Cisco Webex HIPAA Compliance: Webex Suite and Contact Center

Overview of Cisco Webex Suite and Cisco Webex Contact Center

Cisco Webex Suite ("Webex Suite") and Cisco Webex Contact Center ("Webex Contact Center") (collectively" Webex") are made available by Cisco to companies or persons ("Customer") who acquire them for use by their authorized users.

Webex Suite is a cloud-based collaboration platform that provides a complete collaboration suite for teams to create, meet, message, make calls, and share, regardless of whether they are together or apart, in one continuous workstream before, during, and after meetings. For a detailed description of the Webex Suite, please visit website.

Webex Contact Center is a native cloud contact center solution that enables enriched customer engagement experiences between businesses and their customers. For a detailed description of Webex Contact Center, please visit website.

Scope

The following are in scope for this Cisco Webex HIPAA document:

1. Webex Suite includes Webex Meetings (including what was formerly known as Webex Support and Webex Training and features and functionality included as of September 30, 2021), Webex Events (classic) (formerly known as Webex Events), Webex Calling, Webex App, Webex for Developers (APIs), and Webex Control Hub;[1]

2. Webex Contact Center located at Cisco-owned data centers in Mountain View, CA, Richardson, TX and Allen, TX, and the data center facilities provided by Amazon Web Services (AWS), and CyberCenter, Equinix, Bharti Airtel, Telx, OneWilshire, and Telstra (hereby collectively referred to as the "Co-location Services Providers").

The scope includes services sold and also known as Webex Teams, BroadCloud Carrier, Webex Calling Carrier and UCM Cloud.

The managed hosting services provided by AWS and the co-location services provided by Co-location Services Providers are not included in the scope.

Customers as Covered Entities

Cisco understands that customers may have to meet standards, implementation specifications and requirements of a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA").

[1] Separately, Cisco has made available on the Trust Portal a HIPAA Self-Assessment for Webex Webinars.

Webex enables customers to meet their privacy compliance requirements in part through its strong privacy and security practices, which include a privacy impact assessment designed to ensure appropriate privacy features and security controls are built in from the start, so that customers may use them to help meet their HIPAA requirements. As detailed below, Cisco also engages qualified third parties to evaluate Webex products for their ability to enable HIPAA compliance.

It is the customer's responsibility to understand if electronic Protected Health Information (PHI) is included in user-generated information and data. The customer and its end users are responsible for providing PHI in the user-generated information and any other data they submit and provide to Cisco through Webex. The customer is responsible for the security of the workstations and systems that are used to generate, process, and store electronic PHI within their information systems.

Third-Party Attestation[2]

As part of its efforts to demonstrate that Webex enables HIPAA compliance, Cisco requested a licensed, independent, certified public accounting firm ("Third-party") to examine Cisco's description of its information security program supporting Webex. This examination was performed in accordance with the Statement for Standards Attestation Engagements (SSAE) 18: Attestation Standards, Clarification and Recodification, section 205 specifically. Upon completing the examination, the Third-party provided a report which included the opinion that, "in all material aspects, a) the description [of Cisco's information security program provided to the Third-party] fairly presents the information security program supporting the Webex Suite and Webex Contact Center system that was provided to user entities, as of September 30, 2021; and b) the information security program conformed to the applicable implementation specifications within the HIPAA Security Rule, as described in Part 164 of CFR 45, as of September 30, 2021."

This Third-party examination gives customers peace of mind that Cisco's information security program supporting Webex as of September 30, 2021, enables them to meet their HIPAA compliance requirements.

The Third-party report is available on request on Cisco's Trust Portal.

[2] Prior to seeking a third-party attestation, Cisco performed a self-assessment of its information security program supporting Webex against the Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule" or "Security Rule") as described in Part 164 of CFR 45. Based on this self-assessment, Cisco determined that its information security program supporting Webex, as of September 30, 2021, conforms to the HIPAA Security Rule.

HIPAA Security Standards and Implementation Specifications

One of the goals of HIPAA is to safeguard individuals' PHI. Per the U.S. Department of Health and Human Services (HHS), the HIPAA Security Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.

As written in the HHS HIPAA page (or sub-pages), the Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic PHI. Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

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:

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

Each safeguard consists of a list of "standards", and each standard consists of "implementation specifications." The standards and implementation specifications are listed in the tables below.

Some of the implementation specifications are outside the scope of Webex because they are not technology-specific or are a different technology area that is not related to Webex. The implementation specifications in italics and marked with "not applicable" in the tables below are not relevant to Webex.

Administrative Safeguards

Standard	Section	Implementation Specifications (R)=Required, (A)=Addressable	Webex
Security Management Process	164.308(a)(1)	• Risk Analysis (R) • Risk Management (R) • Sanction Policy (R) • Information System Activity Review (R)	Cisco has formal policies, standards, and procedures relevant to the design and operations of controls.

Assigned Security Responsibility	164.308(a)(2)	• (R)	The Cisco Webex team assigns responsibility to the Cisco Collaboration Chief Security Officer.
Workforce Security	164.308(a)(3)	• Authorization and/or Supervision (A) • Workforce Clearance Procedure (A) • Termination Procedures (A)	Cisco maintains a list of authorized persons and procedures for privileged access to the Webex system.
Information Access Management	164.308(a)(4)	• *Isolating Health care Clearinghouse Function (R) – not applicable* • Access Authorization (A) • Access Establishment and Modification (A)	Cisco has formal policies and procedures for authorizing access to the Webex system.
Security Awareness and Training	164.308(a)(5)	• Security Reminders (A) • Protection from Malicious Software (A) • Log-in Monitoring (A) • Password Management (A)	Cisco employees are required to complete an annual security awareness training and to maintain antimalware on their workstations. Log-in monitoring is in place for Cisco systems, including Webex. Cisco's password policy requires strong passwords, changing passwords on a periodic basis and protecting passwords.
Security Incident Procedures	164.308(a)(6)	• Response and Reporting (R)	Cisco has a mature process for reporting and managing potential security problems.
Contingency Plan	164.308(a)(7)	• Data Backup Plan (R) • Disaster Recovery Plan (R) • Emergency Mode Operation Plan (R) • Testing and Revision Procedure (A)	Cisco has a backup and disaster recovery plan which includes testing and impact analysis.

		• Applications and Data Criticality Analysis (A)	
Evaluation	164.308(a)(8)	• (R)	Independent internal audits, external audits, security assessments, and risk assessments are performed for Webex.
Business Associate Contracts and Other Arrangement	164.308(b)(1)	• Written Contract or Other Arrangement (R)	Cisco has policies and procedures for managing its suppliers (including those that may be considered Business Associates).

Physical Safeguards

Standard	Section	Implementation Specifications (R)=Required, (A)=Addressable	Webex
Facility Access Controls	164.310(a)(1)	• Contingency Operations (A) • Facility Security Plan (A) • Access Control and Validation Procedures (A) • Maintenance Records (A)	Webex uses Cisco-owned data centers, co-location data centers or Cloud Service Providers (CSP) each of which has ISO/IEC 27001:2013 certification which includes these physical controls.
Workstation Use	164.310(b)	• (R)	Cisco has implemented policies and procedures for acceptable use of workstations.
Workstation Security	164.310(c)	• (R)	Cisco has policies and procedures for physical protection of workstations, protecting unattended workstations, and for use of workstations outside of the facility.
Device and Media Controls	164.310(d)(1)	• Disposal (R) • Media Re-use (R) • Accountability (A) • Data Backup and Storage (A)	Webex uses Cisco owned data centers, co-location data centers or Cloud Service Providers

			(CSP) each of which has ISO/IEC 27001:2013 certification which includes controls for secure disposal of devices and media.

Technical Safeguards

Standard	Section	Implementation Specifications (R)=Required, (A)=Addressable	Webex
Access Control	164.312(a)(1)	• Unique User Identification (R) • *Emergency Access Procedure (R) – not applicable* • *Automatic Logoff (A) – not applicable* • Encryption and Decryption (A)	Refer to the Privacy Data Sheets and technical papers on the Trust Portal for more information.
Audit Controls	164.312(b)	• (R)	The Cisco Webex team logs and monitors activity and takes action for potential incidents.
Integrity	164.312(c)(1)	• *Mechanism to Authenticate Electronic Protected Health Information (A) – not applicable*	Not Applicable.
Person or Entity Authentication	164.312(d)	• (R)	Refer to the Security papers for more information.
Transmission Security	164.312(e)(1)	• Integrity Controls (A) • Encryption (A)	Refer to the Security papers for more information.

In addition to the safeguards, there are additional requirements listed as “Organizational” and “Policies and Procedures and Documentation.”

Organizational Requirements

Standard	Section	Requirements	Webex

Business Associate Contracts or Other Arrangements	164.314(a)(1)	• Contract Must Provide that Business Associates Adequately Protect EPHI • Contract Must Provide that Business Associate's Agents Adequately Protect EPHI • Contract Must Provide that Business Associates will Report Security Incidents • Contract Must Provide that Business Associate Will Authorize Termination of the Contract if it has been Materially Breached • *Government Entities May Satisfy Business Associate Contract Requirements through Other Arrangements– not applicable*	Agreements with suppliers include each of the requirements that are applicable.

Policies and Procedures and Documentation Requirements

Standard	Section	Requirements	Webex
Policies and Procedures	164.316(a)	• Create and Deploy Policies and Procedures • Update Documentation of Policy and Procedures	Cisco, including the Cisco Webex team, has policies and procedures that are reviewed and updated.
Documentation	164.316(b)(1)	• Draft, Maintain and Update Required Documentation • Retain Documentation for at Least Six Years • Assure that Documentation is Available to those Responsible for Implementation • Update Documentation as Required	Webex maintains, and updates required documentation. The documentation is retained as required.

HIPAA Compliance for Webex

Cisco extensively documents and makes available its security and privacy practices. You may find additional information in the Cisco Webex Trusted Platform, Cisco Online Privacy Statement, Cisco Webex Privacy Data Sheets and Cisco Webex Privacy Data Maps.

Cisco makes security the top priority in the design, development, deployment, and maintenance of its networks, platforms, and applications. You can incorporate Webex into your business processes with confidence. For more information about Cisco's overall security and privacy practices please refer to Cisco Trust Center. Webex has, among other applicable certifications, the following: ISO/IEC 27001:2013, ISO 27017:2015, ISO 27018:2019, ISO 27701:2019 and SOC2 Type II

The ISO/IEC 27001:2013, ISO 27017:2015 and ISO 27018:2019 certificate assures compliance with requirements for an Information Security Management System (ISMS), of which Privacy is an integral element. An ISMS is a systematic approach to managing sensitive company information so that it remains secure. ISO 27017:2015 assures the system is meeting information security controls in relation to cloud services. ISO 27018:2019 assures the system is meeting commonly accepted control objectives, controls and guidelines for implementing measures to protect Personal Information (PI). ISO 27701:2019 specifies requirements and provides guidance for a Privacy Information Management System (PIMS). The ISO 27001, 27017, 27018 certificate is publicly available.

The SOC2 Type II report includes the Privacy trust principle. The Privacy trust principle addresses the collection, use, retention, disclosure and disposal of personal information. The report contains the auditor's attestation of compliance and is available via your account manager under NDA.