HIPAA Compliance: Delivering Privacy and Security for ePHI with a Business-driven SD-WAN

HIPAA: Privacy and Security for Healthcare

The Healthcare Insurance Portability and Accountability Act (HIPAA) was passed in 1996. Its primary goals were to modernize the flow of healthcare information and to ensure the security and privacy of electronic protected health information (ePHI). Strengthened by the HITECH act in 2009 and updated in 2013, HIPAA mandates technical, physical and administrative safeguards that must be implemented to control access to health-related information.

HIPAA regulations apply to a broad range of organizations that handle ePHI including healthcare providers such as hospitals and physicians' offices, healthcare clinics, health plans and healthcare clearinghouses, and "business associates" (entities that process or transmit protected information for purposes like claims processing, data analysis, accounting, and legal services). Its requirements influence a wide variety of applications and systems, including electronic health records (EHR), computerized physician order entry (CPOE), radiology, pharmacy, laboratory, and claims processing systems.

HIPAA violations can result in fines of up to $1.5 million from the U.S. Department of Health and Human Services (HHS), lawsuits from state attorneys general, and severe damage to the reputations of healthcare institutions and their business partners.

HIPAA requirements are not technology standards in the sense of IEEE standards for networking or W3C standards for web technologies. They do not mandate specific product features, or protocols, or APIs. Instead, they describe general outcomes ("ensure the confidentiality, integrity, and availability of all electronic protected health information") or technology goals ("implement a mechanism to encrypt and decrypt electronic protected health information").

What is HIPAA Compliance?

HIPAA requirements are not technology standards in the sense of IEEE standards for networking or W3C standards for web technologies. They do not mandate specific product features, or protocols, or APIs. Instead, they describe general outcomes ("ensure the confidentiality, integrity, and availability of all electronic protected health information") or technology goals ("implement a mechanism to encrypt and decrypt electronic protected health information"). As a result, organizations can be HIPAA compliant (or non-compliant), but technology products and services themselves cannot be.

> *Network and security products cannot be "HIPAA compliant" themselves, but they can help organizations maintain HIPAA compliance.*

The HIPAA regulations at CFR Part 164 delineate general standards for security and privacy, for example saying that covered entities and business associates must "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." These general standards are then operationalized in a series of more detailed safeguards (section §164.308), physical safeguards (section §164.310), technical safeguards (section §164.312), and requirements related to the organization (section §164.314) and to policies and procedures and documentation (section §164.316).

How the Silver Peak Unity EdgeConnect SD-WAN Platform Helps Healthcare Providers Maintain HIPAA Compliance

The Silver Peak Unity EdgeConnect™ Software Defined WAN (SD-WAN) edge platform can transform the network into a business accelerant rather than a constraint. One example of this is how EdgeConnect can help organizations achieve and maintain HIPAA compliance with less effort by combining the power of zone-based firewalls, network micro-segmentation, WAN optimization, routing, and application visibility and control.

1. Access Control and Management

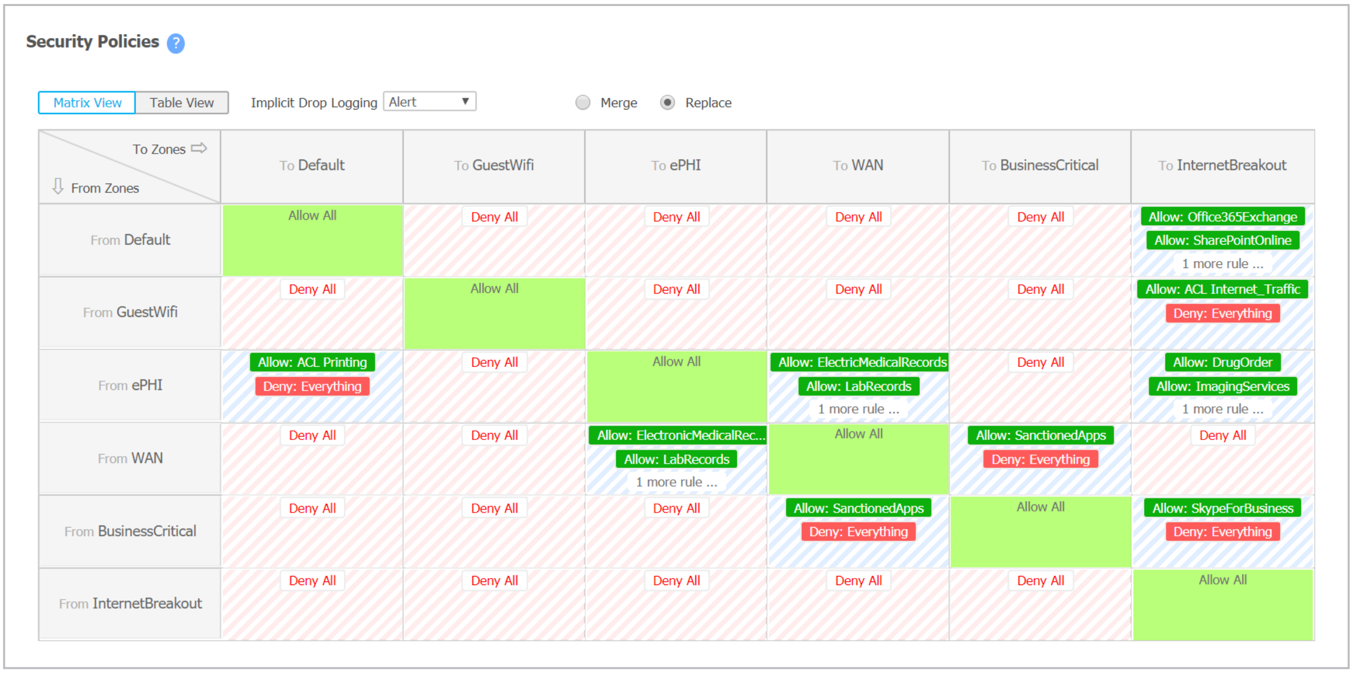
HIPAA safeguards related to access control and management include **§164.308(a)(4)(i)** *Administrative safeguards: Information access management*; **§164.312(a)(1)** *Technical safeguards: Access control*; and **§164.502(b)(1)** *Privacy — Uses and disclosures of protected health information: Minimum necessary applies*. These focus on policies, procedures, and technology to limit access to PHI to authorized people and software programs.

EdgeConnect SD-WAN zone-based firewall capabilities can keep attackers and malicious outsiders out and help prevent violations of privacy policies by unauthorized insiders. Administrators can create zones, assign applications to them, and create unique security policies that control access between and across zones. The policies can completely block access, allow traffic in one direction only, or restrict inter-zone traffic to specific uses.

For example, applications that handle ePHI can be assigned to protected zones. Access into these zones can be restricted to other protected zones, and access out can be limited to other protected zones and a printer on the main corporate network.

> *The EdgeConnect zone-based firewall features dramatically simplify network segmentation and can restrict access to systems that handle ePHI.*

A security policy configuration matrix (Figure 1) makes the segmentation rules easy to understand and manage. The SD-WAN platform orchestrates policy updates automatically, so administrators don't have to modify and test policies on individual devices when the underlying infrastructure changes.



Security Policies ?

Matrix View | Table View   Implicit Drop Logging: Alert ▼   ○ Merge   ● Replace

To Zones ⇨ ⇩ From Zones	To Default	To GuestWifi	To ePHI	To WAN	To BusinessCritical	To InternetBreakout
From Default	Allow All	Deny All	Deny All	Deny All	Deny All	Allow: Office365Exchange Allow: SharePointOnline 1 more rule ...
From GuestWifi	Deny All	Allow All	Deny All	Deny All	Deny All	Allow: ACL Internet_Traffic Deny: Everything
From ePHI	Allow: ACL Printing Deny: Everything	Deny All	Allow All	Allow: ElectricMedicalRecords Allow: LabRecords 1 more rule ...	Deny All	Allow: DrugOrder Allow: ImagingServices 1 more rule ...
From WAN	Deny All	Deny All	Allow: ElectronicMedicalRec... Allow: LabRecords 1 more rule ...	Allow All	Allow: SanctionedApps Deny: Everything	Deny All
From BusinessCritical	Deny All	Deny All	Deny All	Allow: SanctionedApps Deny: Everything	Allow All	Allow: SkypeForBusiness Deny: Everything
From InternetBreakout	Deny All	Deny All	Deny All	Deny All	Deny All	Allow All

Figure 1: A security policy configuration matrix makes it easy to create and manage intra-zone segmentation rules

EdgeConnect also enables organizations to create application-specific end-to-end segments spanning LAN, WAN, and data center zones. Each zone can have unique security policies and quality of service (QoS) parameters. For example, if an electronic health records system on a LAN in a remote office is connected through broadband links to a server in a data center, all data transmitted through this logical zone could be protected by the highest levels of encryption (Figure 2). In addition, traffic in this zone can be given priority over other applications that share the same infrastructure.

2. Encryption and Transmission Security

HIPAA safeguards related to encryption and transmission security include **§164.312(a)(2)(iv)** *Technical safeguards: Encryption and decryption*; **§164.312(e)(1)** *Technical safeguards: Transmission security*; and **§164.312(e)(2)(i)** *Technical safeguards: Integrity controls*. These addressable standards provide that ePHI should be encrypted, and that technical security measures guard against unauthorized access or modification of ePHI when it is being transmitted over a network.

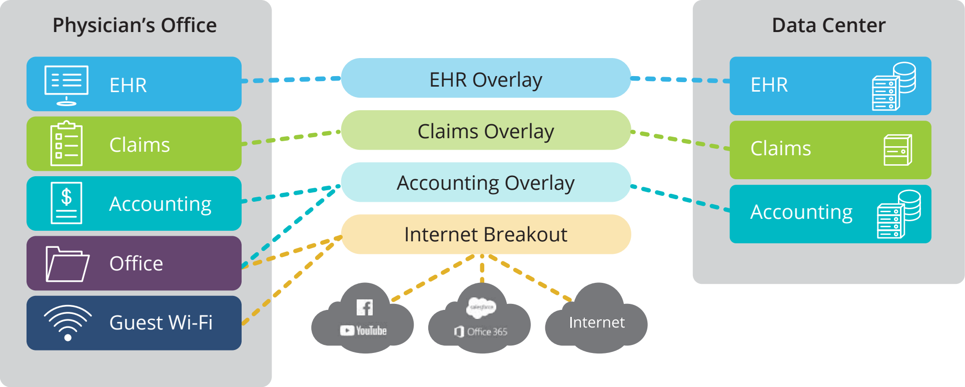


Figure 2: End-to-end segmentation: application-specific overlays can have unique security and QoS policies

The EdgeConnect SD-WAN platform can ensure that ePHI traffic is fully encrypted using NIS-recommended cryptography algorithms and security protocols (including IPsec tunnels with 256-bit AES encryption) as it travels across the wide area network.

Data integrity is assured as well. Automatic key rotation and integral message authentication prevent "data in motion" from being improperly modified without detection. SHA2 hashing is supported for message authentication.

> *Network traffic that contains ePHI is fully encrypted; data remains secure and cannot be improperly modified.*

3. Protection from Malicious Software

HIPAA includes a safeguard **§164.308(a)(5)(ii)(B)** *Administrative safeguards: Protection from malicious software* that mandates procedures for detecting and reporting malicious software.

EdgeConnect is a hardened appliance using out-of-the-box "harden" factory default mode. This approach ensures utmost security for appliances plugged in for the first time. Subsequently, on zero touch provisioning and configuration, a strong password per standard FIPS 140-2 guidelines is always enforced on the appliance. This prevents malware from using default passwords to gain unauthorized access to the appliance. Apart from the default security posture, for continuous traffic inspection, EdgeConnect SD-WAN with First-packet iQ™ application classification can identify applications and web domains based on the first packet in a session and steer traffic that contains ePHI and other sensitive information to next-generation firewalls, secure web gateways, anti-malware tools, sandboxing products, and other advanced security services. A simple drag-and-drop interface makes it easy to assign policies to traffic from specific applications and to route the traffic to specific tools located in the same facility, at a headquarters data center, or in the cloud (Figure 3).

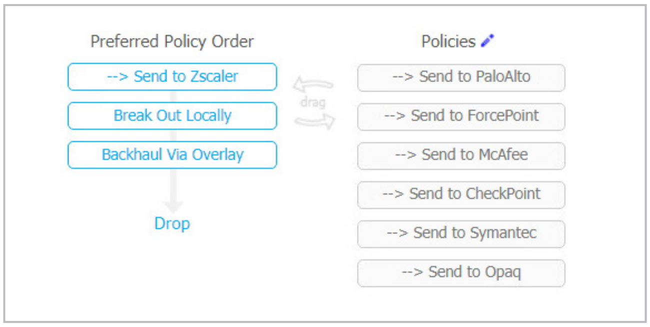


Figure 3: A drag-and-drop interface makes it easy to send traffic containing ePHI to local, remote, and cloud-based products from industry-leading security companies

4. Logging and Audits

HIPAA safeguards related to logging and audits include **§164.308(a)(6)(ii)** *Administrative safeguards: Response and reporting*; and **§164.312(b)** *Technical safeguards: Audit controls*. These require organizations to identify and respond to security incidents and to record and examine activity in information systems that use ePHI.

The EdgeConnect SD-WAN platform captures deny, accept, and drop events related to traffic sessions, as well as reasons for those events. This information can be sent in syslog message format to logging tools, SIEMS, and security analytics tools, to help analysts identify and respond to security incidents (and also to troubleshoot network and application problems that affect performance and availability).

5. Availability

HIPAA includes a general standard, **§164.306(a)(1)** *General Rules* and safeguards such as **§164.308(a)(1)(ii)(A)** *Administrative safeguards: Risk analysis* that obligate covered entities and business associates to ensure the confidentiality, integrity, and availability of ePHI that they create, receive, and transmit.

EdgeConnect offers many capabilities that enhance application performance and availability. These include:

- **DDoS protection:** Detecting distributed denial-of-service attacks and dynamically routing traffic over unaffected network links
- **Dynamic path selection:** Monitoring the performance of WAN connections and routing traffic around paths with performance issues

- **WAN optimization:** Increasing WAN performance through techniques such as application and protocol acceleration, data deduplication, and data compression

- **Traffic shaping:** Dynamically routing high-priority traffic (such as traffic containing ePHI) over the best-performing links

- **Path conditioning**: Increasing the effective bandwidth of broadband connections through techniques such as forward error correction (FEC) and packet order correction (POC)

- **High availability (HA) clusters:** Protecting against device failures through device and circuit-level redundancy

- **Real-time visibility into network health and application performance:** A dashboard with a network-wide health map, loss, jitter, and latency charts, alarms, bandwidth consumption charts, and other tools to troubleshoot network and application issues

6. Cost and Ease of Management

Cost and ease of management are not discussed explicitly in the HIPAA regulations, but obviously IT organizations can only deploy HIPAA controls if the cost and management efforts are within their reach. The Silver Peak EdgeConnect platform can be deployed can be deployed quickly and managed easily through capabilities such as zero-touch deployment for appliances at remote sites, automated policy orchestration, and single-pane-of-glass monitoring and reporting for all Silver Peak appliances.

The Silver Peak EdgeConnect SD-WAN Security Advantage

HIPAA compliance puts a lot of demands on covered entities and "business associates." The Silver Peak Unity EdgeConnect SD-WAN edge platform uniquely helps to address the critical compliance areas covered in this document.

Capabilities include end-to-end network segmentation to minimize the exposure of ePHI to unauthorized users and systems, the enforcement of strong encryption of data in motion, traffic steering and service chaining to ensure that traffic is scanned for malware by industry-leading security products, the capture of network events for logging and analysis, and a long list of features for ensuring high availability and performance in the face of attacks and network issues.

In addition to simplifying HIPAA compliance, the EdgeConnect SD-WAN platform creates networks that are business-driven, where network resources are deployed to match the business priority of every application. The results include the highest quality of experience for employees and the patients they serve, improved network visibility and simplified management for IT and network organizations, and increased business agility and lower costs for the enterprise.

Company Address

Silver Peak Systems, Inc
2860 De La Cruz Blvd.
Santa Clara, CA 95050

Phone & Fax

Phone: +1 888 598 7325
Local: +1 408 935 1800

Online

Email: info@silver-peak.com
Website: www.silver-peak.com