

Access to Information and Protection of Privacy

*Professional Municipal Administrators
Convention*

April 21, 2010

Presenters:
Jean Myrick &
Blaine Edwards

Today's Agenda



- *Access to Information and Protection of Privacy Act (ATIPP Act)* – General Overview
- Access provisions of the *ATIPP Act*
- Privacy provisions of the *ATIPP Act*

Purpose of the Act



- Increase Openness and Accountability
 - Gives the public a right of access to records
 - Creates specific and limited exceptions to access
 - Provides an independent review process (OIPC)
 - Gives individuals a right of access to, and correction of, their own personal information
 - Prevents the unauthorized collection, use and disclosure of personal information

Application of ATIPPA



- ATIPPA applies to all public bodies in the Government of Newfoundland and Labrador:
 - **Departments and Agencies;**
 - **Health Boards and School Boards;**
 - **Post-secondary institutions (public); and,**
 - **Municipalities**



Municipalities' Obligations



1. Designate a “Head.”
 - » Through a resolution or by-law (s. 66)
 - » Inform ATIPP Office of Head by mail.

2. Designate an ATIPP Coordinator.
 - » Head must designate under section 67.
 - » Inform ATIPP Office of designation by letter from Head.

3. Forward access requests to ATIPP Office.
 - » Fax requests to (709) 729-5466 to obtain file number.
 - » ATIPP Office will provide support and keep statistics.

4. Fill access requests pursuant to ATIPPA.

5. Comply with privacy provisions.

ATIPP Coordinator Role



- The ATIPP Coordinator:
 - Coordinator processes access requests
 - Gathers and vets records for release
 - Educates staff on access and privacy
 - Collaborates with ATIPP Office, and OIPC
- Please report any change in ATIPP Coordinator to ATIPP Office.



Other Stakeholders



- **Office of the ATIPP Coordinator**
 - Division of the Department of Justice, 5th Floor West Block
 - Coordinates all aspects of ATIPP program delivery
- **Office of the Information and Privacy Commissioner (OIPC)**
 - Oversight body for the *ATIPP Act*
 - Investigates complaints on access and privacy
 - Reviews public bodies' decisions and makes recommendations
 - Informs the public

Access to Information Process



1. Applicant applies in writing for records in the custody, or under the control of, a public body. A \$5.00 fee also applies (fee may be waived);
2. Application is date stamped and 30 day time limit is calculated;
3. Request is faxed to ATIPP Office to open file;
4. ATIPP Coordinator gathers records, and removes information as required by law;
 - Personal information, cabinet records and some 3rd party information must be withheld.
 - Other types of information may be withheld at the discretion of the Municipality.
5. Materials are provided to applicant once all fees have been paid;

Mandatory Disclosure



- **S. 31 – Public Interest Override**

- Information about a risk of significant harm to the environment, health or safety of the public must be disclosed without delay, whether or not a request has been made (ex: water reports)
- Must be “clearly in the public interest”
- “Override” refers to information that is normally protected under another exception (*Cabinet confidence, personal information, etc.*)

Mandatory Exceptions



- S. 18** Cabinet confidences
- S. 27** Harmful to third party business interest
- S. 30** Personal Information
- S. 30.1** Privileged House of Assembly files

Discretionary Exceptions



- S. 13** - Repetitive or incomprehensible request
- S. 14** - Information soon to be published
- S. 19** - Local public body confidences
- S. 20** - Policy advice and recommendations
- S. 21** - Legal advice
- S. 22** - Harmful to law enforcement
- S. 23** - Harmful to intergovernmental relations
- S. 24** - Harmful to financial/economic interests of public body
- S. 25** - Conservation of heritage sites
- S. 26** - Harm to Individual or public safety

Final Note



The ATIPP process is not required where a process already exists to provide the desired information

(e.g. Municipalities Act, Sec 215)

Upcoming Events



- **Newfoundland and Labrador Access & Privacy Workshop 2010**
 - Organized by Verney Conference Management with the support of ATIPP Office, OIPC, MUN and CNA
 - One session looks at “Identifying Unique ATIPP Needs of Municipalities”
 - Website address: <http://www.verney.ca/nlapw2010/>
- **Legislative Review**
 - Mr. John Cummings has been appointed as the review commissioner
 - will be conducting public consultations.
 - Findings and Recommendations due Nov. 30, 2010
 - His e-mail address is: jcumplings@gov.nl.ca

Access to Information and Protection of Privacy

Working with Personal Information

Blaine Edwards
Privacy Analyst
Department of Justice

Overview



1. Privacy Legislation
2. Creating and Working with Public Records
3. Working with Personal Information
4. Privacy Breaches

Why should I listen to this guy?

- Privacy is disappearing
- Public has certain expectations
- It's federal and provincial law.
- The longer its around, the more of a policy issue it will become



International Privacy



- **International**
 - Over 90 countries have “Freedom of Information” laws.
 - Sweden, “Freedom of the Press Act, 1766”
 - USA, “Freedom of Information Act, 1966”
 - Many acts also cover issues of privacy, records management and/or data protection.
- **The information held by governments/ businesses is the property of clients.**

Canadian Privacy



- Access to Information Act, 1982
- Privacy Act, 1983
- Personal Information Protection and Electronic Documents Act, 2000
- Acts covered all Provinces until they introduced their own Access & Privacy Legislation



Access and Privacy Legislation



Privacy

- Not everything can be provided to the public.
- Based on ideals of respect and personal privacy
- The Act makes it LAW to keep personal/confidential information protected
- Protect from unauthorized access and disclosure

Restricts

- When information can be collected,
- How it can be collected,
- How the information is used by public bodies,
- When it can be disclosed
- How when, and how, it can be destroyed

Creating and Working with Public Records

Creating Public Records



- **What is a record?**
 - E-mails, post-its, calendar entries, etc.
 - Anything that we create as part as our jobs.
 - Assessing clients, ordering road salt, contracting out work.
- **Clients have right to access their personal records.**
- **The public has the right to review public records.**

Personal and Confidential Information



Good to distinguish between the two:

- **Personal** – individual (e.g. income \$)
- **Confidential** – organization
(cabinet paper, communication)

Email Policy

- E-mail is a public record – treat in same manner as all public records
- Public records cannot be destroyed without authorization
- Transitory messages



Email Policy



- It is undesirable and unnecessary to maintain both electronic and paper copies of e-mails.
- Deleted email if stored in TRIM, shared drive or printed.



Email Tips



- Essential Elements of work.
- Inappropriate content
 - Errors cannot be deleted
 - Even if they're embarrassing
- Keep private life and work life separate



Email Tips



- Reduce the amount of personal information included in e-mails -- Use client IDs/initials instead
- Only carbon copy (Cc) when necessary
- Double check the e-mail recipient's name before sending
- Use specific subject headings (without personal identifiers)

Personal Information

Personal Information



- Recorded information about an identifiable individual, including
 - Name, address and telephone number
 - Race, ethnicity, religious or political beliefs
 - Age, sex, sexual orientation, marital status
 - Health, financial and educational information
 - Criminal history, fingerprints, blood type, etc.
 - Identifying numbers, SIN, Drivers Licence, etc.

Personal Information



- ATIPP Act defines how Personal Information is to be:
 - Collected
 - Used
 - Stored
 - Disclosed
 - Transferred
 - Destroyed



Collecting Information



No Public body can collect information unless its authorized by law.

1. Expressed by an Act or Agreement
2. Information is required for Law Enforcement
3. Information relates directly to the program its being collected for
 - Ex: Power Rebate Application Form can only collect information relating to the Power Rebate Program,

We are on a Need-to-Know basis

We need to have legal authority (a legitimate need) to collect personal information:

- Even then, it must be the minimum amount necessary.
- Can collect for:
 - Programs, projects, operating activity of a public body.

What do you mean by Collection?



- When a public body collects personal information through:
 - Forms, applications, interviews or correspondence,
 - Provided to the public body by another public body,
 - Collected by a contractor or other third party,
 - Correspondence, including unsolicited letters and resumes.

Manner of Collection



- It's necessary to inform:
 - the purpose for collecting it
 - the authority for collecting it
 - the contact information of a person who can answer questions regarding the collection

E.g. Privacy Notices on ALL forms that collect personal information.

Consent



We need to get an individual's consent before disclosing his or her information – collected in Reporting Requirements or Consent forms

- written (always best)
e.g. Parents of children with disabilities
- verbal (take notes)
e.g. MHA request – note on client file



Consent Not Always Needed



- There are times, however, when we **can't** or **shouldn't** get the individual's consent, such as for:
 - Criminal investigations
 - Court proceedings
 - Determining eligibility for a scholarship, honour or award
 - If the individual's health and safety are at risk
(E.g. child protection, neglected adults)

Using Information



- We should only use personal information for the same purpose we collected it or for a similar/ required purpose
- Use may include interdepartmental disclosure/ transfer as part of the work process.
- Using information often means disclosing it to others. This must be authorized.
- Example: Every department collects its own information, as they cannot acquire it from another



Accuracy



- We are now legally required to keep records containing personal information up-to-date and accurate if we will be using them to make decisions about the individual.
- Citizens have the right to view their information once it has been corrected.

Unauthorized Access & Use



- Personal information should be protected to ensure only persons with authorization handle it.
- Difficult to enforce within organizations

Examples: Britney Spears
Eastern Health



Storage



- Government records must be stored in suitable locations such as:
 - Locked drawer or file cabinet
 - Commercial storage with security
 - Building specifically for records storage purposes
 - Designated records storage rooms (information services centers, records centers or others)
 - Provincial Records Centre

ATIPP Release VS Disclosure



- Formal release of information (ATI requests)
 - Opportunity to formally review the file.
 - Sever out personal or confidential information prior to release.
- Not all requests will be formal
- Other organizations will often ask for information. Always best to ask questions for: purpose, authority and if the individual is aware.
 - Researchers, other agencies, NGOs.

Disclosing Information



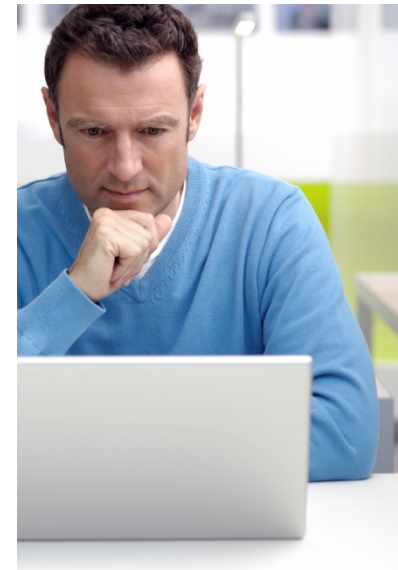
Personal information may only be disclosed to third party:

- for the reason it was collected
- with the individual's consent
- if it's in the public's interest
- to comply with a subpoena, warrant or court order (*if releasing in advance need consent & remove 3rd party info)

Disclosing Information



- to an MHA (working on behalf of a client)
- to protect the health & safety of an officer, employee or minister
- to notify next of kin (injured / ill)

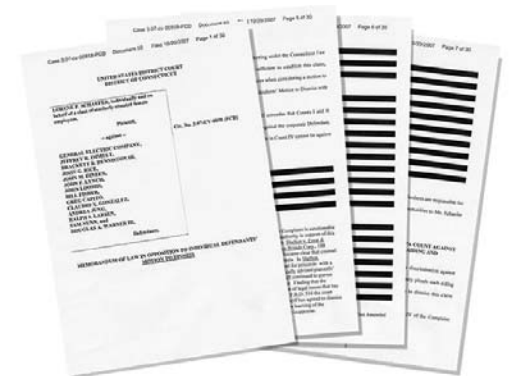


Disclosing Information



Keep it to the **minimum amount necessary** to accomplish the job at hand.

E.g. contact info not entire file



CYFS and Education



- Exchange between Departments very common
- Challenges
 - Turnover
 - Awareness
 - Policies and Procedures

Labrador Region Provided Good Example

Disposal of Information



- We can't keep everything forever.
 - HRLE keeps files for 7 years after end date
 - Education looking at 50 year retention
- Destroyed Information must not be readable.
 - Shred ALL Personal and Confidential Information.
 - Review Recycling Program
 - Some Departments Shred Everything Pre-Recycling Stage



Privacy Breaches

What is a Privacy Breach?



- A privacy breach is an incident that puts a record of *personal* information **at risk of harm**.
- A breach usually involves the **unauthorized disclosure** of personal information, either intentionally or by mistake.
- A privacy breach can occur if information

Responding to a Privacy Breach



- Notify your supervisor or ATIPP Coordinator and Alternate
- Together, determine:
 - If personal information is involved
 - If it's an unauthorized disclosure
 - If risk is involved (physical, financial, security)
- Record details of the possible breach

Together you will:



- Retrieve the information right away
- Notify the appropriate individuals
 - PSC
 - OCIO, Security, RNC, ATIPP Office, etc.
 - Clients, contractors, partners
- Evaluate the situation

Consequences of Breach



- to clients and others
- to the department
- to partners (business, government)
- to GNL



Thank You



Questions/ Comments?

Blaine Edwards

bedwards@gov.nl.ca

729.0077

Brenda Howell

brendahowell@gov.nl.ca

729.7072

Jean Myrick

jeanmyrick@gov.nl.ca

729.7073

Jennifer Berlin

jenniferberlin@gov.nl.ca

729.7939