Authors: Sean Caragata, Barbara Casey, Forrest Foster, Matt Fussa, Deepa Mahendraker, Andy Russ

HIPAA Compliance: Trust Cisco Webex services including Cisco Webex Teams, Cisco Webex Meetings, Cisco Webex Control Hub, Cisco Webex for Developers to secure your Data. For the rest of the document, we will refer to the services described above as Cisco Webex services.

Introduction

At Cisco, we take our customers' compliance seriously. Cisco Webex services provides world class collaboration that is simple, scalable, and designed to meet your HIPAA compliance needs. This whitepaper summarizes the security practices Cisco uses for Webex services. Described below are the many ways Cisco supports the security and privacy of electronic personal health information (PHI) processed and stored in Cisco Webex. Cisco Webex services has been well-designed to help customers satisfy HIPAA requirements.

Cisco: A Trusted Security Partner

Cisco is home to some of the world's top security researchers, including the teams behind Sourcefire, Threat Grid, and Talos. These experts in security provide us with a level of research and intelligence beyond that available to others. Our security ecosystem, Cisco Collective Security Intelligence (CSI), collects threat intelligence from several teams throughout the company. They work together to offer unparalleled visibility into the threats facing our customers, and can track threats across networks, endpoints, mobile devices, virtual systems, email, and the web. Our approach to security shows Cisco's holistic approach of understanding of threats, their root causes, and determining the scope of outbreaks.

This security mindset can be seen in the way we develop and maintain our products. Cisco uses the information it collects to design, operate, and maintain our products and services to best defend against security risks. We utilize secure engineering processes throughout the development and maintenance lifecycle. Our products and services undergo rigorous testing by employees, customers, third-party labs, and some of the best engineers in the world. Our vulnerability management team seeks to prevent new threats by constantly scanning the environment to proactively block potential threats. Further, our incident response team rapidly resolves any incident impacting our business operations by providing 24-hour coverage to detect and manage incident impact and resolution. Cisco believes that maintaining trust with our customers is paramount, and we do everything we can to earn that trust.

HIPAA Self-Assessment

Cisco has conducted a HIPAA self-assessment on Cisco Webex services. The self-assessment is based on a shared responsibility model depicted in the table below.

HIPAA Shared Responsibility Model for Cisco Webex services	
HIPAA Compliance Requirements	
Cisco's Responsibilities	Customer's Responsibilities

Within the Cisco Webex services platform Cisco is responsible for maintaining customer data: • Confidentiality • Privacy • Security	Within the Cisco Webex services platform the customer is responsible for: • Classifying data they submit and retrieve • Maintaining data they submit and retrieve

*The customer is responsible for the security of the workstations and systems used to generate, process, and store electronic PHI within their information systems.

HIPAA Security Standards & Implementation Specifications

One of the goals of HIPAA is to safeguard individuals' PHI. HIPAA security requirements protect the privacy of individually identifiable health information and the HIPAA Security Rule has become a key pillar of PHI security. The Security Rule seeks to:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures; and
4. Ensure HIPAA compliance.

By following guidelines for administrative, physical, and technical compliance with HIPAA, the Security Rule creates a framework for assessing security. The Security Rule identifies three types of security safeguards required for compliance with HIPAA:

1. Administrative safeguards – personnel and management processes to train employees who come into contact with PHI, detect privacy violations, and handle those violations.
2. Physical safeguards – policies and procedures that govern adding and removing hardware, access to equipment, etc.
3. Technical safeguards – guidelines for data encryption, data corroboration, and audit logging.

Each safeguard consists of a list of "standards", and each standard may consist of one or more "implementation specification". Implementation specifications are designated as either "required" or "addressable". Just because an implementation specification is "addressable" does not mean that it is optional, and Cisco implements all of the "addressable" specifications that are relevant to Cisco Webex services. Some of the implementation specifications are outside the scope of Cisco Webex services because they either pertain to overarching security policies and processes (e.g., workforce clearance procedure) that are not technology-specific, or a different technology area that is not related to Cisco Webex services. The implementation specifications in ***bold italics*** in the tables below are not relevant to Cisco Webex services.

Administrative Safeguards

Standard	Section	Implementation Specifications (R)=Required, (A)=Addressable
Security Management Process	164.308(a)(1)	Risk Analysis (R)

		Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)
Information Access Management	164.308(a)(4)	***Isolating Health care Clearinghouse Function (R)*** Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)

Security Management Process: Risk Analysis, Risk Management, Sanction Policy, and Information System Activity Review

Policies and procedures must be in place to prevent, detect, contain, and correct security violations. The Cisco Webex cloud security team has established formal policies, standards, and procedures relevant to the design and operations of controls over Cisco Webex services for Teams, Meetings, Control Hub, and Developer API services. Policies are reviewed and approved periodically, published on the Cisco company intranet, and shared with Cisco employees and contractors. Cisco management has an independent group within the Cisco Security & Trust Organization that performs periodic risk assessments. Activities, remediation, and initiatives are monitored and reported to management.

Assigned Security Responsibility

A security official responsible for the development and implementation of policies and procedures required by HIPAA must be assigned. Cisco Webex services assigns responsibility to the Cisco Webex Chief Security Officer who manages the cloud security and operations team. Both teams oversee security issues, provide training for new hires, and hold an annual Security Awareness training.

Workforce Security: Authorization and/or Supervision, Workforce Clearance Procedure, and Termination Procedures

Policies and procedures must be implemented to ensure workforce members have appropriate access to electronic PHI, and to prevent workforce members who do not have access from obtaining it. Cisco maintains a list of authorized persons who have privileged access to the Cisco Webex services system. Requests for access must be approved by management and there is a periodic review of role-based access to the systems.

Cisco Webex services management segregates duties and has a formal procedure for requesting and terminating access to Cisco Webex services systems. Cisco follows a structured on-boarding process and our policies and guidelines require background checks for all Cisco Webex services personnel.

Information Access Management: Access Authorization, and Access Establishment and Modification
Policies and procedures for authorizing access to electronic PHI must be implemented. Cisco has done this by creating policies and procedures that define how access is granted for the workforce and business associates. All access to systems must be authorized by Cisco Webex services management.

Security Awareness and Training: Security Reminders, Protection from Malicious Software, Log-in Monitoring, and Password Management
A security awareness and training program for all workforce members must be implemented. Cisco Webex services' workforce is required to complete an annual security awareness training. Every member of the workforce receives an email with information about the employee's security responsibilities and how to communicate significant issues in a timely manner. Workforce members are also required to maintain anti-malware on their workstations. Cisco Webex services has log-in monitoring in place for the cloud systems. Cisco's password policy requires strong passwords, changing passwords on a periodic basis and protecting passwords.

Security Incident Procedures: Response and Reporting
Policies and procedures must be in place to address security incidents. Cisco has a mature process for reporting and managing potential security problems. The process is included in new hire and refresher training courses on security awareness. Cisco employs external and internal incident response reporting mechanisms. Customers can notify Cisco and Cisco Webex services of incidents by contacting the Cisco Product Security Incident Response Team (PSIRT).

Contingency Plan: Data Backup Plan, Disaster Recovery Plan, Emergency Mode Operation Plan, Testing and Revision Procedure, and Applications and Data Criticality Analysis
Policies and procedures must be established and implemented as needed for responding to an emergency or other occurrence (such as a fire, vandalism, system failure, or natural disaster) that damages systems containing electronic PHI. Cisco Webex services' cloud-hosted data is continuously backed up using near-real time replication of data across geographically remote locations. Cisco Webex services is hosted by multiple Cloud Service Provider (CSP) or co-location sites across the United States. This means a loss of a single location will not result in data or functionality loss. Cisco Webex services has an impact (criticality) analysis document and contingency (disaster recovery) plan and procedures. The alternate system is put into operational usage periodically and testing of the contingency plan and procedures is performed annually.

Evaluation
Periodic technical and nontechnical performance evaluations must be conducted in response to environmental or operational changes affecting the security of electronic PHI. Independent internal audits, external audits, security assessments, and risk assessments are performed for Cisco Webex services. The results provide identification of risks, risk treatments, and remediation as appropriate to address any potential risks.

Business Associate Contracts and Other Arrangement: Written Contract or Other Arrangement
Business associates creating, receiving, maintaining, or transmitting electronic PHI on behalf of Cisco must provide satisfactory assurances that information will be appropriately safeguarded. Cisco has policies and procedures for managing its suppliers (Business Associates). Our suppliers undergo a security evaluation to

identify risks to customers and/or Cisco data. Suppliers enter into agreements with Cisco, which cover supplier access, duties, services, licenses, intellectual property rights, security requirements, Service Level Agreements, confidentiality, integrity, and availability.

Physical Safeguards

Standard	Section	Implementation Specifications (R)=Required, (A)=Addressable
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Facility Access Controls: Contingency Operations, Facility Security Plan, Access Control and Validation Procedures, and Maintenance Records
Physical access to electronic information systems and facilities must be limited while also ensuring that properly authorized access is allowed. To meet this standard, Cisco Webex services uses Cisco owned data centers, co-location data centers or Cloud Service Providers (CSP). The Cisco Webex ISO/IEC 27001:2013 certification includes Cisco owned data centers and co-location data centers. Each CSP has an ISO/IEC 27001: 2013 certificate, The certificate requires a facility security plan, access control & validation, maintenance records, protections from power failures, and other utility disruptions. Cisco has a Business Associate Agreement (BAA) with each CSP.

Additionally, Cisco Webex services is hosted on multiple sites across the United States providing contingency capabilities. Data and functionality are replicated across the sites meaning a loss of a single location will not result in data or functionality loss. Cisco Webex services client-side encryption of user-generated data ensures that data arriving at the Cisco Webex services cloud is encrypted end-to-end.

Workstation Use
Specifications for workstations that can access electronic PHI must be established. Cisco Webex services has implemented policies and procedures for acceptable use of workstations.

Workstation Security
Physical safeguards for all workstations that access electronic PHI must be implemented to restrict access to authorized users. Cisco has policies and procedures for physical protection of workstations, protecting unattended workstations, and for use of workstations outside of the facility. The person assigned to the workstation is responsible for ensuring the protection of electronic and computing devices used to conduct Cisco business or interact with internal networks and business systems.

Device and Media Controls: Disposal, Media Re-Use, Accountability, and Data Backup and Storage

Policies and procedures must be established to govern the receipt and removal of hardware and electronic media that contain electronic PHI into, out of, and within a facility. The Cisco Webex ISO/IEC 27001:2013 certification includes Cisco owned data centers and co-location data centers. Cisco Webex services' Cloud Service Providers (CSP) have the ISO/IEC 27001:2013 certification. The certificate requires controls to be in place for secure disposal of devices and media. Cisco Webex services also provides end-to-end client-side encryption. Data is replicated across multiple CSP sites meaning a loss of a single location will not result in data loss.

Technical Safeguards

Standard	Section	Implementation Specifications (R)=Required, (A)=Addressable
Access Control	164.312(a)(1)	Unique User Identification (R) ***Emergency Access Procedure (R)*** ***Automatic Logoff (A)*** Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Access Control: Unique User Identification, and Encryption and Decryption
Technical policies and procedures for electronic information systems that maintain electronic PHI must be implemented to allow access to only those persons or software programs that have been granted access. This includes assigning a unique name and/or number for identifying and tracking user identity. In order to limit exposure of user identity information, we distinguish between "real" and "obfuscated" identity in the Cisco Webex services cloud. The data that we collect as part of Cisco Webex services user registration—user name, email address, phone number, and so on—is considered "real identity" and stored in the user's profile in a Cisco Webex services cloud component known as Common Identity. For each user, Cisco Webex services generates a random 128-bit universally unique identifier (UUID), which is the user's obfuscated identity. Similarly, for enterprises, Cisco Webex services utilizes a random 128-bit "organization ID" as the obfuscated identity of each enterprise.

Within Cisco Webex services we use obfuscated identity everywhere we can, including:

- Message routing – All messages in Cisco Webex services are routed from sender to recipient solely on basis of obfuscated identity.
- Cloud-internal queries – All cloud-internal queries related to individual users also rely on obfuscated identity.

A mechanism to encrypt and decrypt electronic PHI must also be established. Cisco Webex services encrypts the transmission of data from client devices to the Cisco Webex services cloud using Transport Layer Security (TLS). All media in Cisco Webex services, such as voice, video, and desktop share, is transmitted using Secure Real-Time Transport Protocol (SRTP; defined in RFC 3711).

Cisco Webex services encryption key management system sits in its own domain and Cisco Webex services maintains physical separation of domains. In addition, Cisco offers a Hybrid Data Security deployment option to enable enterprise customers to host their encryption key management system on customer-managed servers.

Cisco Webex services uses an open architecture for secure distribution of encryption keys. This means that content is encrypted on the user client and remains encrypted until it reaches the recipient. Cisco Webex services, and any intermediaries, will not access decryption keys for content unless the enterprise explicitly chooses to grant such access. The caveat to the previous statements are certain cloud services continue to have access for processing content in order to enable capabilities like preview of documents, API integrations, and DLP processing. All such access is automated and for processing in memory only.

Audit Controls
Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI must be implemented. Cisco Webex services is designed to encrypt data in transit and at rest based on risk analysis. Cisco Webex services restricts personnel that have access to and can perform activities on the system based on risk analysis and the security principle of least privilege. Cisco Webex services also logs and monitors activity and takes action for potential incidents.

Integrity: Mechanism to Authenticate Electronic Protected Health Information
Policies and procedures must be established to protect electronic PHI from improper alteration or destruction. Cisco Webex services' end-to-end encryption helps to prevent data from being altered or destroyed in transit or at rest in an unauthorized manner. Cisco employees do not have access to the content or purpose of the data the customer is transmitting or storing under normal circumstances, as per the operational security deemed necessary for operating our offer.

Person or Entity Authentication
A verification process must be in place to verify the identity of a person or entity seeking access to electronic PHI. Cisco Webex services is designed to give both users and enterprises privacy choices without presenting complicated configuration interfaces. For enterprise administrators, choices include:

- Single Sign-On (SSO) – Administrators can configure Cisco Webex services to work with their existing SSO solutions. Cisco Webex services supports identity providers using Security Assertion Markup Language (SAML) 2.0 and OAuth 2.0.
- Directory synchronization – Administrators can have employee lifecycle changes reflected in Cisco Webex services in real-time when using Microsoft Active Directory.
- Aggregated data sharing with Cisco partner – Enterprises can choose whether to share quality of service and engagement data with their Cisco partners to enable higher level partner support.

For users, choices include:

- Device permissions – Depending on the mobile or browser platform on which the user is running Cisco Webex services, Cisco Webex services will request a variety of device permissions, including phone, microphone, camera, audio recording, screen sharing, calendar, contacts, files and photos, and push notifications. On most platforms, these require explicit permission that the user can revoke at any time.
- Proximity features – On mobile devices, Cisco Webex services clients can automatically pair with Cisco voice and video endpoints by listening for ultrasonic signals when the Cisco Webex services client is active. Users can turn off this feature if they so choose.

- External participant indicators – Cisco Webex services clients make it clear to users, through visual indicators, when a space contains participants who are not part of their enterprise organization.
- Space moderator control – Users can moderate spaces, allowing chosen participants to be designated as moderators with exclusive control of the space name and participant list.

Transmission Security: Integrity Controls, and Encryption
Technical security measures must be implemented to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network. Cisco Webex services uses TLS encryption in transit to prevent data from being improperly modified.

Cisco also has measures in place to protect customer data against accidental or unlawful loss, destruction or alteration, and unauthorized disclosure or access. These measures include policies, procedures, and internal controls for Cisco personnel, equipment, and processes. We also enforce similar measures with our vendors and subcontractors.

Protecting Personal Data and Privacy in the Cloud

Privacy is a top priority for Cisco. We comply with the applicable privacy and data protection laws wherever we do business, including the European Union General Data Protection Regulation (GDPR). We are aware of the legal obligations we must meet in the jurisdictions where we operate, and we address them through a common control framework that is the basis for our global privacy policies.

One of the most important considerations in privacy and data protection is defining and understanding the different types of data that may be migrated, processed, or stored in the cloud.

This data may include:
- Protected Health Information (PHI) defined under HIPAA
- Personally Identifiable Information ("PII" or "Personal Data") defined by applicable laws
- Sensitive business information defined by applicable laws or considered as sensitive by our customers
- Data that is subject to data residency restrictions by law
- Sensitive data that is subject to data residency restrictions by customer requirements
- Telemetry data
- Geo-location data

Cisco will work with you to understand your data flows and to clearly identify different types of data in the cloud, including customer data, Cisco data, or third party data.

Cisco is constantly improving its strategy to enhance its privacy and data protection efforts for evolving customer requirements and a rapidly changing regulatory landscape.

Please refer to the Cisco Online Privacy Statement for the latest updates and information.

A Reputation Built On Trust by Design

Cisco's reputation as a trusted security provider rests on our ability to deliver a comprehensive security and data protection experience in the cloud. Our guiding principles for trust -- security, privacy, confidentiality, availability, and integrity – enable simplicity and transparency, accelerate time to market, and improve the ease of doing business with Cisco.

Working together with our customers, partners, and with our industry-leading security expertise and strict internal controls, we are confident in our ability to be a trusted business partner in HIPAA-compliance and secure cloud collaboration using Cisco Webex services including Teams apps, Meetings apps, Control Hub, and Developer APIs.

Additional Information

To request a copy of the Cisco Webex HIPAA Self-Assessment, please contact your account manager.

Please refer to Cisco Trust Portal for up-to-date information on personal data processing, data center locations, access control, data deletion and retention, and personal data security described in Administrative, Physical, and Technical Safeguards sections above.