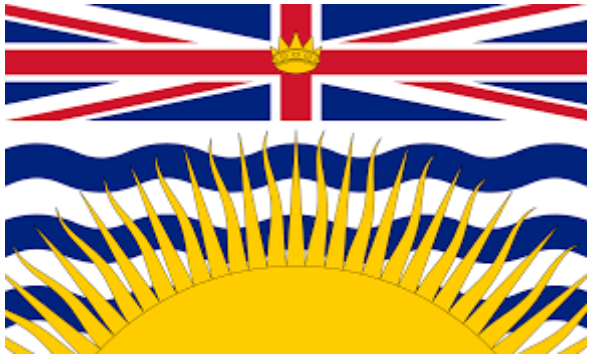
FIPPA Basics

Stephen Gaspar, UFV Legal Counsel

Public Sector Privacy Legislation



Provincial

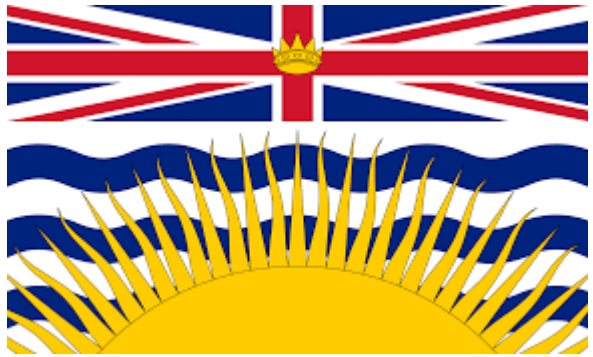
Freedom of Information and Protection of Privacy Act (FIPPA, FOIPPA)

Federal

1. *Access to Information Act*

2. *Privacy Act*

Private Sector Privacy Legislation



Provincial

Personal Information Protection Act (PIPA)

Federal

Personal Information Protection and Electronic Documents Act (PIPEDA)

Who does FIPPA apply to?

- Public bodies
- Examples:
  - Government ministries
  - K-12 and post secondary institutions
  - Municipalities
  - Provincial Crown Corporations
  - Provincial government agencies
  - Schedules 2 and 3 of FIPPA provide a complete list

FIPPA affects all UFV Employees

- UFV is a public body
- As a public body employee, you are required to manage information as part of your job
- That means that your work must be carried out in accordance with FIPPA

The Four Domains of Information Management

- Records Management, Access to Information, Privacy, and Security are all essential to the management of information held by public bodies

1. **Records Management:** is the system an organization uses to capture and maintain information associated with its activities. Examples include printed documents, emails, and notes.
2. **Access:** Public bodies are accountable to the public for ensuring access to records under the custody or control of the public body, with limited exceptions. This includes individuals' right of access to their personal information.

The Four Domains of Information Management (continued…)

3. **Privacy:** Privacy is protected by public bodies treating personal information responsibly and lawfully. This includes ensuring personal information is collected, used, and disclosed appropriately
4. **Security:** Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability of that information or system.

Note: These slides are focused on Access and Privacy but it is important for you to be aware of the other two domains

Custody and Control

- FIPPA applies to all records in the “custody” or under the “control” of UFV unless explicitly outside the scope of the Act
  - **Custody:** means the physical possession of a record, and normally includes responsibility for access to, and security of, that record, as well as managing, maintaining, preserving and disposing of it.
  - **Control:** means the authority to make decisions about how a record ought to be managed. This means that if UFV has control of a record even though it does not have custody of a record, the record may still be subject to FIPPA. For example, a record that is held by a service provider may be under UFV’s control even if not in its custody.

Access

- Under FIPPA, individuals have a right of access to:
  1. Their own personal information held by UFV
  2. General information held by UFV, including information about UFV's operations, programs and services, with limited exceptions
- Anyone, including individuals, businesses (whether for-profit or non-profit), researchers, interest groups may make an FOI request
- A request may be made in any written format.
- Generally, at UFV these are directed to the Privacy Office and are sent to our email account: FIPPA@ufv.ca.

Access: Employee tips

- It is not always the case that the request will be sent to the Privacy Office
  - If you have received an access request or have any questions about whether you may have, please contact the Privacy Office as soon as possible
- Be aware that any record you create may, one day, become the subject of an access request
- If a matter is particularly sensitive, consider whether a record needs to be created at all
- Be cautious in how email is used (i.e. humour and adjectives) and maintain professionalism
- Limit distribution of information to those who have a need to know

Access: FOI Exceptions to Disclosure

Public bodies must withhold information if disclosure would be:

- harmful to the business interests of a third party
- harmful to a third party's personal privacy
- harmful to the interests of an indigenous people

Public bodies may withhold the following information:

- Privileged information (i.e. Solicitor-Client privilege)
- Records of in-camera meetings
- Policy advice and recommendations (including draft documents)
- Information which, if disclosed, would be harmful to law enforcement; intergovernmental relations or negotiations; financial or economic interests of a public body; conservation of heritage sites; or, individual or public safety

Access: How long must records be retained?

- FIPPA establishes a 1 year minimum retention period for personal information that is used to make a decision that affects someone
- However, depending on the record other retention periods apply
- In general, transitory records do not need to be retained

Access: Key Points

- Any record that is created by an employee in course of performing duties may be requested
- Generally: records (i.e. emails) that are embarrassing or contain inappropriate comments cannot be excluded from production
- The FOI process cannot be avoided by using a personal email account
- UFV has a mandatory obligation to comply with FOI process

Protection of Privacy

What is “personal information”

- S. 1 of FIPPA: “Recorded information about an identifiable individual other than contact information”
  - Note: “contact information” means business contact information of employees or faculty (not personal contact information)
- Examples of “personal information” include (but are not limited to):
  - Name, SIN number, home address and telephone number, government ID card number, employee personal information, and many more things
    - Ask if in doubt

How personal information is protected by FIPPA

1. Public bodies must have legal authority to collect, use and disclose personal information. See section 26 of FIPPA for full list.
2. Most commonly used authority:
   - s. 26 (c) the information relates directly to and is necessary for a program or activity of the public body.
3. Information collected must be used in a way that is consistent with the purpose it was collected for in the first place

How personal information is protected by FIPPA (continued…)

4. Personal information must be collected in a lawful fashion (either directly from the affected individual) or one of the other methods described in s. 27 of FIPPA. A key requirement is the use of a collection notice (more info to follow)
5. FIPPA establishes safeguards regarding the collection, use and disclosure of personal information: (i.e. Privacy Impact Assessments)
6. FIPPA requires public bodies to be transparent and accountable regarding how they manage personal information

Collection Notices

- Required by section 27 of FIPPA
- With limited exceptions, public bodies must collect personal information directly from the person to whom it pertains
- Collection notices should include the following information:
  - The nature of information being collected
  - The legal authority for collecting the information
  - The contact information of an employee who can answer questions about the collection

Key points: Collection

- Collection: UFV should only collect personal information that is necessary for our operations
  - In practice, consider whether each piece of information requested on a form is actually necessary for the delivery of a program or service
  - If we ask for more information than we need then the risk to an individual of a privacy breach is potentially more severe

Key points: Use

- Personal information under our control should only be accessed by individuals on a “need to know basis”
- If an employee needs to know certain details of personal information to perform their duties then it should be limited to that amount of information
- Information collected for one purpose should not be used for another purpose without the individual’s consent

Key points: Disclosure

- Personal information under our control can be shared externally as authorized by part 3 of FIPPA. Generally, these instances are permissive (not mandatory). Examples include:

1. Law enforcement (to assist in a specific investigation)
2. If authorized or required by law
3. Certain other public bodies or agencies
4. “Compelling circumstances” related to public health or safety
5. Limited public interest exceptions

Privacy Impact Assessments (PIAs)

- Privacy Impact Assessments (PIAs) are required for all new or changed UFV initiatives
- A PIA is an assessment to determine if an initiative collects, uses, or discloses personal information in compliance with FIPPA
- A PIA includes the following:
  - A description of initiative and list of elements of personal information involved
  - Identification of sensitive personal information stored or accessed outside Canada
  - Legal authority to collect, use or disclose personal information
  - Description of security measures related to the initiative
  - Explanation of procedures to ensure accuracy, correction, and retention of personal information

Security of Personal Information

Things to keep in mind

- Assume all personal information that is collected and used by your area is “sensitive”
- It is important to establish safeguards to those accessing personal information to control who has access and that it is not being over-used

Privacy Breaches

- Information wrongfully accessed or disclosed
  - May arise from human error by employee (most common) or from wrongful access to our IT systems
  - Examples: laptop stolen from car (unencrypted), email with PI in body sent to wrong recipient
  - More broadly: any handling of PI in contravention of FIPPA

How to handle a Privacy Breach

- Basic Steps (to be carried out with assistance from Privacy Office):

1. **Report ASAP** to Supervisor and/or Privacy Office
2. **Contain** the breach to limit its impact (determine who may have wrongfully been given the PI)
3. **Assess** the scope and potential consequences (type of info and damage that could occur to the affected individual)
4. **Remediate:** In most cases, notification to affected individuals is required. In serious cases, further steps may be necessary.
5. **Prevent:** Consider what steps may be taken to prevent or mitigate future privacy breaches.
6. **Document:** Steps taken to respond to the privacy breach

- Any Questions?