Privacy Legislation and Practice in Canada
A Primer for Homelessness Response Systems

What is this Document?

This document is intended support communities to understand the privacy landscape as they work to implement By-Name Lists, Coordinated Access Systems, multi-agency case conferencing, and homelessness Management Information Systems (HMIS).

In this document you will find a quick overview of Canada's privacy framework (national, provincial and local) followed by a section providing quick access to privacy related documents and resources that may be of assistance. While we cannot provide you with legal advice, we hope this general information will be of assistance to you. You are encouraged to consult a lawyer, your organization's privacy officer, and/or contact your provincial Information and Privacy Commissioner (IPC) office for further information and assistance.

Contents:

Why is this Document Needed?

Local homeless serving systems typically include municipalities, charitable organizations. and health related organizations. Often, each of these organizations is governed by different privacy legislation (which is also different in every province/territory). This can be quite confusing when trying to work together in a community, especially when different organizations and their privacy officers or lawyers have different interpretation or approaches to applying the legislation. It can be helpful to have a "lay of the land" of what legislation is out there and who it applies to as well as good practices for moving forward.

The Bottom Line

Privacy can be managed in a way that facilitates providing good service and should not be seen as a barrier. However, there are rules for the handling personal information that must be complied with. The conversation should be more about "how" we move forward, not

"whether" we move forward in sharing information to provide effective, non-retraumatizing service to support people to end their homelessness.

Federal Level Privacy[1]

Canada has two privacy laws that are enforced by the Office of the Privacy Commissioner of Canada (OPC):

1. **Privacy Act** -governs the personal information handling practices of federal government institutions. The Act applies to all the personal information the federal government collects, uses and discloses—be it about individuals or federal employees.

2. **Personal Information Protection and Electronic Documents Act (PIPEDA)** - sets the ground rules for how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities[2] across Canada.

When does PIPEDA NOT apply?

PIPEDA only applies to organizations engaged in commercial, for-profit activities and does not include:

- Not-for-profit/charity groups – unless organizations are engaging in commercial activities that are not central to their mandate and involve personal information – such as selling a donor list.
- Political parties and associations.
- Municipalities, universities, schools, and hospitals - generally covered by provincial laws unless organizations are engaging in commercial activities that are not central to their mandate and involve personal information – such as a university selling an alumni list.
- Some provinces have their own private sector privacy laws, and if so, commercial organizations are subject to the provincial law and not PIPEDA[3].

When DOES PIPEDA apply?

- Federal Works, Undertakings and Businesses (FWUBs) operating in provinces continue to be subject to PIPEDA. Organizations in the Northwest Territories, Yukon and Nunavut are considered FWUBs and therefore are covered by federal PIPEDA.

---

[1] Information from https://www.priv.gc.ca/en

[2] "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."

[3] Privacy Compliance Principle - if the provincial privacy law has been ruled to be "substantially similar" to the federal law by the Privacy Commissioner of Canada, then the provincial law supersedes the federal law and the organizations only have to comply with the provincial legislation (i.e., Alberta, BC, Quebec for privacy) (i.e., Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador for health). If the provincial law is not considered to be "substantially similar" to PIPEDA, then organizations operating in that province must comply with both the federal and provincial laws.

- PIPEDA also applies to inter-provincial and international transactions involving personal information in the course of commercial activities.

1. Provincial Level Privacy

Each province and territory have their own laws that apply to provincial government agencies, municipalities, and health privacy, as well as having a commissioner or ombudsperson responsible for overseeing provincial and territorial privacy legislation.

See Appendix A for a list of the provincial and territorial privacy laws, their oversight body, and what types of organizations that are typically part of the homeless services sector that fall under each.

In a recent report on child welfare, the differences in legislation and balancing information sharing with privacy was found to be a widespread challenge:

> "Broadly, there are two themes present in legislation discussing privacy and access to information rights. The first theme is privacy and confidentiality vis-a-vis sharing of information, and the second is the right to access one's own information. Balancing information sharing with privacy considerations, especially when considering platforms that benefit from data use is a challenge faced by most provinces and territories. Our scan found that record keeping, privacy, and data utilization requirements differed significantly by province or territory".[4]

2. Quick Resources

The Built for Zero Canada website has a whole section with information, resources and sample materials from communities related to **Privacy, Consent and Data Sharing** – see the By-Name List page.

From Charity Central (Canadian): See the Privacy Policy Checklist

3. Personal Information[5]

"Personal information" means information about an identifiable individual which includes any factual or subjective information about that individual, including, for example:

- Name
- Opinions about the individual

[4] Using Data to Enable Better Outcomes for Young People Leaving Care- Dr. Naomi Nichols, McGill University Arisha Khan, Youth in Care Canada (May 2019).

[5] From https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/

- Birth date
- Income
- Physical description
- Medical history
- Gender
- Religion
- Address
- Political affiliations and beliefs
- Education
- Employment
- Visual images such as photographs, and videotape where individuals may be identified

What is generally ***not*** considered personal information can include:

- Information that is not about an individual, because the connection with a person is too weak or far-removed (for example, a partial postal code on its own which covers a wide area with many homes)
- Information about an organization such as a business.
- Information that has been rendered anonymous, as long as it is not possible to link that data back to an identifiable person
- Certain information about public servants such as their name, position and title
- A person's business contact information that an organization collects, uses or discloses for the sole purpose of communicating with that person in relation to their employment, business or profession.
- Government information. Occasionally people contact us for access to government information. This is different from personal information. For access to government information, contact the Information Commissioner of Canada.

4. Ten General Principles[6]

There are 10 principles, typically incorporated in legislation governing use of personal information, you need to keep in mind. It is good practice to follow these principles regardless of whether or not your charity is required by law to adhere to them:

1. **Accountability** - A charity is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the charity's compliance with privacy principles.

[6] From https://www.charitycentral.ca/book/export/html/402

2. **Identifying purpose**s - The purposes for which personal information is collected shall be identified by the charity at or before the time the information is collected.

3. **Consent** - The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. **Limiting collection** - The collection of personal information shall be limited to that which is necessary for the purposes identified by the charity. Information shall be collected by fair and lawful means.

5. **Limiting use, disclosure, and retention**- Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. **Accuracy** - Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards** - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness** - A charity shall make readily available to individuals' specific information about its policies and practices relating to the management of personal information.

9. **Individual access** - Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging compliance** - An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the charity's compliance.

Asking for Health Cards[7]: In general, homeless serving system organizations (that are not health care related) should not ask people to produce a health card. Only the following can or should ask someone to produce a health card:

- health care providers in your province (e.g. doctor's offices, walk-in clinics, hospitals)
- schools who need to keep a child's health information on-hand, for medical reasons

If you use your health card as identification, those you show it to should not record or copy the information on it.

[7] From https://www.ontario.ca/page/personal-information-and-privacy-rules

5. Privacy Related Documents You Should Create[8]

The following are privacy related documents you should create for your By-Name List/Coordinated Access/HMIS. You will have to create the following if you are using HIFIS 4 but beyond that, the following are simply good practice. See "Quick Resources" for community level examples.

1. **Privacy Impact Assessment (PIA)**

   A privacy impact assessment (PIA) is a process used to determine how a program or service could affect the privacy of an individual. It can also help to eliminate or reduce potential privacy risks resulting from that program or service. Overall, a PIA helps promote transparency and accountability regarding how organizations manage personal information. In some circumstances PIA's are required by legislation and in other areas they may be governed by organizational policy rather than mandated by legislation.

   The following information could be included in a PIA:

   - Data sharing among organizations;
   - Collection of clients' consents for: use and disclosure of client information or migration of personal information from a legacy system
   - Data collection and storage;
   - Access to client information;
   - Access model and permissions granted to users;
   - Disclosure of personal data to the ESDC and the Government of Canada;
   - Measure of protection and security of personal information

Here are some sample PIA resources:

- Federal information about PIA's - Required for virtually all federal government institutions for new or redesigned programs and services that raise privacy issues. Completed PIA's are submitted to the Treasury Board of Canada Secretariat.
- Privacy Impact Assessment Guidance Document - This resource was created by using resources developed by Office of the Information and Privacy Commissioners from across Canada, in particular, we relied heavily on resources developed by Ontario's Office of the Information and Privacy Commissioner as well as Alberta's Office of the Information and Privacy Commissioner.
- Ontario Privacy Impact Assessment Guide (for FIPPA and MFIPPA)
- Government of Nova Scotia Privacy Impact Assessment Template
- Newfoundland/Labrador Guide to Completing a PIA
- Alberta
    - PIA's required in some situations:
        - Section 64 of the *Health Information Act* (HIA) requires submission of a PIA for review by the OIPC.
        - Under the *Freedom of Information and Protection of Privacy Act* and *Personal Information Protection Act*, the OIPC encourages public bodies and organizations to submit PIAs

[8] Adapted from the HIFIS Implementation Guide with PIA resources from Google search

- Sample template PIA's:
  - PIA - Provincial (.doc) This template is intended for Government of Alberta departments, as well as agencies, boards and commissions.
  - PIA - Local (.doc) This template is for local public bodies, such as school jurisdictions, municipalities, police services or commissions, Metis settlements or libraries.

2. **Data Sharing Agreement – Between the List/HMIS Host and Service Providers (Agency Level)**

   A Data Sharing Agreement to obtain authority to share client personal information with each other. The Data Sharing Agreement will usually outline the purpose of data sharing, including a description of the data, the roles and responsibilities of participants, the privacy and security protocols, and other relevant data management practices.

3. **Confidentiality and User Agreement – Signed by List/HIFIS users (Individual Staff Level)**

   A Confidentiality and User Agreement (CUA) is a legal contract between parties agreeing not to disclose information specified in the agreement. Prior to having access to HIFIS, users could be required to sign a CUA that outlines their responsibilities respecting clients' personal information.

4. **Client Consent Form – Signed by the client (Client Level)**

   To collect, use and disclose personal information from clients, service providers are required to obtain consent from clients, which is normally done via a client consent form (consent form). The consent form should provide information on the personal information being collected and the purpose for which it is collected. For example, it should inform individuals who their personal information (on an identifiable and/or non-directly identifiable basis) will be shared with (e.g., local homeless serving system, province and/or ESDC and other federal departments for the purposes of analysis, research and evaluation of policies and programs).

APPENDIX A
Provincial Privacy Legislation[9]

Alberta

The Information and Privacy Commissioner of Alberta is responsible for overseeing and enforcing the following provincial access and privacy laws:

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

British Columbia

The Information and Privacy Commissioner for British Columbia is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Freedom of Information and Protection of Privacy Act* (FIPPA) - BC's public sector privacy law;
- *Personal Information Protection Act* (PIPA) - 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* (PHIAPPA) - BC's privacy law relating to health records.

Manitoba

The Office of the Ombudsman is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Freedom of Information and Protection of Privacy Act* (FIPPA) - Manitoba's public sector privacy law
- *Personal Health Information Act* (PHIA) – Manitoba's privacy law relating to health records

New Brunswick

The Office of the Integrity Commissioner for New Brunswick is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Right to Information and Protection of Privacy Act* (RIPPA) - New Brunswick's public sector privacy law

[9] Information in IPC contacts and legislation from https://www.priv.gc.ca/en. Further information on which legislation generally impacts different bodies was added from websites and/or conversations with the provincial oversight bodies.

- *Personal Health Information Privacy and Access Act*, (PHIPAA) - 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

The Office of the Information and Privacy Commissioner for Newfoundland and Labrador is responsible for overseeing and enforcing the following provincial access and privacy laws:

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

Northwest Territories

The Information and Privacy Commissioner of the Northwest Territories is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Access to Information and Protection of Privacy Act* (AIPPA) - The Northwest Territories' public sector privacy law
- *Health Information Act* (HIA) - The Northwest Territories' privacy law relating to health records.

Nunavut

The Information and Privacy Commissioner of Nunavut is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Access to Information and Protection of Privacy Act* (AIPPA) - Nunavut's public sector privacy law.

Nova Scotia

The Information and Privacy Commissioner of Nova Scotia is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Privacy Review Officer Act* (PROA) - Nova Scotia's public sector privacy laws
- *Personal Health Information Act* (PHIA) - Nova Scotia's privacy law relating to health records that has been 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* (MGA)
- *Personal Information International Disclosure Protection Act* (PIIDPA)

Ontario

The Information and Privacy Commissioner of Ontario (IPC) is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Freedom of Information and Protection of Privacy Act* (FIPPA) - Ontario's provincial public sector privacy law - applies to Ontario's provincial ministries and most provincial agencies, boards and commissions, as well as community colleges, universities, Local Health Integration Networks (LHINs) and hospitals (as of January 1, 2012)
- *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) - Ontario's municipal public sector privacy law - applies to local government institutions, including municipalities, police services boards, school boards, conservation authorities, boards of health and transit commissions
- *Personal Health Information Protection Act, 2004* (PHIPA), Ontario's privacy law relating to health records that has been that has been deemed "substantially similar" to the federal private sector privacy law (PIPEDA) with respect to health information custodians. See this further PHIPA Orientation – a quick summary with resources.

Municipalities generally fall under: MFIPPA with different areas falling primarily under other legislation as appropriate (e.g., Long-Term Care Homes under PHIPA and airports under federal PEPIDA for commercial activities). For FIPPA and MFIPPA, consent is not necessary for collecting personal information, and instead, other criteria set out in the act must be satisfied. Some local public health organizations are covered by MFIPPA.

Not-for-profit/charitable (not health custodians) generally fall under: The Ontario government does **not** regulate the privacy practices of charitable or non-profit organizations. Some of their commercial activities may be covered by the federal PIPEDA[10].

Health organizations generally fall under: PHIPA (health custodians) and FIPPA (hospitals). Some local public health organizations are covered by MFIPPA. In some cases, health organizations may fall under two laws.

Prince Edward Island

The Information and Privacy Commissioner of Prince Edward Island is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Freedom of Information and Protection of Privacy Act* (FIPPA) - PEI's public sector privacy law.

[10] https://www.ontario.ca/page/personal-information-and-privacy-rules

Québec

The Commission d'accès à l'information du Québec is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *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.

Saskatchewan

The Information and Privacy Commissioner of Saskatchewan is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Freedom of Information and Protection of Privacy Act* (FIPPA), Saskatchewan's provincial public sector privacy law
- *Local Authority Freedom of Information and Protection of Privacy Act* (LAFIPPA), Saskatchewan's municipal public sector privacy law
- *Health Information Protection Act* (HIPA), Saskatchewan's privacy law relating to health records.

Yukon

The Ombudsman and Information and Privacy Commissioner of the Yukon is responsible for overseeing and enforcing the following provincial access and privacy laws:

- *Access to Information and Protection of Privacy Act* (AIPPA) - Yukon's public sector privacy law
- *Health Information Privacy and Management Act* (HIPMA) - Yukon's privacy law relating to health records.