VMware SD-WAN
Healthcare Industry Privacy Supplement for HIPAA

Protecting what matters: You!

This datasheet supplements the VMware SD-WAN datasheet, which explains VMware’s privacy program in more detail.

Healthcare Industry Customers
VMware understands some of our customers may be subject to the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations as a covered entity or business associate. HIPAA sets forth standards to protect the confidentiality, integrity, and availability of individuals’ protected health information (PHI) that is collected, stored, and processed by healthcare institutions and other covered entities governed by HIPAA. With more medical professionals leveraging technologies to interact and collaborate on patient concerns, it is important for organizations to address HIPAA compliance in their use of technology. VMware SD-WAN facilitates healthcare providers’ HIPAA compliance by allowing them to customize settings in ways that align with their outcomes and technology goals.

Technical Safeguards
Under HIPAA, customers have various security obligations with respect to electronic PHI (ePHI). VMware SD-WAN includes a number of features and functionalities that customers can incorporate into their security compliance program to safeguard their data.

Access Controls
- Accounts are password protected and accessed via Transport Layer Security (TLS)
- 99.99 percent uptime service-level agreement, with 24x7 automated failure detection

Audit Controls
- Audit controls provide logs, metadata, and network performance metrics, along with firewall and audit logs for activity monitoring and recording
- Granular user role-based access controls and policy framework help to manage third-party access
- Firewall rules capture denied, allowed, and rejected events related to traffic sessions as well as reasons for these events
- Harden Internet connectivity with Layer 7 application-aware stateful firewall. The Stateful firewall feature provides the following benefits:
  - Prevent attacks such as denial of service (DoS) and spoofing
  - More robust logging
  - Improved network security
Person or Entity Authentication
- VMware SD-WAN Edges support user authentication against Radius server for wired access and 802.1x (WPA2-Enterprise) authentication for wireless access before they are allowed to connect to the secure network environment.
- 802.1x (WPA2-Enterprise) wireless access control and Radius user authentication are used for wired access control.

Transmission Security
- The VMware SD-WAN solution provides strong cryptography and secure protocols to secure both wired and wireless transmission of all network data. The VMware SD-WAN Edge uses standards-based IKE for key management and IPsec for encryption. Authentication is done through device certificates anchored to a trusted CA. The VMware SD-WAN solution also offers customers FIPS 140-2 compliant IPsec tunneling. All communication from one VMware SD-WAN Edge to another is encrypted using AES 256 encryption and integrity protected with SHA256. Network ports are locked down to a minimum with packets to closed ports silently discarded.
- Provides the ability for the covered entity to configure end-to-end segmentation, enabling isolation of the PHI data environment from the rest of the network.
- Application-aware firewall controls traffic allowed between internal networks and untrusted networks, as well as traffic into and out of more sensitive areas within a company’s internal trusted network.
- All data transmission traversing our SD-WAN is encrypted with Advanced Encryption Standard (AES) 256-bit encryption, in line with the guidelines laid out by NIST for IT security.
- The VMware SD-WAN Edges protect the privacy and integrity of the electronic PHI traffic with Advanced Encryption Standard (AES) 256-bit encryption.
- VPN tunnels are set up using PKI authentication to maximize security and prevent man-in-the-middle attacks.

VMware SD-WAN facilitates transmission of customer data by monitoring and steering traffic, without ever accessing customer network payload information. The VMware SD-WAN Gateways act as a conduit for customer data by transmitting the customer’s data to the destination. No customer data is stored (i.e., written to hard drive or SSD) on the VMware SD-WAN Gateway.

Any storage of customer data is only temporary and transient in nature to optimize data transmission. Envelope metadata is the only data that is stored by VMware SD-WAN, for purposes of querying and alerts for approximately two weeks. The VMware SD-WAN Services do not require any health-related information in order to provide the services, and envelope metadata should not include PHI.

About VMware SD-WAN
VMware SD-WAN simplifies branch WAN, and in a COVID-19 Era, Work from Home networking by automating deployment and improving performance over private, broadband Internet, and LTE links for today’s increasingly distributed enterprises. VMware SD-WAN includes: a choice of public, private or hybrid cloud network for enterprise-grade connection to cloud and enterprise applications; branch office enterprise appliances and optional data center appliances; software-defined control and automation; and virtual services delivery. Learn more at sdwan.vmware.com or see the VMware SD-WAN Service Description.