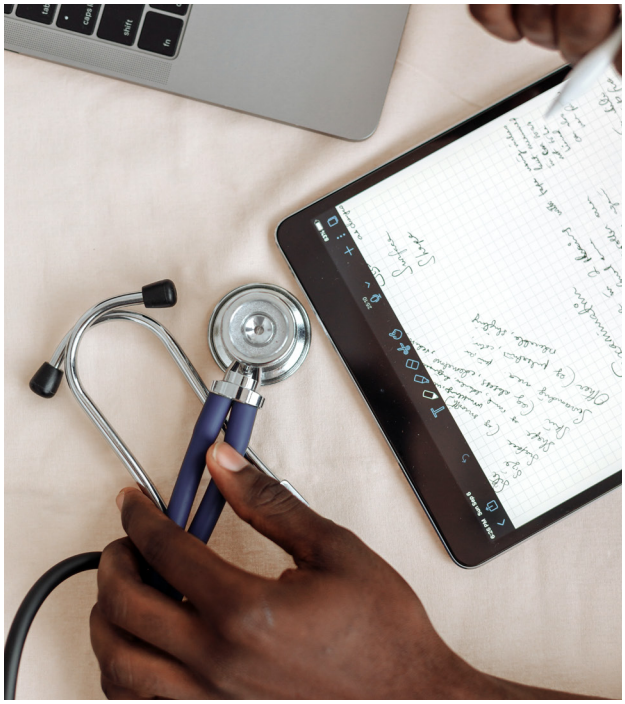
HIPAA Compliance

COMPLIANT WORLD-CLASS COLLABORATION

As the healthcare industry moves towards a new era of patient and employee engagement, more people are experiencing innovative ways to connect with their healthcare providers. Whether its remote video consults with doctors, messaging your provider for quick questions, or checking in on loved ones from a distance, everyone wants to know, is my data secure? At Cisco Webex, we take our customers' data security seriously and we are dedicated to providing world-class collaboration that is simple, scalable, and designed to meet your HIPAA compliance needs.



What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. healthcare law that establishes requirements for the use, disclosure, and safeguarding of individually identifiable health information. It applies to doctors' offices, hospitals, health insurers, and other healthcare companies with access to patients' protected health information (PHI).

How Do Cisco's Webex Services Enable HIPAA Compliance?

Cisco has conducted a HIPAA self-assessment on Cisco Webex services (Teams, Meetings, Control Hub, and Webex for Developers). This self-assessment is based on a shared responsibility model where the Cisco Webex services platform is responsible for maintaining customer data including Confidentiality, Privacy, and Security. In line with the HIPAA Security Rule, Cisco implements all the addressable specifications that are relevant to Cisco Webex services. These are segmented into three safeguards – Administrative, Physical, and Technical.

1. Administrative

The administrative safeguard covers standards that relate to the administration for the Webex platform by Cisco such as, but not limited to, security management processes, assigning security responsibilities, ensuring workforce security, incident reporting procedures, periodic evaluations, and more. 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. These policies and procedures prevent unauthorized access to Webex data, ensure reporting and management of potential security issues, and protect your PHI through a contingency plan for disasters and the like.

2. Physical

The physical safeguard covers physical access (limited and authorized) to electronic information systems. To meet this standard, Cisco Webex services use Cisco owned data centers, co-location data centers, or Cloud Service Providers (CSP). Each data center is certified (ISO/IEC 27001:2013 certification) to ensure the location has a facility security plan, access control and validation, maintenance records, protections from power failures, and other utility disruptions. Cisco also has a Business Associate Agreement (BAA) with each CSP. Being a global platform, Cisco Webex services are hosted throughout multiple locations, ensuring the loss of a single location will not cause data or functionality loss.

3. Technical
The technical safeguard covers the utilization of Webex services and address standards such as access and audit controls, integrity, authentication, and transmission security. Cisco distinguishes a user's identity between their "real identity" and their "obfuscated identity". For each user, Cisco Webex services generate a random 128-bit universally unique identifier (UUID), which is the user's obfuscated identity. Similarly, for enterprises, Cisco Webex services utilize a random 128-bit "organization ID" as the obfuscated identity of each enterprise. These obfuscations are then used everywhere possible such as in message routing and cloud internal inquires.

Additionally, the PHI that is transmitted when using Webex services is encrypted from client devices to the Cisco Webex services cloud using Transport Layer Security (TLS), and all media in Cisco Webex services, such as voice, video, and desktop share, is transmitted using Secure Real-Time Transport Protocol (SRTP). Not only is content encrypted, but the end-to-end encryption services also helps to prevent data from being altered or destroyed in transit or at rest in an unauthorized manner. There are additional policies in place that enable user and enterprise privacy choices such as single-sign-on, directory synchronization, device permissions, proximity features, and more. For a detailed review of Cisco Webex services' safeguard standards, please review the Cisco HIPAA compliance white paper. For access to the Cisco HIPAA self-assessment, reach out to your local account team.

Conclusion
Everyone has the right to data privacy. Whether you are a patient, doctor, medical staff, or insurer, the protection of personal data is critical. By enabling policies and guidelines that adhere to security, privacy, confidentiality, availability, and integrity we can enable users to safely experience a new world of healthcare, on an unprecedented scale. Users of Webex services can feel secure knowing their messaging, voice, and video data are protected.