Cisco Webex: Complying with PIPEDA and PHIPA

Cisco takes our customers' compliance seriously. Cisco® Webex provides world class collaboration that is simple, scalable, and designed to meet your PIPEDA and PHIPA compliance needs. For the purposes of this document, "Cisco Webex" means Webex Teams™, Webex® Meetings, Webex Control Hub, and Webex for Developers.

Q 1. What privacy laws in Canada should I be aware of?

A **PIPEDA** (the Personal Information Protection and Electronic Documents Act). PIPEDA is a Canadian federal privacy law that defines the rules for how organizations across Canada collect, use, and disclose personal information. It also applies to the personal information of employees of federally regulated businesses such as: banks, airlines, and telecommunications companies.

PHIPA (Personal Health Information Protection Act): PHIPA is an Ontario provincial privacy law that defines the rules for the collection, use, and disclosure of personal health information.

Q 2. How is personal information defined under these laws?

A **PIPEDA:** Personal information (PI) means information about an "identifiable individual". It is information on its own or combined with other pieces of data that can identify you as an individual. This can mean information about your:

- Race, national or ethnic origin
- Religion
- Age, marital status
- Medical, education or employment history
- Financial information
- DNA
- Identifying numbers, such as your social insurance number or driver's license
- Views or opinions about you as an employee

Source: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2-2

PHIPA: Personal health information (PHI)is identifying information about an individual in oral or recorded form, if the information:

- Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family
- Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual
- Is a plan of service for the individual
- Relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual
- Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance
- Is the individual's health number
- Identifies an individual's substitute decision-maker

Source: https://www.ontario.ca/laws/statute/04p03

Q

3. How does Cisco Webex comply with PIPEDA and PHIPA?

A

Cisco Webex is built with strong privacy and security practices by design, so that you may use in compliance with PIPEDA, PHIPA and other provincial privacy laws. Please see our Cisco Webex Trusted Platform including Privacy Data Sheet(s) and Data Map(s) for more information about our data practices.

Q

4. What measures does Cisco take to help with protecting my privacy as well as the privacy of my employees, my customers, and my patients?

A

For more information about privacy practices for Cisco Webex, refer to the Cisco Webex Trusted Platform. For more information about Cisco's overall privacy and security practices, refer to Trust Center.

Additionally, Cisco follows data security and data privacy industry standards: ISO 27001, ISO 27017, ISO 27018 and SOC2.

The Cisco Webex SOC2 Type II certification includes the Privacy trust principle. The Privacy trust principle addresses the collection, use, retention, disclosure and disposal of personal information. The SOC3 report is publicly available and contains the auditor's attestation of compliance. The SOC2 report is available via your account manager under NDA.

The Cisco Webex ISO 27001 certification 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. The Cisco Webex ISO 27017 certification assures the system is meeting information security controls in relation to cloud services. The Cisco Webex ISO 27018 certification assures the system is meeting commonly accepted control objectives, controls and guidelines for implementing measures to protect Personal Information (PI).

Q 5. Why is protecting personal information and personal health information important?

A Protecting personal information is important to safeguard a person's identity. With a stolen identify, thieves can steal money, create debt, impersonate and sell the PI to other criminals. Stolen PHI can be used to cause harm to an individual by making medical conditions public, accessing a person's insurance information or disrupting medical care.

PI and PHI are highly valued and targeted by hackers and malware. In particular, PHI breaches have increased significantly in recent years. It is important for an organization to protect PI and PHI to maintain confidentiality of employee and customer/patient data. If the information is stolen, it may result in fines and loss of current and future customers and create a bad reputation for the organization.

Q 6. Does PIPEDA or PHIPA require data to be located in Canada to be compliant?

A No, PIPEDA and PHIPA do not require data localization.

Q 7. Are there similar privacy laws in other countries and how does Cisco comply with them?

A Cisco's global privacy practices are described in our Cisco Privacy Statement.

GDPR (EU): GDPR is the EU's General Data Protection Regulation that regulates privacy in the EU. Cisco has established long-standing security, data protection and privacy programs that comply with GDPR. Please refer to Our View on GDPR.

HIPAA (U.S): HIPAA is the Health Insurance Portability and Accountability Act, which is a U.S. law that sets national standards for healthcare transactions. Webex is designed to meet HIPAA compliance needs. Please refer to the whitepaper, HIPAA Compliance: Trust Cisco Webex services to Secure your Data.

Q 8. What best practices can Cisco recommend to enforce strong privacy practices of PI and PHI for my organization?

A There are a number of actions acustomer (end user) can take to protect their data, including PI and PHI. The Cisco Webex Meetings Security paper describes the role-based and administrative capabilities that can be utilized.

Q 9. What additional security practices does Cisco use?

A Cisco makes security the top priority in the design, development, deployment, and maintenance of our networks, platforms, and applications. You can incorporate Cisco Webex Meetings solutions into your business processes with confidence, even with the most rigorous security requirements. Review the Cisco Webex Meetings Security paper, Cisco Webex Teams Security paper, and the Cisco Webex Teams Application Security paper for more details.

Cisco publishes publicly available service agreements, statements, data maps, datasheets, and policies around data privacy.

Cisco Meetings uses public key cryptography processing ensuring data integrity and confidentiality. Refer to the security papers mentioned previously for more information.

Q

10. Does your platform provide end-to-end encryption?

A

End-to-End Encryption (E2EE) is a method of secure communications where only the communicating and authorized parties have access to the key to decrypt the content and read it. Nobody in between can access or tamper the data.

Cisco Webex uses strong encryption to protect your data. Cisco Webex services are designed to prevent undetected and unintended access to the data by unauthorized parties.

By default, Cisco Webex Meetings uses strong TLS 1.2 encryption to protect your data. Customers who wish to enable end-to-end encryption can enable it by using the “end-to-end encryption” session type. However not all meeting functions are available when enabling end-to-end encryption due to the need to decrypt the data for those functions. For details of the services not available when end-to-end encryption is enabled see: “What Does End-to-End Encryption Do?

Cisco Webex Teams encrypts user content (messages, files, boards, calendar events) end-to-end between communicating parties. End-to-end keys are accessible to only those parties and processing endpoints authorized by the customer (transcoders, DLP engines, virus-scanners, etc.). Customers that require full control over their end-to-end encryption keys may also deploy a Webex Hybrid Data Security (HDS) server within their datacenters.