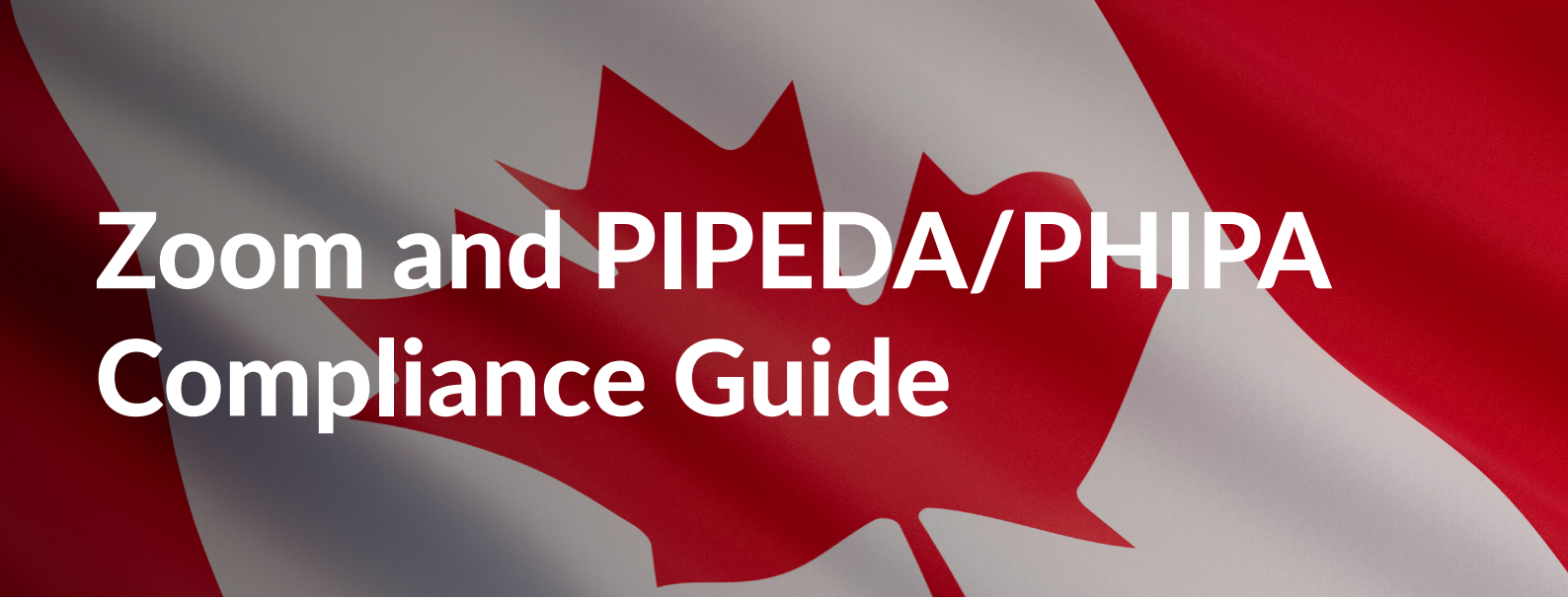

Zoom and PIPEDA/PHIPA Compliance Guide

At Zoom, we are committed to protecting the security and privacy of our customers' data. This includes enabling our customers in Canada to be compliant with Canadian Data Protection regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and, locally, the Personal Health Information Protection Act (PHIPA).

How does Zoom protect its customers data?

Zoom's commitment to protecting the security and privacy of our customers' data includes:

- Undergoing an annual SSAE-16 SOC 2 audit by a qualified independent third-party
- Performing regular vulnerability scans and penetration tests to evaluate our security posture and identify new threats

What is PIPEDA and PHIPA?

PIPEDA is a Canadian federal privacy law, enacted in April of 2000, for private sector business. It sets rules for how businesses must handle personal data in the course of commercial activity.

Enacted in November 2004, PHIPA is a local, provincial (Ontario) legislation that protects the confidentiality and privacy of personal health information (PHI) by establishing rules for the collection, use, and disclosure of PHI during the provision of healthcare.

What is "personal information" and "personal health information"?

Under PIPEDA, personal information is defined as any factual or subjective information, recorded or not, about an identifiable individual. This includes information, such as:

- Age, name, ID numbers, income, ethnic origin, or blood type
- Opinions, evaluations, comments, social status, or disciplinary actions
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, or intentions (for example, to acquire goods or services, or change jobs)

Under PHIPA "personal health information" means any information related to:

- The provisioning of healthcare services and treatment
- Payment for the provisioning of healthcare services
- Mental or physical health information

Are there any PIPEDA or PHIPA certification programs?

No. Currently there are no PIPEDA or PHIPA certification programs to assess third-party compliance.

Does PIPEDA or PHIPA impose any data localization requirements?

No. Data does not need to remain in Canada in order to comply with either of these privacy laws. As long as adequate transfer mechanisms are in place, Canadian data can be stored in the United States.

How does PIPEDA and PHIPA compare to US (HIPAA) and EU (GDPR) privacy regulations?

PIPEDA is a general data privacy regulation not specifically focused on personal health information, while PHIPA is limited to protecting the privacy and confidentiality of PHI. In that respect, PIPEDA is closer to EU GDPR, and PHIPA aligns to the US HIPAA regulations. However, both Canadian regulations focus on the use, transmission, storage, and security of data in ways that are more similar to the EU GDPR and its requirements for consent, access, transparency, etc. Whereas HIPAA looks to establish Business Associate relationships through BAA contracts that enable third parties to receive PHI in order to perform services, PHIPA requires that third parties ensure adequate protection of the data before they can receive it. And their use of data is limited to the purpose for which it was originally collected. Like GDPR, both Canadian regulations can be complied with by entering Data Protection Agreements which will ensure the adequacy of the data protection mechanisms that support the transfer to data.

How does Zoom help with PIPEDA and PHIPA compliance?

Zoom uses privacy practices and technical security measures to ensure that customer data is protected. Our security and privacy measures include:

- The execution of "Data Protection Agreements" to contractually establish adequate transfer mechanisms
- Providing a variety of in-meeting product security features
- Protecting data in transit by TLS 1.2 using 256-bit Advanced Encryption Standard (AES-256)
- Leveraging the physical and environmental protection of our TIER 1 data center providers. Zoom's hosting facilities have 24x7 manned security and monitoring through multiple layers of physical security controls including perimeters fences, manned lobbies, surveillance cameras (CCTV), man trap, locked cages, motion detectors, and biometric access requirements
- No monitoring, viewing, or tracking of the video or audio content of your video meetings or webinars
- No sharing of customer data with third parties
- Limiting retainment of accounts to 30 days after termination to assist with product reactivation (if requested by customer). After 30 days have passed, the account is permanently deleted

Additional Resources

PIPEDA in Brief

Personal Health Information Protection Act

Other Security Certification

SOC2:

The SOC 2 report provides third-party assurance that the design of Zoom, and our internal processes and controls, meet the strict audit requirements set forth by the American Institute of Certified Public Accountants (AICPA) standards for security, availability, confidentiality, and privacy. The SOC 2 report is the de facto assurance standard for cloud service providers.