



National Standard of Canada Standards Proposal

Proposed Standard Title:

Canadian Information Privacy Protection Framework

Proposed Scope:

This proposed standard aims to specify the minimum requirements for organizations that collect, uses, retain, and disclose personal information in Canada, and offers any benefit or consideration regardless of monetary exchange for such benefit or consideration.

The standard aims to provide a baseline framework for organizations seeking to harmonize conformance to the various provincial/territorial, federal, and international legislation and treaties.

The standard is not intended to prescribe how an organization should implement controls. Instead, the standard will guide organizations using jurisdictional and technological agnostic approaches due to differences across sectors the standard will be applied to. It is also not the intent to replace existing standards, certifications, or processes which presently allow organizations to conduct business at the national and global level.

This Standard applies to all sectors, including public and private companies, government entities, and not-for-profit organizations.

Strategic Need:

Identify the strategic need of key stakeholders and confirmation expressing the need.

This includes consideration for:

- a. *The strategic need of key stakeholder (e.g. legislator, industry, government, consumers);*
- b. *The type of standard (international, regional, domestic standards and harmonization need);*
- c. *Addressing up-to-date vs outdated standard to ensure latest innovative/technology/safety features available for businesses;*
- d. *If the standard is intended to support national/regional/international certification programs;*
- e. *If there is stakeholder intention to transition to different standard;*
- f. *The type of maintenance (periodic, continuous, stabilized, best before date); and*

The use of "CAN" descriptor.

In the current domestic privacy environment, Canadian organizations are stymied in their ability to compete internationally owing to the lack of any equivalent legislation or de facto standard consistent with recognized international privacy standards and regulations. Equally, Canadians citizens are stymied in having different executable privacy rights based on the province they inhabit.



Structurally, this is because no Canadian legislative body has ultimate jurisdiction over privacy because no Canadian legislature - neither federal nor provincial - can implement a de facto standard for Canadian privacy.

Canada is a country with fourteen jurisdictions, and there are currently thirty-six pieces of legislation between federal and provincial/territorial borders. Some are territorial in scope (Ontario FIPPA, BC PIPA), some are material in scope (CASL, PIPEDA).

At the global level, Canada's major trading partners continue to enact modern information privacy legislation. In Europe, the European Union General Data Protection Regulation (EU GDPR) is already two years in force and has been mirrored by equivalent national or provincial legislation across the globe to ensure compatibility. California, Brazil, Russia, India, China, South Africa, Egypt and are either in process or have already completed updating their regulations in this matter.

As a result of this, Canadian legislators, industry, governments, consumers all stand to benefit from a harmonized standard for information privacy in Canada put forward.

The proposed standard seeks to align differing coverage and material gaps that exist in Canada's tapestry of federal and provincial privacy legislation as well as address international requirements. With provinces seeking to update their own privacy legislation, the time to bring forward a unified Canadian standard is now.

This proposed National Standard of Canada will:

- support future certification programs developed at national level;
- be maintained on a periodic basis as determined by the technical committee responsible for developing the standard; and
- use the CAN descriptor.

Need for Availability in Both of Canada's Official Languages:

*Do stakeholders need the standard published in both official languages?
 Do users of the standard need the standard published in both official languages?
 Do authorities having jurisdiction need the standard published in both official languages?
 Are there health and safety related needs for the standard to be published in both official languages?
 For adoptions, is there availability of the regional/international standard or other deliverable from the source?
 For adoptions, is there an agreement with the source committee to facilitate official translation?*

Yes



Geographical Representation Considerations:

Identify the Canadian geographical representation appropriate to the subject area covered by the standard.

Geographic representation may consider factors such as:

- a. Industry (e.g. petroleum in petroleum producing provinces);*
- b. Reference in regulation (if a regulation exists in a province); or*
- c. Commodity characteristics and social impact (e.g. heating oil for northern climates).*

All sectors of the economy.

Trade:

Identify how the standard meets the needs of the marketplace and contributes to advancing trade in the broadest possible geographical and economic contexts.

For example:

- a. Facilitate Canadian innovation to lead internationally;*
- b. Support the objectives of “One standard, one test, accepted everywhere”;*
- c. Support the objectives of “First to Market”;* or
- d. Foster international/ regional/ national alignment of requirements.*

Canadian organizations now must meet unprecedented privacy requirements imposed by both their customers, domestic and international regulations. If organizations were to address these requirements on a case-by-case basis, they would be encumbered by trying to meet each requirement independently. By harmonizing their privacy program, organizations can reduce redundancy and streamline their processes to meet several requirements at the same time. A harmonized approach not only makes the organization more efficient (thus more competitive) but also protects the organization further as well as allowing them to expand into new markets.

Relevant existing documents at the international, regional and national level:

International legislation and treaties consistent with GDPR:

- California Consumer Privacy Act
- Lei Geral de Proteção de Dados (Brazil)
- Regulation (EU) 2016/679 - (European Union General Data Protection Regulation)
- Canada-United States-Mexico Agreement (CUSMA)

Canada’s 36 relevant pieces of privacy legislation:

Federal:

- Privacy Act (R.S.C., 1985, c. P-21)
- Personal Information Protection and Electronic Documents Act (S.C. 2000, c.5) - (PIPEDA)
- An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) - (CASL)



Alberta:

- Freedom of Information and Protection of Privacy Act, Alberta's public sector privacy law;
- Personal Information Protection Act, Alberta's private sector privacy law that has been deemed "substantially similar" to the federal private sector privacy law;
- Health Information Act, Alberta's privacy law relating to health records.

British Columbia:

- Freedom of Information and Protection of Privacy Act, BC's public sector privacy law;
- Personal Information Protection Act, BC's private sector privacy law that has been deemed "substantially similar" to the federal private sector privacy law;
- E-Health (Personal Health Information Access and Protection of Privacy) Act, BC's privacy law relating to health records.

Manitoba:

- Freedom of Information and Protection of Privacy Act, Manitoba's public sector privacy law;
- Personal Health Information Act, Manitoba's privacy law relating to health records.
- The Protecting Children (Information Sharing) Act

New Brunswick:

- Right to Information and Protection of Privacy Act, New Brunswick's public sector privacy law;
- Personal Health Information Privacy and Access Act, New Brunswick's privacy law relating to health records that has been deemed "substantially similar" to the federal private sector privacy law with respect to health information custodians.

Newfoundland and Labrador:

- Access to Information and Protection of Privacy Act, Newfoundland and Labrador's public sector privacy law;
- Personal Health Information Act and Pharmacy Network Regulations, Newfoundland and Labrador's privacy laws relating to health records that has been deemed "substantially similar" to the federal private sector privacy law with respect to health information custodians.

Northwest Territories:

- Access to Information and Protection of Privacy Act, The Northwest Territories' public sector privacy law;
- Health Information Act, The Northwest Territories' privacy law relating to health records.



Nova Scotia:

- Freedom of Information and Protection of Privacy Act (PDF) and the Privacy Review Officer Act, Nova Scotia's public sector privacy laws;
- Personal Health Information Act, Nova Scotia's privacy law relating to health records that has been deemed "substantially similar" to the federal private sector privacy law with respect to health information custodians;
- Part XX of the Municipal Government Act (PDF);
- Personal Information International Disclosure Protection Act

Nunavut:

- Access to Information and Protection of Privacy Act, Nunavut's public sector privacy law.

Ontario:

- Freedom of Information and Protection of Privacy Act, Ontario's provincial public sector privacy law;
- Municipal Freedom of Information and Protection of Privacy Act, Ontario's municipal public sector privacy law;
- Personal Health Information Protection Act, 2004, Ontario's privacy law relating to health records that has been deemed "substantially similar" to the federal private sector privacy law with respect to health information custodians.

Prince Edward Island:

- Freedom of Information and Protection of Privacy Act, PEI's provincial public sector privacy law.
- Health Information Act, PEI's health information law.
- Pharmaceutical Information Act

Québec:

- Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, Québec's public sector privacy law;
- Act Respecting the Protection of Personal Information in the Private Sector, Québec's private sector privacy law that has been deemed "substantially similar" to the federal private sector privacy law;
- An Act to amend the Act respecting health services and social services, the Health Insurance Act and the Act respecting the Régie de l'assurance maladie du Québec, Québec's privacy laws relating to health records.
- Bill 64: An Act to modernize legislative provisions as regards the protection of personal information (currently under legislative proposal)
- Civil Code of Québec, articles 35 to 41 (SQ 1991 c64)



Saskatchewan:

- Freedom of Information and Protection of Privacy Act, Saskatchewan's provincial public sector privacy law;
- Local Authority Freedom of Information and Protection of Privacy Act, Saskatchewan's municipal public sector privacy law;
- Health Information Protection Act, Saskatchewan's privacy law relating to health records.

Yukon

- Access to Information and Protection of Privacy Act, Yukon's public sector privacy law;
- Health Information Privacy and Management Act, Yukon's privacy law relating to health records.

Applicable International Standards:

- ISO 8000 Series, Data Standards
- ISO 27000 Series
- ISO 27701:2019 - Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO 29100:2019 - Information technology — Security techniques — Privacy framework
- ISO 31000 Series, Risk Management