Protection of Privacy

Protecting Personal Information in the Workplace

October 2015

A Quick Reference Guide
for employees and managers

Newfoundland Labrador

Protecting Personal Information in the Workplace

A Quick Reference Guide
for employees and managers

Purpose

This booklet is a companion to the *Protection of Privacy Policy Manual*. Its purpose is to assist managers and employees understand the protection of personal information and prevent any privacy breaches.

Policy

The Government of Newfoundland and Labrador is committed to the protection of personal information in its custody. With over 450 public bodies across the province, the public sector collects a large amount of information from citizens every day. It is vital that personal information be kept private, confidential and away from harms reach.

Understanding Personal Information

Personal information is information that can identify an individual (e.g. name, address, social insurance or MCP number, etc.). Some information on its own can identify an individual (e.g. name), while other information needs to be combined to identify an individual (address, age and gender, etc.). Information that relates directly to and can identify an individual is considered personal information.

All public bodies collect personal information from clients or staff. Collection takes place through paper or online application forms, interviews or correspondence. Under the *Access to Information and Protection of Privacy Act, 2015*, public bodies can only collect the minimal amount of information necessary in order to complete a task.

Once personal information is in the custody of a public body it can only be used for the purpose for which it was originally collected. In other words, if information was collected for one program, it cannot be used for another. All additional uses of personal information must follow the provisions in *ATIPPA, 2015*.

The instances for which a public body may disclose personal information to a third party are strictly limited by section 68 of *ATIPPA, 2015*. In many cases consent from the individual is required prior to disclosing the information; however there are other times when information may be disclosed without consent. Employees and managers are encouraged to contact their public body's ATIPP Coordinator or the ATIPP Office if they have any questions about when and how information may be disclosed.

Understanding Privacy Breaches

A ***privacy breach*** occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of *ATIPPA, 2015*. The severity is heightened when there is a risk of access to the individual's information.

Collection breaches occur when personal information is collected in contravention of *ATIPPA, 2015*, where:

- More information is collected than necessary on a form;
- A public body does not have the authority to collect the information (such as SIN);
- A privacy notice is not provided during collection; or
- Explicit consent of the individual is not obtained.

Use breaches occur when personal information is used for a purpose other than its intended use within a public body. Information cannot be shared for unrelated purposes, even within public bodies.

Disclosure breaches are breaches that involve the loss, theft or misdirection of personal information. In many cases these are the breaches that can potentially cause the most harm to individuals, physically, financially or otherwise.

Access breaches occur when you access or attempt to access personal information for a non-work related purpose. For example, as part of you job, you have access to a database that includes the names of people who owe fines and how much they owe. If you access this database to see if you neighbour owes any fines because you are curious (and it in unrelated to your job), this would be an access breach.

When breaches are discovered it's important to:

- Contain the breach;
- Evaluate the risks;
- Notify affected individuals; and
- Prevent similar breaches in the future.

Offences under *ATIPPA, 2015*

It is an offence under *ATIPPA, 2015* to **willfully** collect, use, disclose, access or attempt to access personal information in contravention of the Act (i.e. you intentionally collect, use, disclose, access or attempt to access personal information when it is not allowed under the *ATIPPA, 2015*). An offence under the Act can lead to a fine of up to $10,000 or imprisonment up to 6 months.

Protecting Personal Information in the Workplace

For Managers:

Training and reminding staff about privacy is one of the most effective ways to protect information and make sure they know what's required when collecting, using or disclosing personal information.

It is important for managers to think about privacy while making decisions. Considering potential privacy implications during the design stages of programs is a surefire way to stop the mismanagement of personal information before it happens. The ATIPP Office can assist with privacy policy development and can review programs for privacy compliance.

For Employees:

Adopt a clean desk policy

Ensure that your desk is cleared of all documents, notes, post-its, USB flash drives, CDs, DVDs, etc. at the end of each day. This will help reduce the risk of potential breaches caused by sensitive information being left unattended and in plain view.

Adopt a clean screen policy

Ensure that your computer is locked when leaving your desk for a short period of time and logged off if you are leaving for an extended period of time. This will help protect your computer's content and prevent unauthorized use.

Double check email addresses

Before hitting the send button, this simple act will help prevent unauthorized disclosures or breaches.

Implement a records management program

The practice of maintaining an organization's records throughout their entire lifecycle – from the creation of the record until its disposal, (destruction or archival preservation) ensures that the right information gets to the right people at the right time.

Respect the retention and disposal schedule

These schedules determine how long records should be retained and when they should be disposed (destroyed or preserved archivally).

- **Retention of records** - all physical and electronic records should be kept for a prescribed period of time. This period may be based on an organization's own policies and procedures or may be set by government legislation.

- **Disposal of records** - when records are to be destroyed, physical records containing personal information should be securely shredded and electronic records should be erased, overwritten or physically destroyed. Records which are an integral part of an organization's history or have cultural value should be transferred to an archival institution.

Use cover sheets for faxes

Cover sheets will help ensure that the information being sent will reach its intended recipient. In the event that information is sent to an unintended recipient, the cover sheet will give instructions on how the disclosed information should be addressed or destroyed.

Working outside the office

If you must work from home or on the road, take the minimum amount of information needed to complete the assignment in order to avoid potential breaches. Each employee must ensure that the information is secure at all times.

Traveling with IT assets

If you are required to travel with a public body IT asset, including a laptop or USB flash drive, use encryption when possible. Also, be sure not to leave these assets unattended and avoid leaving them in the back seat or trunk of a car.

Accessing personal / confidential records

Often you will have access to personal records as part of your job. Section 66 of *ATIPPA, 2015* outlines the limited purposes for which you can use this information. It is a violation to view these records for purposes unrelated to work (e.g. out of curiosity, as a favour to a friend, etc.).

Discussing personal information

When discussing personal information of others, such as clients, remember not to discuss the information in public areas, such as elevators, stairwells, or anyplace where others may overhear.

Frequently Asked Questions

Q: I'm transferring information to another public body, that's okay, right?

A: It depends. In some cases the transfer of information may be allowed, but in other cases you may need the individual's consent. If you are unsure whether you can transfer information to another public body, check with your ATIPP Coordinator or the ATIPP Office.

Q: A colleague of mine looks at client records out of curiosity. He doesn't tell anyone else so there's no risk, right?

A: Wrong. This is a privacy breach and must be reported.

Q: We're only collecting name and address. Do we need a privacy notice on our application form?

A: Yes, section 62 states that when collecting personal information, a privacy notice is required, except in very limited circumstances outlined in *ATIPPA, 2015.*

Access to Information and Protection of Privacy (ATIPP) Office

For more information on Breach Protocol, *ATIPPA, 2015* and Regulations please visit our website www.atipp.gov.nl.ca

Please contact the ATIPP office for information/advice on the following:

- Preliminary Privacy Impact Assessments
- Privacy Impact Assessments
- Consent Form Templates
- Privacy Notice Development
- Employee Privacy / Confidentiality Agreements
- Information Sharing Agreements
- Privacy Policy Advice

Office of Public Engagement

Access to Information and Protection of Privacy Office
4th Floor, West Block
P.O. Box 8700, St. John's, NL A1B 4J6
Tel: 709.729.7072
Toll Free: 1.877.895.8891
Fax: 709.729.2226
Email: ATIPPoffice@gov.nl.ca

www.atipp.gov.nl.ca


Newfoundland
Labrador