SOLUTION OVERVIEW

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 ARUBA EDGECONNECT ENTERPRISE HELPS HEALTHCARE PROVIDERS MAINTAIN HIPAA COMPLIANCE

Aruba EdgeConnect Enterprise 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 next-generation 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
- §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.

Aruba EdgeConnect Enterprise next-generation firewall capabilities can keep attackers and malicious outsiders out and help prevent violations of privacy policies by unauthorized insiders.

Coupled with Aruba ClearPass Policy Manager, EdgeConnect enforces a zero-trust architecture that dynamically segments the network and applies least privileged access principles. It ensures that users and devices only communicate with destinations consistent with their role based on identity, access rights, and security posture.

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 interzone 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 next-generation 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.

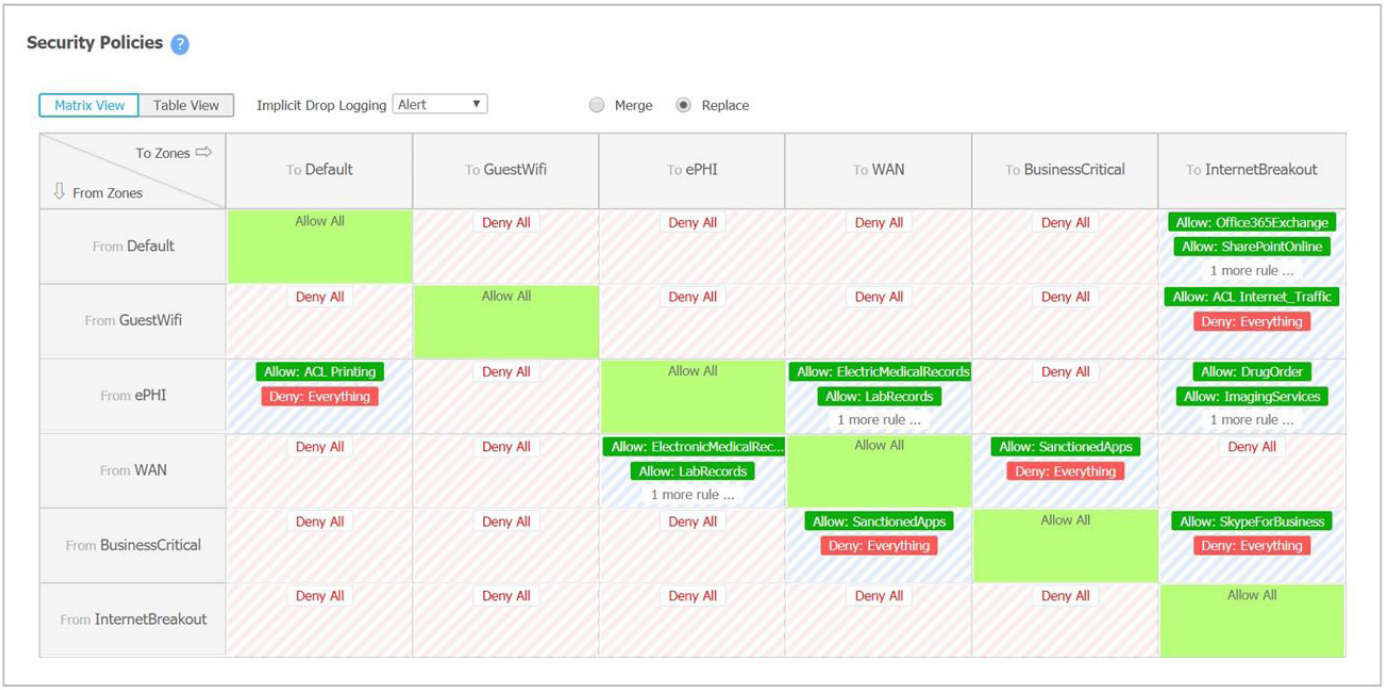

Figure 1: A security policy configuration matrix makes it easy to create and manage intra-zone segmentation rules

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.

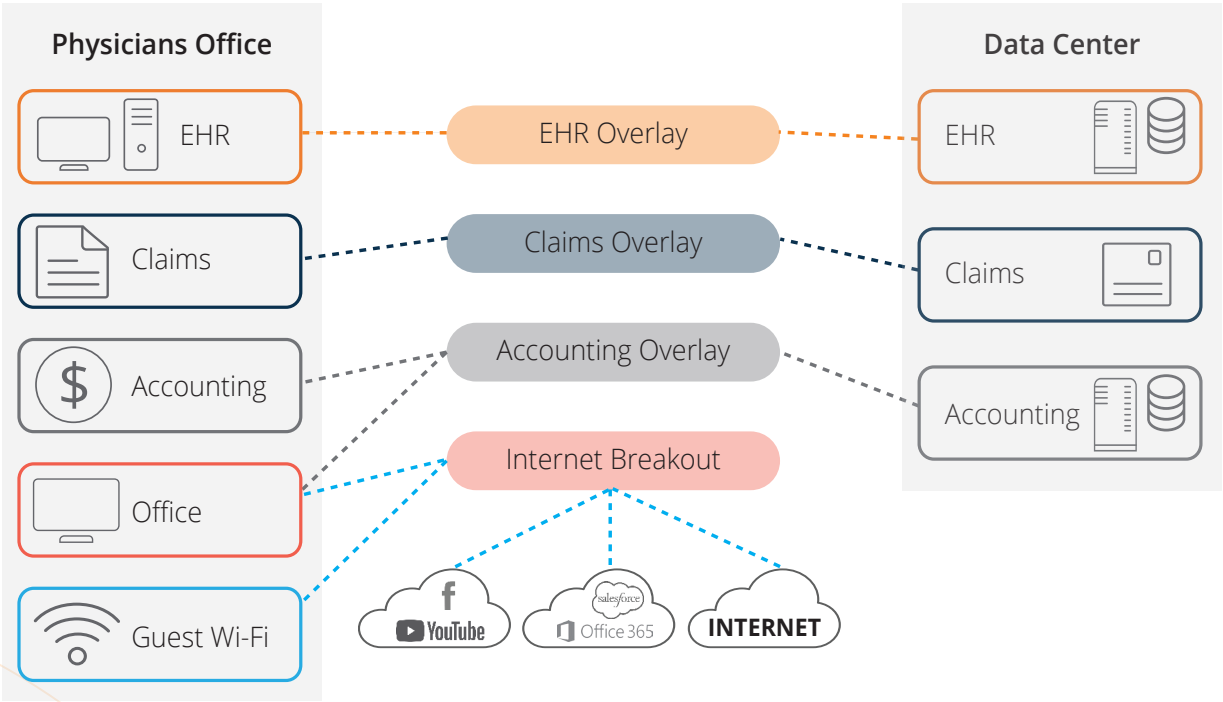

Figure 2: End-to-end segmentation: application-specific overlays can have unique security and QoS policies

With users accessing sensitive data in the cloud from anywhere and from any device, it has become critical for healthcare providers to integrate SSE (Security Service Edge) capabilities such as ZTNA (Zero-Trust Network Access), CASB (Cloud Access Security Broker), SWG (Secure Web Gateway) and DLP (Data Loss Prevention) with advanced SD-WAN capabilities to build a robust SASE (Secure Access Service Edge) architecture and comply with HIPAA requirements.

Aruba EdgeConnect Enterprise is tightly integrated with multiple cloud security vendors delivering a best-of-breed SASE architecture. The integration is completely automated, accelerating HIPAA compliance.

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
- §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.

The Aruba EdgeConnect 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.

Aruba EdgeConnect Enterprise has earned the ICSA Labs Secure SD-WAN certification based on a comprehensive and robust set of SD-WAN functionality and platform security requirements.

ICSA Labs Secure SD-WAN certification requirements include:

- **Advanced SD-WAN features** such as tunnel bonding, dynamic path selection and zero-touch provisioning
- **Native support (or via service chaining) for advanced security** functions such as anti-malware, intrusion prevention and DoS protection
- **Encryption** of sensitive data, as well as administrative and operational communications
- **Policy enforcements** for both WAN-specific functions and security policies
- **Security events logging**

The Aruba EdgeConnect next-generation firewall provides advanced DDoS protection capabilities. The solution detects abnormal network behavior and attacks such as protocol attacks, ICMP floods, SYN floods, IP spoofing attacks and more.

Using firewall Protection Profiles, the solution limits the number of requests using actions such as rapid aging, drop excess, and block source. Actions are based on preset or configurable DoS thresholds (min and max value) set for traffic parameters including flow rate, concurrent flows, and embryonic flows. The solution can also dynamically route the traffic over unaffected network links in case of a DDoS attack ensuring business continuity

Additionally, Aruba EdgeConnect provides intrusion detection and prevention capabilities (IDS/IPS) to monitor, flag, and drop traffic in case of a security threat. Intrusion detection and prevention is based on threat signatures and utilizes the common Aruba UTM framework. It is integrated with the next-generation firewall enabling application-level selection for inspection providing actions such as Drop, Inspect, and Allow traffic.

Threat events are then streamed to Security Information and Event Management (SIEM) systems for log review.

Apart from the default security features embedded in the solution, Aruba EdgeConnect Enterprise enables health care providers to build a best-of-breed SASE architecture. Thanks to a tight integration with industry leading security vendors such as Zscaler and Netskope, the First-packet iQ™ application classification feature identify applications and web domains based on the first packet and steer traffic that contains ePHI and other sensitive information to advanced security services such as secure web gateways, anti-malware tools and sandboxing products.

4. Logging and Audits

HIPAA safeguards related to logging and audits include:

- §164.308(a)(6)(ii) Administrative safeguards: Response and reporting
- §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.

Aruba EdgeConnect Enterprise 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, SIEM solutions, 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).

The Aruba EdgeConnect Security App for Splunk, a leader in the SIEM space, provides a dashboard view of all security event notifications exported from EdgeConnect devices within an enterprise's SD-WAN. Healthcare providers can easily configure EdgeConnect to forward all security event notifications to Splunk, centralizing logging, visualization, and analysis of security events alongside other telemetry or network events. From Splunk, users can filter, sort, navigate and view the collective security event notifications generated across the entire SD-WAN fabric, overall trends, and top talkers to help them pinpoint network events that require further investigation.

Figure 3: Splunk security dashboard

5. Availability

HIPAA safeguards related to availability include:

- §164.306(a)(1) Security standards: General rules: General requirements
- §164.308(a) (1)(ii)(A) Administrative safeguards: Risk analysis

These standards obligate covered entities and business associates to ensure the confidentiality, integrity, and availability of ePHI that they create, receive, and transmit.

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

- 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 networkwide health map, loss, jitter, and latency chart, 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. Aruba EdgeConnect Enterprise 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 EdgeConnect appliances.

THE ARUBA EDGECONNECT SECURITY ADVANTAGE

HIPAA compliance puts a lot of demands on covered entities and "business associates." Aruba EdgeConnect Enterprise 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 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

SO_HIPAACompliance_RVK_080422 a00119353enw