CONTENTS

3 Is This Resource for You?
5 Landscape of Privacy in Canada
6 Federal Privacy Laws
8 Provincial and Territorial Privacy Laws
15 OCAP and First Nations
16 International Privacy Frameworks
19 Conclusion
21 Appendix
Are you collaborating with a partner in another jurisdiction?
If yes, think about what jurisdictional legislation may apply.

Are you working with a provincial, federal, or private sector partner?
If yes, think about what type of privacy legislation may apply.

Are you working with specific sectors (e.g., healthcare, finance)?
If yes, think about what additional legislation exists (beyond privacy) that may affect how you manage data.

This resource highlights various privacy legislation that might apply to your research.
Emily Carr University and its employees are governed by several different privacy documents.

---

**Freedom of Information and Protection of Privacy Act (FIPPA)**

---

University policies + procedures, including but not limited to:

- 5.1 Ethics in Research (and associated procedures)
- 8.13 Confidentiality (and associated procedure)
- 9.6 Information Protection
- 9.3 Code of Conduct for Appropriate Use of Information Technology, Facilities + Services
- Employee Code of Conduct

---

Applicable professional regulations (e.g., TCPS 2 for researchers, financial reporting requirements)

---

All ECU employees are bound by the above. However, research material is exempted from FIPPA to prevent the public from accessing a researcher’s materials through “freedom of information” requests. That said, as ECU employees, researchers are still required to follow university policies and best practices, in addition to their ethics obligations.
LANDSCAPE OF PRIVACY IN CANADA

The following section will highlight different types of privacy legislation in Canada and internationally.

It gives an idea of how privacy is addressed at a provincial and federal level, within the public and private sector, and also within the healthcare field. The guide is not exhaustive, but it aims to bring to the reader’s attention any unique provisions that may be of interest.

It includes:
- Federal privacy laws
- Provincial and territorial privacy laws
- OCAP and First Nations
- Laws outside Canada

What are your legal privacy obligations?
FEDERAL PRIVACY LAWS

Researchers working in close collaborations with federal government institutions should be familiar with ATIA and PA, as well as all other federal policies, standards and directives that flow from their research.

Privacy Act (PA)
R.S.C., 1985, c.P-21

Access to Information Act (ATIA)
R.S.C., 1985, c.A-1

The PA and ATIA explain how federally regulated federal public bodies can collect, use, and disclose personal information.
Depending on the jurisdiction of research, one or more statutes may need to be considered. For example, an Emily Carr University researcher collaborating with Ontario healthcare may have to consider both BC’s and Ontario’s public and health sector laws. The following are BC and Canada’s public vs private laws:

— Public sector (e.g. government, government agencies, BC universities + colleges):
  — BC: *Freedom of Information and Protection of Privacy* (FIPPA)
  — Canada: *Privacy Act*

— Private sector (e.g. business, not-for-profits):
  — BC: *Personal Information Protection Act* (PIPA)
  — Canada: *Personal Information Protection & Electronic Documents Act* (PIPEDA)

*Under the TCPS 2, researchers are responsible for understanding and complying with the privacy legislation that applies to their context. It also stresses the duty of confidentiality and safeguarding personal information.*
Oversight

Federal and provincial “privacy commissioners” oversee the privacy and security practices of organizations dealing with personal (including health) information in Canada. The Office of the Information and Privacy commissioner (OIPC) of BC provides independent oversight, engages in investigations, rulings, guidelines and support.

*REBs also play an important, legally dedicated, oversight role in data research.*
FOIPPA
What it is: FOIPPA (aka FIPPA) ensures that public bodies are open and accountable to the public by providing a right of access to records and information maintained or controlled by a public body, and it prevents the unauthorized collection, use or disclosure of personal information by public bodies.
Who it’s for: Public bodies in British Columbia and Alberta each have FIPPA (very similar but not identical).

FOIPOP
What it is: FOIPOP provides public with access to records in the custody or control of institutions.
Who it’s for: Public bodies in Saskatchewan, Ontario and Nova Scotia.

FIPPA
What it is: FIPPA provides a right of access to information in records and also protects personal information. It establishes rules for the collection, use and disclosure of personal information by public bodies.
Who it’s for: Public bodies in Manitoba.

ATIPPA
What it is: The ATIPPA is promotes accountability and transparency in the public sector by allowing individuals access to records and information maintained or controlled by a public body, and it prevents the unauthorized collection, use or disclosure of personal information by public bodies.
Who it’s for: Public bodies in Yukon, Newfoundland and Labrador.

ACCESS ACT
What it is: Access Act represents two fundamental rights set out in the Quebec Charter of Human Rights and Freedom: the right to information, and the right to privacy.
Who it’s for: Public bodies in Quebec.

PHIPAA
What it is: Provincial privacy legislation in the context of health and medical information, but applies equally to non-health related personal information (like an address or date of birth).
Who it’s for: Public bodies in New Brunswick.

PROVINCIAL AND TERRITORIAL PRIVACY LAWS

Every province and territory in Canada has their own specific public sector privacy legislation.

See slides 11-14 for a comparison of public vs. private sector.
PIPEDA
What it is: PIPEDA applies only to a “federal work, undertaking, or business” as defined by the Act. Consent is considered to be the cornerstone of the Act which heavily focuses on accountability and ethical use of personal information and/or on a risk-based approach.
Who it's for: Applies to private organizations in Saskatchewan, Manitoba, Ontario, Newfoundland and Labrador and Nova scotia.

PIPA
What it is: The PIPAs apply to the collection, use and disclosure of personal information, with obligations of reasonableness, consent and consent. Any organization to which PIPA applies is exempted from the federal legislation.
Who it's for: Private-sector organizations in British Columbia and Alberta – each province enacted PIPA, independent of each other.

PIPHA
What it is: PHIPA provides a set of rules for the collection, use, and disclosure of personal health information. Health information custodians are required under the act to treat all personal health information as confidential and maintain its security.
Who it's for: “Health information custodians” in Ontario.

PRIVATE SECTOR ACT
What it is: The Private Sector Act principles for the private sector businesses, to collect, store, and disclose information.
Who it's for: The Private Sector Act applies to any person or company carrying on an enterprise in the province of Quebec, who collects, holds, uses or communicates personal information.

PHIA
What it is: Provincial privacy legislation in the context of health and medical information, but applies equally to non-health related personal information (like an address or date of birth).

PROVINCIAL AND TERRITORIAL PRIVACY LAWS

Only BC, AB and QC have their own private sector privacy legislation which supersedes PIPEDA. All other provinces must comply with PIPEDA.
## PROVINCIAL AND TERRITORIAL PRIVACY LAWS

<table>
<thead>
<tr>
<th>Province</th>
<th>Public Sector</th>
<th>Private Sector</th>
<th>Health Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>— FIPPA is one of strictest public sector laws in Canada, if not North America</td>
<td>— PIPA is “substantially similar” to the federal private sector privacy law (PIPEDA)</td>
<td>— E-health applies to designated databases containing personal health information, called “health information banks”</td>
</tr>
<tr>
<td></td>
<td>— FIPPA prohibits transborder data flow (S.30.1) - personal information in custody or control must be stored and accessed ONLY in Canada (provides for exceptions: must follow prescribed manner to obtained informed consent for use)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Main compliance principles are to provide notice + knowledge.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>— What PI is needed/may be collected</td>
<td>— Purpose for collection of PI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Purpose for collection of PI</td>
<td>— How PI is used, collected, accessed or stored</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— How PI is used, collected, accessed or stored</td>
<td>— Storage, location + duration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Storage, location + duration</td>
<td>— Personal information safeguards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Personal information safeguards</td>
<td>— Implications/risks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Implications/risks</td>
<td>— Obtain informed meaningful + voluntary consent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Obtain informed meaningful + voluntary consent</td>
<td>— Provide for risk mitigation</td>
<td></td>
</tr>
</tbody>
</table>

These tables are not exhaustive. Please visit the [OPC website](https://www.priv.gc.ca) for more information.
<table>
<thead>
<tr>
<th>Province</th>
<th>Public Sector</th>
<th>Private Sector</th>
<th>Health Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB</td>
<td><strong>Freedom of Information and Protection of Privacy Act (FOIPPA)</strong></td>
<td><strong>Personal Information Protection Act (PIPA):</strong></td>
<td><strong>Health Information Act (HIA):</strong></td>
</tr>
<tr>
<td></td>
<td>— Applies to government institutions,</td>
<td>—“substantially similar” to the federal private sector privacy law</td>
<td>— Relates to health records</td>
</tr>
<tr>
<td></td>
<td><strong>Local Authority Freedom of Information and Protection of Privacy Act</strong></td>
<td>— PIPA has mandatory breach notification</td>
<td>— Provisions permit the collection, use, and disclosure of non-identifying</td>
</tr>
<tr>
<td></td>
<td>(FOIPOP)</td>
<td></td>
<td>health information for any purpose</td>
</tr>
<tr>
<td></td>
<td>— Applies to local authorities, including post-secondary institutions</td>
<td></td>
<td>— HIA empowers the ethics review board to determine whether consent is</td>
</tr>
<tr>
<td>SK</td>
<td><strong>Freedom of Information and Protection of Privacy Act</strong></td>
<td><strong>Freedom of Information and Protection of Privacy Act (PIPEDA):</strong></td>
<td>required from an individual for research</td>
</tr>
<tr>
<td></td>
<td>— Applies to government institutions,</td>
<td>— Does NOT prohibit transborder data flow</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Local Authority Freedom of Information and Protection of Privacy Act</strong></td>
<td>— Collection, use and disclosure of personal information without knowledge or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(FOIPOP)</td>
<td>consent as long as the information is publicly available</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— Applies to local authorities, including post-secondary institutions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These tables are not exhaustive. Please visit the OPC website for more information.
## PROVINCIAL AND TERRITORIAL PRIVACY LAWS

<table>
<thead>
<tr>
<th>Province</th>
<th>Public Sector</th>
<th>Private Sector</th>
<th>Health Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ON</strong></td>
<td><strong>Freedom of Information and Protection of Privacy Act (FOIPOP)</strong></td>
<td><strong>Freedom of Information and Protection of Privacy Act (PIPEDA):</strong></td>
<td><strong>Personal Health Information Protection Act (PHIA):</strong></td>
</tr>
</tbody>
</table>
|          | **Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)** | — Does NOT prohibit transborder data flow | — “substantially similar” to the PIPEDA  
— Establishes risks for individuals  
— Imposes obligations on “health information custodians” for protecting PI |
| **QC**   | **An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (Access to information):** | **Act Respecting the Protection of Personal Information in the Private Sector:** | — Québec has several privacy laws relating to health records. Laws are overseen and enforced by the Commission d’accès à l’information du Québec.  
— QC privacy is also governed by the Civil Code of Quebec (C.C.Q) |

These tables are not exhaustive. Please visit the [OPC website](#) for more information.
# PROVINCIAL AND TERRITORIAL PRIVACY LAWS

<table>
<thead>
<tr>
<th>Province</th>
<th>Public Sector</th>
<th>Private Sector</th>
<th>Health Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS</td>
<td><strong>Freedom of Information and Protection of Privacy Act (FOIPOP):</strong>&lt;br&gt;Part XX of the Municipal Government Act:&lt;br&gt;— Applies to municipal bodies&lt;br&gt;<strong>Personal Informational International Disclosure Protection Act (PIIDPA):</strong>&lt;br&gt;— Similar language as BC re. trans-border data flows (i.e. personal information in custody or control must be stored and accessed ONLY in Canada (provides for exemptions: must follow prescribed manner to obtained informed consent for use)</td>
<td><strong>Freedom of Information and Protection of Privacy Act (PIPEDA):</strong>&lt;br&gt;— No specific privacy legislation in private sector. Instead, PIPEDA applies to the private sector.&lt;br&gt;— Collection, use and disclosure of personal information without knowledge or consent as long as the information is publicly available</td>
<td><strong>Personal Health Information Act (PHIA):</strong>&lt;br&gt;— Relates to health records&lt;br&gt;— “substantially similar” to the federal private sector privacy law with respect to health information custodians</td>
</tr>
</tbody>
</table>

*These tables are not exhaustive. Please visit the [OPC website](https://www.priv.gc.ca) for more information.*
OCAP is widely referenced framework for First Nations governance over research, community knowledge, and data, as it relates to ownership, control, access and possession.

The principles of ownership, control, access and possession (OCAP) have been developed as an accepted, standalone framework for researchers to follow with respect to data and information management prior to, during and after a project has been completed.

OCAP is consistently and judiciously applied wherever applicable. Generally, it is assumed that the Acts give OCAP broad authority. Where OCAP principles are not fully integrated into Canada’s privacy regime and voids exist, other legislative framework (e.g., FIPPA) are employed to fill these gaps and to minimize any potential liabilities under the provincial Acts.

Many First Nations communities have developed their own protocols around privacy. These are implemented at the community, regional and national levels.

For more information regarding OCAP visit the FNIGC national website at www.fnigc.ca or the AFNIGC regional website at www.afnigc.ca.
There are privacy concerns related to the transnational flow of data, and it is especially important if a researcher (and/or their collaborator) is transferring data to another jurisdiction. One way for researchers to address these privacy concerns is to familiarize themselves with privacy requirements outside of Canada.
Are you collecting research data from EU residents?
Any collection, use, disclosure, or storage of personal data belonging to individuals living in the EU (EU residents, not citizens) must comply with the GDPR — regardless of where the actual data processing occurs.

Researchers should understand if GDPR is applicable (there are certain research exemptions), if there is a “lawful basis for processing” (GDPR, art. 6) such as consent, and to ensure there are appropriate safeguards in place.
In the US, *sector specific* data protection laws and regulations work together with state-level legislation.

Privacy is enforced through government bodies such as the Federal Communication Commission (FCC), Federal Trade Commission (FTC), and non-profit privacy organizations such as the American Civil Liberties Union (ACLU) or the Electronic Frontier Foundation (EFF) which provide a legal framework for them.

Once Canadians’ personal information is transferred to the US, it is subject to their law, including the PATRIOT Act. The PATRIOT Act allows search/seizure of data held on US servers without requiring court orders/intervention.
— There are many privacy laws!
— Researchers have a professional responsibility to adhere to the laws, the ethical norms and codes of conduct appropriate, as per university policies and procedures.
— Research conducted at ECU is expected to adhere to these laws, REB requirements, norms and standards.
— If you are collaborating with partners from other jurisdictions (and sectors, such as the health sector), you have to be aware of what legislation applies and to whom. Each research project is unique, and privacy should be assessed on a case-by-case basis.
— Decide whether there are adequate provisions to protect the privacy of your research subjects and maintain the confidentiality of the identifiable data at each segment of your research, from recruitment to maintenance to disposal of the data.
The Privacy + Access office is part of the university HR department, and is responsible for:

— Overseeing university compliance with FIPPA and privacy best practices, including supporting ECU privacy policies, procedures, and guidelines;
— Providing advice and training to faculty and staff on FIPPA-related matters;
— Investigating complaints about alleged violations of privacy and requests for correction of personal information;
— Responding to FOI requests;
— Assisting investigations and inquiries by BC's Office of the Information and Privacy Commissioner;
— Conducting Privacy Impact Assessments.

Contact us: privacy@ecuad.ca
APPENDIX 1: PRIVACY BEST PRACTICES

1. Determining the research objectives and justifying the data needed to fulfill these objectives
2. Limiting the collection of personal data
3. Determining whether consent from individuals is required
4. Managing and documenting consent
5. Informing prospective research participants about the research
6. Safeguarding personal data
7. Controlling access and disclosure of personal data
8. Setting reasonable limits or retention of personal data
9. Ensuring accountability and transparency in the management of personal data

The best practices are firmly embedded in commitments to TCPS 2.
## APPENDIX 2:
AREAS OF SPECIAL INTEREST IN LEGISLATION

<table>
<thead>
<tr>
<th>AREAS OF SPECIAL INTEREST</th>
<th>FIPPA</th>
<th>REQUIREMENT</th>
</tr>
</thead>
</table>
| Collection                | s.26  | 26  A public body may collect personal information only if  
|                           |       | (a) the collection of the information is expressly authorized under an Act,  
|                           |       | (b) the information is collected for the purposes of law enforcement,  
|                           |       | (c) the information relates directly to and is necessary for a program or activity of the  
|                           |       | public body,  
|                           |       | (d) with respect to personal information collected for a prescribed purpose,  
|                           |       | (i) the individual the information is about has consented in the prescribed manner to  
|                           |       | that collection, and  
|                           |       | (ii) a reasonable person would consider that collection appropriate in the  
|                           |       | circumstances,  
|                           |       | (e) the information is necessary for the purposes of planning or evaluating a program  
|                           |       | or activity of a public body,  
|                           |       | [...] |
|                           | s.27  | 27 (2) A public body must ensure that an individual from whom it collects personal  
|                           |       | information is told  
|                           |       | (a) the purpose for collecting it,  
|                           |       | (b) the legal authority for collecting it, and  
|                           |       | (c) the title, business address and business telephone number of an officer or  
|                           |       | employee of the public body who can answer the individual's questions about the  
|                           |       | collection. |
## APPENDIX 2:
### AREAS OF SPECIAL INTEREST IN LEGISLATION

<table>
<thead>
<tr>
<th>AREAS OF SPECIAL INTEREST</th>
<th>FIPPA</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>s.30</td>
<td><strong>30</strong> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.</td>
</tr>
<tr>
<td>Storage</td>
<td>s.30.1</td>
<td>Stored in Canada unless otherwise authorized by FIPPA</td>
</tr>
<tr>
<td>Retention + Disposal</td>
<td>s.31</td>
<td><strong>31</strong> If an individual's personal information (a) is in the custody or under the control of a public body, and (b) is used by or on behalf of the public body to make a decision that directly affects the individual, the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.</td>
</tr>
<tr>
<td>Use</td>
<td>s.32</td>
<td><strong>32</strong> A public body may use personal information in its custody or under its control only (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34), (b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or (c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.</td>
</tr>
</tbody>
</table>
—FIPPA is available online at: www.bclaws.ca/eplibraries/bclaws_new/document/id/freeside/96165_00
—Relevant information about FIPPA is also available on the OIPC’s website at: www.oipc.bc.ca
—The BC government has also developed some additional information and privacy materials that may be useful to you in understanding FIPPA or in making an access request or privacy complaint at: www.cio.gov.bc.ca/cio/priv_leg/foippa/index.page
—FOIPPA Policy and Procedures Manual
—Guide to FIPPA
   —https://www.oipc.bc.ca/guidance-documents/1466
—Provincial and territorial privacy laws and oversight
—The Researcher’s Guide to Data Privacy (UBC)
   —https://universitycounsel.ubc.ca/files/2014/01/The-Researchers-Guide-to-Data-Privacy.pdf
—Top Ten Tips for Privacy in Research (UBC)
—Key Steps to Responding to Privacy Breaches
   —http://www.oipc.bc.ca/guidance-documents/1428
—Protecting Personal Information Outside the Office
   —http://www.oipc.bc.ca/guidance-documents/1447