PRIVACY – An Overview
Institute of Internal Auditors, NL Chapter

Janet O’Reilly, Access and Privacy Analyst
7 April, 2017
Privacy Under the ATIPPA, 2015

- Privacy under the ATIPPA, 2015 involves the protection of personal information from unauthorized collection, use and disclosure.

- All collection, use, disclosure and protection of personal information by public bodies is governed by ATIPPA, 2015.

- Citizens who believe there has been a failure to protect or an unauthorized collection, use or disclosure of their personal information may file a complaint with the OIPC.
PIPEDA and the Privacy Principles

- The Personal Information Protection and Electronic Documents Act is the Federal legislation that applies to personal information collected, used or disclosed in the course of commercial activities.

- This Act requires compliance with the 10 Privacy Principles set out in a schedule to the Act.

- The requirements of ATIPPA, 2015 are formulated based on the 10 Privacy Principles.
1. **Accountability**

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

2. **Identifying Purpose**

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
The 10 Privacy Principles

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 organization. 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 fulfilment 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.
The 10 Privacy Principles

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

8. Openness
   An organization 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 organization’s compliance.
What is Personal Information?

- **ATIPPA, 2015** defines it as “recorded information about an identifiable individual.” It includes, but is not limited to:
  - Name, address and telephone number
  - Race, ethnicity, religious or political beliefs
  - Age, sex, sexual orientation, marital status
  - Identifying numbers and symbols
  - Fingerprints, blood type and inheritable characteristics
  - Educational, financial, criminal or employment status or history
  - Opinions about an individual.

- **PIPEDA** defines personal information as “information about an identifiable individual”.

No personal information may be collected by a public body unless:

- the collection is expressly authorized by an Act,
- is collected for the purpose of law enforcement, or
- it relates directly to and is necessary for an operating program or activity of the public body.
ATIPPA, 2015 - Direct Collection

Information must come directly from the individual, unless:

- another method is authorized by the individual, the OIPC or an Act or regulation,
- it is collected as part of an authorized disclosure from another public body,
- in the interest of the individual and time circumstances do not permit collect directly from individual.
- the collection is for the purpose of -
  - determining suitability for an award;
  - an existing or anticipated proceeding before a court or judicial or quasi-judicial tribunal;
  - collecting a debt or fine; or
  - Law enforcement
Communication at time of Collection

• Under ATIPPA, 2015 a public body must inform the person
  1. the purpose for collecting,
  2. the legal authority for collecting it, and
  3. the contact information of someone who can answer questions/concerns.

• PIPEDA Accountability requires the identification of a person(s) responsible for compliance and Identifying Purpose requires this before collection.
Method of Collection

• Form of collection:
  • Written information (forms, applications etc.)
  • Verbal then converted to writing (record created)
  • Video
  • Audio recordings
  • Any electronic media
  • Transferred from another public body

• If decisions are made based on this information, the public body has an obligation to make every reasonable effort to ensure its accuracy (PIPEDA **Accuracy** Principle).
Use of Personal Information

• **ATIPPA, 2015** - Public body may use personal information only:
  • for the reason for which it was collected or a use consistent with that original purpose for collection,
  • where individual has consented to the use, or
  • for a disclosure authorized by the Act

• **PIPEDA Principle 5** - 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.
Limiting Principle

- **ATIPPA, 2015**
  - Collection, use and disclosure must be limited to minimum amount necessary to accomplish the purpose.

- **PIPEDA “Limiting Collection” and “Limiting Use, Disclosure and Retention” Principles**
  - 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.
ATIPPA, 2015 - Consent

• Generally, you need to get an individual’s consent before collecting, using or disclosing an individual’s personal information for a purpose other than that for which it was collected (or substantially similar).

• Written consent is the best method however verbal consent is acceptable if written consent cannot be obtained.

• Consent is not needed if the information is required for:
  • Criminal investigations
  • Court proceedings
  • Determining eligibility for a scholarship, honour or award
  • If the individual’s health and safety are at risk
PIPEDA - Consent

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

• Section 7(1) *PIPEDA* lists the exceptional circumstances where consent is not required, these are described in the Principle as:
  • legal, medical, or security reasons may make consent impossible or impractical
  • for the detection and prevention of fraud or for law enforcement
  • the individual is a minor, seriously ill, or mentally incapacitated
ATIPPA, 2015 - Disclosure of Personal Information

- Means showing, sending, or giving personal information to another division or outside department or agency.

- Public body may disclose information only:
  - in accordance with an Access Request, with exceptions to access applied,
  - when individual has consented,
  - for the reason for which it was collected or a use consistent with that original purpose for collection,
  - complying with or in accordance with an Act, or other listed authority,
Disclosure of Personal Information

- Public body may disclose information only (continued):
  - in compelling circumstances that affect a person’s health or safety,
  - to notify next of kin or a friend of illness or injury,
  - where disclosure would not be an unreasonable invasion of the person’s privacy, or
  - for common or integrated programs.
ATIPPA, 2015 - Access to, Correction of & Retention Personal Information

• Where a Public body uses personal information to make a decision that directly affects the individual, the public body must retain that information for at least one year so that the person has a reasonable opportunity to obtain access.

• Access to one’s own personal information held by a public body is permitted under the ATIPPA, 2015 at no charge,

• People may request a correction of their information. If refused, an annotation must be made and an explanation sent to the Applicant.
PIPEDA - Access to, Correction of & Retention Personal Information

The Accuracy Principle states that:

Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

The Individual Access Principle states that:

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. [and] When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required.
ATIPA, 2015 - Protection of Personal Information

• Public bodies must take reasonable steps to ensure that:
  • personal information is protected against theft, loss, unauthorized collection, access, use or disclosure;
  • records are protected against unauthorized copying or modification; and,
  • records are retained, transferred and disposed of securely.

• Notification to the individual of theft, loss, improper disposal or unauthorized access or disclosure *unless the Public Body reasonably believes the loss does not create a risk of significant harm*. 
The Safeguards Principle states:

- The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.
Questions