OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Privacy Management Programs

Ruth Marks and Stacey Pratt
April 2018

Agenda

- Quick overview of the *ATIPPA, 2015.*
- Public body responsibilities in *ATIPPA, 2015* administration.
- Role of the Privacy Officer.
- Assessing a public body's compliance with the *Act.*
- Development of policies and procedures.
- Understanding of continuing commitment to compliance.

Purposes of the Act

- Public right of access to records.
- Access to and correction of own personal information.
- Specific exceptions to right of access.
- Protect personal information.
- Independent review – OIPC.

Role of the OIPC

- Duties of the OIPC include:
  - investigating complaints regarding access to information requests and breaches of privacy;
  - receiving privacy breach notifications;
  - processing time extension and disregard requests;
  - conducting own motion investigations; and
  - additionally, the OIPC is responsible for education, advocacy, audits, commenting upon draft legislation and more.
- The OIPC is an independent office of the House of Assembly which utilizes a hybrid model (recommendations → Court orders).

Privacy – *ATIPPA, 2015*

- Privacy under the *ATIPPA, 2015* involves the protection of personal information from unauthorized collection, use and disclosure.
- Persons who believe there has been an unauthorized collection, use or disclosure of their personal information may file a complaint with the OIPC.

Protection of Personal Information

- How can public bodies protect personal information from unauthorized collection, use and disclosure?
  - Know what personal information it holds.
  - Know why it was collected (identified purpose).
  - Know how it is used.
  - Know to whom it is disclosed.
  - Know the legislative authorities for the above.

- May already be documented in PIAs.

Protection of Personal Information (section 64)

- 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*.

Privacy Management Program

- Developing a Privacy Management Program ("PMP") will assist public bodies in:
  - ensuring legislative compliance; and
  - demonstrating accountability.

Building a Culture of Accountability

- What can a public body do to build a culture of accountability?
  - Accept responsibility to protect privacy.
  - Develop and promote a PMP.
  - Ensure privacy is built into all initiatives, programs and services.
  - Build and maintain public trust.
  - Continually adapt your PMP as volume, type and sensitivity of PI held varies.

Setting up a PMP

- Appoint a project lead.
- Ensure oversight and support by executive.
- Involve HR, IM, Risk Management, Policy, Internal Audit, IT, and Information Security Personnel.
- Obtain outside privacy program development expertise (third party vendor, ATIPP Office, OIPC).
- Obtain and document the information necessary to assess compliance.
- Identify gaps and develop action plan.

Designating a Privacy Officer

- Designation of the Privacy Officer ("PO")
  - Fairly senior level.
  - Position, not an individual.
  - Full time versus part time: assess program resources, size of the organization and the designation of overall duties.
  - Budget for compliance.

Role of the PO in the PMP

- Establish relationships.
- Develop program controls.
- Identify necessary resources.
- Develop and deliver training and awareness.
- Assess the effectiveness of the program.
- Review and revise the program.

Training and Awareness

- Lack of awareness causes breaches.
- Employees should participate in mandatory privacy education (training and awareness).
- Provide knowledge of policy and procedures for all aspects of privacy protection.
- Goal for all employees is to recognize and address issues as they arise and create a culture of privacy.

Training and Awareness

- Delivery
  - New hire orientation.
  - Ongoing performance management.
  - Event driven updates and notices.
  - Periodic courses.
  - Workshops.
  - Newsletters.
  - Etc.

Executive Involvement

- Ensure executive receives regular reports on progress and any direction provided is implemented.
- Report any risks associated with non-compliance to executive.
- Provide a final report of findings to executive.
- Complete any others steps that might be desirable to document current state or compliance and the way forward.

Getting Buy-In

- Privacy Matters
  - *ATIPPA*, 2015 and *PHIA* establish expectations.
  - "The OIPC will apply these guidelines in our privacy investigations when looking for indications of accountable privacy management."
- Possible Consequences
  - Breach
  - Privacy Complaint
  - Audit/Own Motion Investigation (*ATIPPA, 2015*)
  - Offence ("Wilful" = A fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.)

Personal Information Inventory

- What information do you have?
- Why do you have it?
- How is it used?
- How was it collected?
- Under what authority was it collected?
- Where it is located?
- How is it protected?
- How long do you keep it?
- Do you disclose it? Under what authority?

Why a Personal Information Inventory?

- How can you demonstrate to OIPC and clients that information is protected if you do not know what you have, why you have it and where it is?
- Other jurisdictions have found this to be an effective tool.
- Example – if breach occurs, one of our first questions is what information could have been involved/was involved?

Method of Collection

- Review all existing and new forms used to collect personal information.
- When information is no longer required, advise staff and change forms.
- Review should include all other collection instruments, including:
  - surveys (print or electronic); and
  - collection through websites (data submitted electronically via an online form; metadata).

Policies and Procedures

- PMPs should include a requirement for developing and maintaining policies and procedures relating to:
  - requirements for notification of collection purposes and consent;
  - access to and correction of personal and/or personal health information;
  - retention and secure destruction of personal and/or personal health information;
  - administrative, technical and physical safeguards;
  - process for handling privacy-related complaints.

Policies and Procedures

- Manual establishes legislative requirements.
  - How do these apply in your organization?
  - Do you have organization-specific policies and procedures?
  - Do you have policies and procedures for specific programs and initiatives?
  - Has a copy been made available to staff?
  - Have staff been trained on the policies and procedures? If so, is this training documented?

Policy Example: Retention

- When writing policies and procedures, determine whether there is any applicable legislation.
- Under the *ATIPPA, 2015*, the requirements include:
  - retaining personal information where it is used to make decisions affecting an individual (section 65). If information is subject to a request for access or correction, retain as long as necessary to exhaust any recourse under the *Act;* and
  - safeguarding the information (section 64).

Policy Example: Retention (cont.)

- Safeguarding the information:
  - requires organized and secure records management;
  - includes ensuring disposed of in a secure manner (i.e. the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances); and
  - any information in the cloud should have retention and disposal addressed in contract.

Policy Example: Retention (cont.)

- Once you have determined your organizational and legislative requirements, you must create the policy in writing.
- You must also consider whether the policy needs to address specific circumstances.
  - Were commitments made at the time of collection for individual programs and initiatives?
  - What is the secure disposal procedure? Does it differ based on the sensitivity of the information?

Breach Protocol

- Government has breach resources online.
- Have you trained your staff on what a breach is and what they should do?
- Are staff aware of common inadvertent breaches and how they could be avoided?

Note: Mandatory breach reporting has been in effect since June 2015.

Threat and Risk Assessment

- Conduct assessments that allow the public body to identify potential threats/risks versus benefits of a program or action.
  - Threat Risk Assessments.
  - Privacy Impact Assessments.
  - Vulnerability Assessments.

Threat and Risk Assessment

- What needs to be protected?
- What level of protection is required?
- Define the threats to protect against.
- Estimate the likelihood and potential impact.
- Are current or proposed safeguards appropriate to reduce the risk?
- Manage the residual risk.

Why Conduct a PIA?

- Consider potential privacy impacts of project on individual privacy
  - Privacy by design.
- Document what PI collected, used, disclosed.
- Document how PI flows/is accessed.
- Industry/project snapshot.

Why Conduct a PIA?

- Risk assessment
  - Not just risks to organization; risks to impacted individuals.
  - Likelihood and impact.
- Better ensure legislative compliance.
- Due diligence.

Oversight and Review

- Conduct random audits according to risk level.
- Initiate investigation if a breach has occurred.
- Compile thorough reports to establish due diligence.
- Update personal information inventory annually.
- Anticipate revisions for annual review or in response to identified risks.
- Communicate to employees any changes to processes or policy.

Questions