INTRODUCTION TO PRIVACY IN RESEARCH

Click on the tag for the extended resource with more information:
CONTENTS

3 Is this Resource for You?
6 Definitions
10 Privacy, Law + Research
12 TCPS 2 + Privacy
13 ECU + Privacy
14 Conclusion
16-20 Appendix
IS THIS RESOURCE FOR YOU?

Does your research involve personal information?

Are you working on research involving human participants?

If you answered yes to any of these questions, you need to be aware of your privacy obligations under legislation and university policy.

Are you collaborating with other researchers in the private sector, health sector, or outside of BC?
Introduce the application of the Freedom of Information and Protection of Privacy Act (FIPPA) to ECU research;

Identify some key privacy principles and requirements; and

Highlight your legal privacy obligations.
“New technologies provide researchers with the ability to work with larger data sets than ever before, and to share data around the world. **The risks to personal information today, therefore, are far greater than in the past,** and it is reasonable for people to expect that their personal information, if it is subject to academic research, will be protected”

-Elizabeth Denham, Former Commissioner, OIPC BC, 2015
DEFINITIONS

“RECORD”
Any information recorded or stored by any means whether in hard copy or in electronic format.

“PERSONAL INFORMATION”
Recorded information about an identifiable individual other than contact information.
- May directly identify a specific individual (e.g. name and street address).
- Any element of a combination of elements that allows indirect identification of an individual (e.g. if birth date combined with postal code and other personal information on the record such as ethnicity could lead to the identification of an individual).

“CONTROL”
Authority to manage, restrict, regulate or administer the use or disclosure of a record.

“CUSTODY”
- Physical possession of the record.
- May not be responsible for the actual content of the record.
- Responsible for providing access to an security of the record.
- Responsible for managing, maintaining, preserving and disposing of the record.

TCPS 2 DEFINITION
“personal information” generally denotes identifiable information relating a person. It includes information about personal characteristics such as culture, age, religion and social status, as well as their life experiences and educational or employment histories.”
Tri-Council Policy Statement 2 (“TCPS 2”) p.56

Tri-Council Policy Statement 2 ("TCPS 2") p.56
At the outset of the research design process, researchers should:

- Identify and document research objectives and question as a basis for determining what data will be needed;
- Anticipate and document research questions related to the primary research objectives, which might become relevant after the initial data analysis; and
- Anticipate and document likely future uses of the data, including possible collaborations with other researchers or possible commercial use.

The TCPS2 generally requires “full and frank disclosure” of all relevant information, including detailed information about handling of private and sensitive information (TCPS2 2014, arts. 2.7 & 3.2). Consent requirements include detailed information about how data will be managed, though a research ethics board (REB) may waive or modify consent requirements where research is minimal risk, unlikely to adversely affect participant rights and welfare, transparent, and where consent is not practicable (TCPS2 2014, art. 2.1).
What type of information are you collecting and using in your research?

Does your research involve personal health information?
TYPES OF PERSONAL INFORMATION

**Personal Information:** Direct identifiable personal information (e.g. name and street address, personal health number, etc.) or any element that allows indirect identification of an individual (e.g. if birth date combined with postal code and other personal information on the record such as ethnicity could lead to the identification of an individual).

**Personal Health Information:** One of the most sensitive types of personal information because it encompasses the physical, mental and emotional status of individuals over their lifetime.

The following provinces have health-related privacy laws:
- Ontario;
- New Brunswick;
- Newfoundland and Labrador; and
- Nova Scotia.
What are the key challenges for researchers?

- Understanding privacy obligations
- Ensuring the research team is aware of their obligations – what type of training, who, to what extent, etc.
- Identifying and mitigating privacy risks early on, and throughout the course of research
- Having the necessary tools to protect privacy
Respect for privacy in research is an internationally recognized norm and ethical standard.

Researchers have an ethical duty to safeguard personal information and ensure informed meaningful consent for research participants.

Global trends of stricter privacy legislation.

Increasing number of privacy and data breaches around the world.

Failure to comply can result in an investigation or audit through the OIPC or funding agency; this can suspend research and negatively impact the perception of your practices.

Why should you care?
Researchers’ Legal Responsibility

“In addition to the principles and guidelines in this Policy, researchers are responsible for ascertaining and complying with all applicable legal and regulatory requirements with respect to consent and the protection of privacy of participants”

TCPS 2, 2014, p.26
Emily Carr University and its employees are governed by several different privacy documents.

ECU + PRIVACY

— **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.
The ethical conduct of research involving humans is governed by guidelines and by privacy legislation.

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.

Take appropriate measures to protect the privacy of research participants, to ensure the confidentiality of their personal information, and to minimize harms to them.

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. Ensure adequate privacy protection of your research subjects’ data at each segment of your research, from recruitment to maintenance to disposal.
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
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>
<tbody>
<tr>
<td>Collection</td>
<td>s.26</td>
<td>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, [...]</td>
</tr>
<tr>
<td></td>
<td>s.27</td>
<td>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.</td>
</tr>
</tbody>
</table>
# 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 for (a) 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>
LINKS TO RESOURCES

— 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