentation, Config. Mgt	Access Control, Authentication, Backups	

Physical	Facility Access Controls	§164.310(a)(2)(iii)	Access Control and Validation Procedures	Description: Implement procedures to control and validate a person's access to facilities based on their role or function and control access to software programs for testing and revision.	Yes	Yes	Electronic Access, Intrusion Detection, Visual Surveillance			
Technical	Access Controls	§164.312(a)(2)(ii)	Emergency Access Procedures	Description: Design and implement procedures for securely accessing ePHI in	Yes	Yes		Network, Remote, Wireless Access, network authentication, FW,	Access Control, Authentication, Backups	Access Control, Authentication, Logging/Auditing
		§164.312(a)(2)(iv)	Encryption and decryption	Description: Implement a mechanism to encrypt and	Yes	Yes		Firewall, Encryption	Encryption	
	Audit Controls	§164.312(b)	Audit Controls	Description: Ensure that there is a mechanism in place to record and examine activity in systems that contain or use	Yes	Yes		Network, Remote, Wireless Access, network authentication, FW, Segmentation, Event Mgt.,	Access Control, Authentication, Logging/Auditing Backups IDS/IPS	
	Integrity	§164.312(c)(1)	Integrity	Description: Implement policies and procedures to protect ePHI from improper alteration or	Yes	Yes		Encryption	Access Control, Authentication, Logging/Auditing Backups IDS/IPS	
	Transmission Security	§164.312(e)(2)(ii)	Encryption	Description: Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Yes	Yes		Firewall, Encryption	Encryption	

5. Control Mapping to Cisco's Healthcare Reference Architecture

The applicability of Cisco's Reference Architecture to the healthcare requirements is shown as follows.

Domain Control	Control Description	Safeguards Assessed	Solution Components Reviewed
Physical Security Safeguards	Physical access, intrusion detection, and surveillance of users attempting to access or accessing physical network devices of systems containing or transporting ePHI	§164.308(a)(1)(i) Security Management Process §164.308(a)(3)(ii)(A) Authorization and/or Supervision §164.308(a)(4)(ii)(B) Access Authorization §164.308(a)(6)(ii) Response and Reporting §164.310(a)(1) Access Control	Cisco Physical Access Manager Cisco Physical Access Gateway

Administrative Safeguards	Supports access control at the network device level. Cisco devices have authentication on devices transiting the device and authentication on administrators configuring the device. IAM: Identification, Authentication, and Access Management controls for users and systems seeking access to ePHI across networks, systems, or applications. Supports access control at the System/Server levels. LAM: Logging, Auditing, and Monitoring of users and systems attempting to access or accessing ePHI across networks, systems, or applications.	§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	Server Vitalization—Servers - ISR SRE 900, UCS Express server ESXi Cisco Security Manager (CSM) Cisco Secure Access Control Server (ACS) Cisco Identity Services Engine (ISE) Ip Phone RSA Access Manager RSA Authentication Manager RSA Data Protection Manager RSA enVision HyTrust Cisco Prime Infrastructure VBlock—UCS - MDS - EMC SAN ASA Cisco Routers (ISR) Cisco Switches MDS Switch Fabric Cisco Wireless Cisco Security devices

Technical Safeguards	Supports independent protection of EPHI while at rest and in transit. E/D Common controls to protect data, independent of network or system layer. IAM: Identification, Authentication, and Access Management controls for users and systems seeking access to ePHI across networks, systems, or applications. Supports access control at the System/Server levels. Supports identifying anomalous activity in advance of more serious issues, and incident response. Supports data integrity and emergency operations	164.312(a)(2)(i) Unique User Identification 164.312(a)(2)(ii) Emergency Access Procedures 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	Server Vitalization—Servers - ISR SRE 900, UCS Express server ESXi Cisco Security Manager (CSM) Cisco Secure Access Control Server (ACS) Cisco Identity Services Engine (ISE) Ip Phone RSA Access Manager RSA Authentication Manager RSA Data Protection Manager RSA enVision HyTrust Cisco Prime Infrastructure VBlock—UCS - MDS - EMC SAN ASA Cisco Routers (ISR) Cisco Switches MDS Switch Fabric Cisco Wireless Cisco Security devices

6. Application of the Healthcare Reference Architecture

Cisco's Healthcare Reference architecture provides a robust networking core and infrastructure that can support a Customer's implementation of network security controls and system security controls as part of their security program and as required HIPAA-Required Risk Management process.

The architecture also provides both strong common security controls through network devices and security control and management systems that are highly Capable to support data security, and specific security management components that are directly Applicable to meet HIPAA safeguard' control requirements. Strong common controls include:

- Protection from Malicious Software (§164.308(a)(5)(i)).
- Password Management (§164.308(a)(5)(i))
- Periodic Technical and Non-Technical Evaluation (§164.312(a)(1))
- Unique User Identification (§164.312(a)(1))

- Automatic Logoff (§164.312(a)(1))
- Person or Entity Authentication (§164.312(d))
- Integrity Controls (§164.312(e)(1))

The fact that Cisco devices universally support the core security controls outlined in HIPAA safeguards, allows a customer to implement the reference architecture with the confidence that their resulting infrastructure will support HIPAA compliance from the outset, and with the knowledge that any additional use of Cisco's security management tools, will only enhance the protection of ePHI and further support Healthcare compliance.

Cisco's Healthcare Reference Architecture also provides directly applicable security control features and capabilities owing to the depth of security management tools provided in this model. Directly Applicable control include:

- **Physical Access Control, Intrusion Detection, and Visual Surveillance.** Cisco's Physical Access Manager and Physical Access Gateway products provide the control structure for to use electronic access controls, intrusion detection, and visual surveillance components to control physical access to a wide range of healthcare facilities from landlord closets housing Clinic IT equipment in leasing situations, to the control of physical security at remote and co-located Clinics, to the development and integration of remote facilities into Hospital physical security systems.
- **Network Access and Authentication Controls for wired, wireless, and remote Networks**. Cisco's Reference architecture provides for network access control and authentication of both users and systems operating on wired WAN/LANs, access wireless networks, and access Customer networks remotely, in a seamless approach that supports multiple HIPAA safeguard requirements for Identify Management, Access Controls, user and system authorization, and authentication.
- **Network Segmentation, Segregation, and Isolation Capabilities**. Cisco's healthcare reference architecture provide unsurpassed capability to deliver fine grained control over the ability of a user on a clinical or administrative workstation, on a medical device, or administrative console to have network access to systems, servers, and storage devices that contain ePHI. Cisco's architecture allow a Customer to develop and maintain segmentation between administrative and clinical systems, to structure sub-networks for only administrative workstations, medical devices, server farms, and publicly-facing web servers. Customers can establish and maintain user and system segregation by their role/function within Clinics and Hospitals, and Customers can demonstrate isolation of EPHI-containing systems/storage as a part of their overall ePHI protection strategy. Customer can meet HIPAA's clearinghouse isolation requirements. Customers can plan for and execute emergency rerouting and access strategies to support continued operations during natural disasters, in order to maintain patient data security while support emergency care. Customers can ensure that workforce members are granted access based on their role in the institution, and can also terminate access at the network level to support HIPAA's Sanction/Termination requirements.
- **Logging, Auditing, and Monitoring Capabilities**. Cisco's Healthcare Reference Architecture also provides robust and well managed logging capabilities, support routine and event-driven authoring, support continuous monitoring of the network and system environment for control, and provides the ability to investigate and interrogate devices as needed in support of data breach events. The Reference Architecture supports HIPAA's Information System Activity Review requirements by providing an infrastructure to log, audit, and monitor network and system behavior and support the tracking of user and system access or patient information. While used as part of a total activity review strategy, Cisco's Security Manager, Identity Service Engine, and Suite of RSA products, for a solid platform for developing a total activity review and control solution. Cisco' Reference Architecture provide the centralized logging capabilities and auditing features to support effective audit of ePHI controls by Customer's security team, internal auditors, external auditors, and regulators. Cisco's suite of IDS/IPS products in the Reference Architecture provide the Customer with ab alerting foundation to support the "Response and Reporting" Safeguard requirements.

- **Encryption of ePHI**. Cisco's reference architecture allows Customers to realize the substantial security control that can be exerted through ePHI encryption while at rest and in transit to further protect ePHI when application layer security control might fail or be bypassed, or when operational errors inadvertently release patient information or lose track of servers containing ePHI. The reference architecture core and vBlock products support seamless data encryption and decryption on the fly, without the traditional performance concerns. The reference architecture also support HIPAA's data integrity requirements, protecting ePHI from "improper alteration" while stored or while in transit across private and public networks.

7. Appendix

Healthcare Security Requirements

Standards	Sections	Implementation Specifications R=Required, (A)=Addressable	Type
Security Standards: General Rules			
Security Standards: General Rules	§164.306	Security Standards General Rules	R
Administrative Safeguards			
Security Management Process	§164.308(a)(1)	Security Management Process	R
	§164.308(a)(1)(ii)(A)	Risk Analysis	R
	§164.308(a)(1)(ii)(B)	Risk Management	R
	§164.308(a)(1)(ii)(C)	Sanction Policy	R
	§164.308(a)(1)(ii)(D)	Information System Activity Review	R
Assigned Security Responsibility	§164.308(a)(2)	Assigned Security Responsibility	R
Workforce Security	§164.308(a)(3)(i)	Workforce Security	R
	§164.308(a)(3)(i)(A)	Authorization and/or Supervision	A
	§164.308(a)(3)(i)(B)	Workforce Clearance Procedures	A
	§164.308(a)(3)(i)(C)	Termination Procedures	A
Information Access Management	§164.308(a)(4)(i)	Information Access Management	R
	§164.308(a)(4)(i)(A)	Isolating Healthcare Clearinghouse Functions	R
	§164.308(a)(4)(i)(B)	Access Authorization	A
	§164.308(a)(4)(i)(C)	Access Establishment and Modification	A
Security Awareness and Training	§164.308(a)(5)(i)	Security Awareness and Training	R
	§164.308(a)(5)(i)(A)	Security Reminders	A
	§164.308(a)(5)(i)(B)	Protection from Malicious Software	A
	§164.308(a)(5)(i)(C)	Log-in Monitoring	A
	§164.308(a)(5)(i)(D)	Password Management	A

Security Incident Procedures	§164.308(a)(6)(i)	Security Incident Procedures	R
	§164.308(a)(6)(ii)	Response and Reporting	R
Contingency Planning	§164.308(a)(7)(i)	Contingency Plan	R
	§164.308(a)(7)(i)(A)	Data Backup Plan	R
	§164.308(a)(7)(i)(B)	Disaster Recovery Plan	R
	§164.308(a)(7)(i)(C)	Emergency Mode Operation Plan	R
	§164.308(a)(7)(i)(D)	Testing and Revision Procedures	A
	§164.308(a)(7)(i)(E)	Applications and Data Criticality Analysis	A
Evaluation	§164.308(a)(8)	Evaluation	R
BA Contracts and Other Arrangements	§164.308(b)(1)	BA Contracts and other arrangements	R
	§164.308(b)(2)	BA Exceptions	R
	§164.308(b)(3)	Satisfactory Assurances under b2	R
	§164.308(b)(4)	Satisfactory Assurances under b1	R

Physical Safeguards			
Facility Access Controls	§164.310(a)(1)	Facility Access Controls	R
	§164.310(a)(2)(i)	Contingency Operations	A
	§164.310(a)(2)(ii)	Facility Security Plan	A
	§164.310(a)(2)(iii)	Access Control and Validation Procedures	A
	§164.310(a)(2)(iv)	Maintenance Records	A
Workstation Use	§164.310(b)	Workstation Use	R
Workstation Security	§164.310(c)	Workstation Security	R
Device and Media Controls	§164.310(d)(1)	Device and Media Controls	R
	§164.310(d)(2)(i)	Disposal	R
	§164.310(d)(2)(ii)	Media Re-use	R
	§164.310(d)(2)(ii)	Accountability	A
	§164.310(d)(2)(iv)	Data Backup and Storage	A
Technical Safeguards			
Access Control	§164.312(a)(1)	Access Control	R
	§164.312(a)(2)(i)	Unique User Identification	R
	§164.312(a)(2)(ii)	Emergency Access Procedure	R
	§164.312(a)(2)(iii)	Automatic Logoff	A
	§164.312(a)(2)(iv)	Encryption and Decryption	A
Audit Controls	§164.312(b)	Audit Controls	R
Integrity	§164.312(c)(1)	Integrity	R
	§164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	A
Authentication	§164.312(d)	Person or Entity Authentication	R

Transmission Security	§164.312(e)(1)	Transmission Security	R
	§164.312(e)(2)(i)	Integrity Controls	A
	§164.312(e)(2)(ii)	Encryption	A
Organizational Requirements			
BA Contracts and Other Arrangements	§164.314(a)(1)(i)	Business Associate Contracts and Other Arrangements	R
	§164.314(a)(2)(i)(A)	Business Associate Compliance	R
	§164.314(a)(2)(i)(B)	BA Subcontractor Compliance	R
	§164.314(a)(2)(i)(C)	BA Security Incident Reporting	R
	§164.314(a)(2)(ii)	Other Arrangements	R
	§164.314(a)(2)(iii)	Other Arrangements Subcontractor Compliance	R
Requirements for Group Health Plans	§164.314(b)(1)	Requirements for Group Health Plans	R
	§164.314(b)(2)(i)	BA Information Security Controls	R
	§164.314(b)(2)(ii)	Separation of GHP and sponsor	R
	§164.314(b)(2)(iii)	Ensure Agents implement security	R
	§164.314(b)(2)(iv)	Report incidents to group health plan	R
Policies and Procedures and Documentation Requirements			
Policies and Procedures and Documentation Requirements	§164.316(a)	Maintaining Policy and Procedures	R
	§164.316(b)(1)(i)	Written Policy and Procedures	R
	§164.316(b)(1)(ii)	Written Record of Risk Management	R
	§164.316(b)(2)(i)	Documentation Time Limit	R
	§164.316(b)(2)(ii)	Documentation Availability	R
	§164.316(b)(2)(iii)	Documentation Updates	R

List of Interviews

The following members of the Cisco Architecture Team were interviewed as part of the PCI Assessment. The results from the PCI Assessment were used as a direct reference for the HIPAA Assessment.

Interviewee(s)	Title
Christian Janoff, Bart McGlothin	Network architecture, firewalls, routers, switches, wireless, IDS/IPS, Audit Logging, Access Control / Authentication, CSM, Wireless, LMS, Cisco Virtual Service Gateway, ASA
Sai Balabhadrapatruni	ASA, Cisco IPS
Jamey Heary	Cisco ISE
Raju Satyan	Cisco Prime LMS with Pari Compliance Module
Tom Hua	CSM
Sheri Spence	EMC SAN
Syed Ghayur	Nexus 1kv
Mike Adler, Sujit Ghosh	Wireless lab
K. Sigel, R. Budko	HyTrust

Syed Ghayur	Cisco Virtual Service Gateway
Pandit Panburana, Mourad Cherfaoui	CUCM
Rupesh Chakkingal, David Valiquette	RSA Data Protection Manager
Danny Dhillon	RSA enVision, RSA Authentication Manager, RSA Data Protection Manager, RSA Access Manager, RSA Authentication Manager

List of Documents

The following documents were reviewed as part of the PCI Assessment. The results of the PCI Assessment were used as a direct reference for the HIPAA Assessment.

Document	Date
Enterprise Retail PCI DSS 2.0 pdf	11/17/2010
Switch and router configs	4/15/2011
Switch configs - branches	4/15/2011
Common requirements questions across all devices.xls	12/01/2010
Products Alignment_2010-10-13.xlsx	10/13/2010
PCI Retail Solution Products.xlsx	04/15/2011
ASA, router, ACE Load Balancer, and IPS configurations	11/12/2012
Compliance_LAB_Diagram_2012-12-03 - Internet Edge Page.pdf	12/06/2012
20121130 PCI DSS and IPv6.docx	11/30/2012
LMS and Pari_DIG Revision_2012-11-11.docx	11/12/2012
Lab_IP_Addressing_and_Consoles.xlsx	11/12/2012
Cisco ISE at a glance	11/30/2012
Cisco ISE Data Sheet	11/30/2012