Access to Information and Protection of Privacy

Guide for Municipalities

October 2015

Table of Contents

Introduction

The *Access to Information and Protection of Privacy (ATIPP) Act, 2015* sets out how public bodies should protect personal information and respond to formal ATIPP requests.

In complying with the *ATIPP Act*, 2015, municipalities face unique challenges. They have their own practices and procedures and must ensure that they comply with other legislation, including the *Municipalities Act, 1999.*

All municipalities must designate an ATIPP Coordinator; the coordinator is often the town clerk. The coordinator's obligations include:

- Receiving and processing ATIPP requests;
- Ensuring compliance with privacy provisions of the *ATIPP Act, 2015*;
- Educating staff about the *ATIPP Act, 2015*; and
- Preparing statistical reports on requests.

This Guide will provide direction on how to handle various access and privacy issues. Topics include:

- Public Documents;
- Dealing with Privacy Breaches;
- The Process for Responding to an ATIPP Request; and
- Guidance on some of the specific types of requests municipalities are likely to receive.

This Guide has been developed to support municipalities in following the *ATIPP Act, 2015*. A further update will be provided to municipalities when a standard for public disclosure for municipal governance is enacted within the *Municipalities Act, 1999* as recommended by the ATIPPA Statutory Review Committee.

Contact the ATIPP Office

The ATIPP Office is available to answer questions and provide assistance on any issue relating to the *ATIPP Act*. Please contact the ATIPP Office if you:

- have questions about the *ATIPP Act, 2015;*

- have questions about this Guide;
- have any suggestions for ways to improve this Guide; or
- would like training on access to information and protection of privacy.

You can contact the ATIPP Office at (709) 729-7072 or toll-free at 1-877-895-8891. You can also reach us by email at atippoffice@gov.nl.ca.

Important Terms

Applicant: A person who submits an ATIPP request.

ATIPP Coordinator: The designated person in a municipality (or other public body) responsible for handling ATIPP requests. This person is often the town clerk.

ATIPP Office: The office responsible for assisting public bodies on access to information and protection of privacy. The ATIPP Office is part of the Department of Justice and Public Safety (JPS).

ATIPP Request: A formal request from an individual for access to records/information.

ATIPP Act, 2015: The *Access to Information and Protection of Privacy Act, 2015*.

Exceptions: The types of information that you may withhold when responding to an ATIPP request. Some exceptions are mandatory (i.e. *must* withhold) and some are discretionary (e.g. *may* withhold).

JPS: The Department of Justice and Public Safety; a department of the provincial government of Newfoundland and Labrador.

MAE: Municipal Affairs and Environment; a department of the provincial government of Newfoundland and Labrador.

OIPC: Office of the Information and Privacy Commissioner. This office approves requests for extensions and reviews complaints about the handing of personal information or ATIPP Requests.

Public Documents: Documents that must be made available for public inspection at a municipality's town office. Public documents are listed in section 215 of the *Municipalities Act, 1999*.

Personal Information: Personal information means recorded information about an identifiable individual. It includes information such as name, address, phone number, race, age, opinions and other information. For a full definition, see section 2(u) of *the ATIPP Act, 2015*.

Privacy Breach: Situation where personal information is collected, accessed, used or disclosed inappropriately.

Redact: same as 'sever'; means to black out information before release.

Overview of Public Documents

Section One

Section

Public Documents

Adopted Minutes of the Council

Assessment Rolls

Regulations and Municipal Plans

Opened Public Tenders

Financial Statements, Auditors Reports and Adopted Budgets

Contracts

Orders

Permits

Correspondence and other Documents Tabled at a Public Meeting

Government of Newfoundland and Labrador
ATIPP Office, Department of Justice and Public Safety

Overview of Public Documents

Section 215 of the *Municipalities Act, 1999* requires municipalities to make certain documents available to the public. These documents are:

- adopted minutes of the council
- assessment rolls
- regulations
- municipal plans
- opened public tenders
- financial statements
- auditor's reports
- adopted budgets
- contracts
- orders
- permits
- documents tabled at or adopted by council at a public meeting

We will refer to these documents as 'public documents.' Public documents should be available during normal business hours. Any person who views public documents may also ask that a copy be made, if there is appropriate copying equipment available. A municipality may charge the person for the costs of copying the document.

A person does not need to submit a formal ATIPP request to view public documents.

Personal Information in Public Documents – Applying Section 40

Public documents may contain various types of personal information such as names, addresses and opinions of residents. It is the responsibility of the municipality to balance the need for access with the need to protect personal information.

Public documents are important for ensuring that municipalities operate in an open and transparent manner. The need for transparency must be balanced with the need to protect personal information contained in these documents. In some situations, it will be appropriate to redact personal information from public documents.

The general rule is that information can be left in public documents if it would not be an unreasonable invasion of privacy to disclose it.

Information that can be released (i.e. not an unreasonable invasion of privacy):

Section 40(2) of the *ATIPP Act, 2015* lists the types of information that may be released. Some examples include:

- personal information where the person the information is about has consented to the release (e.g. a person asks that their letter with their name be tabled at a public meeting);
- Information about an employee or councillor's position, functions, salary range or other remuneration;
- Financial details of a contract to supply goods and services;
- Details of a license, permit, or similar discretionary benefit;
- Travel expenses; and
- Attendance at an event or mention of an honour or award (unless the person asks that their name not be included).

Information that should usually be withheld (i.e. presumed to be an unreasonable invasion of privacy)

Section 40(4) of the *ATIPP Act, 2015* sets out certain types of personal information, the release of which, is presumed to be an unreasonable invasion of privacy. These types of information should usually be withheld, unless there are strong factors in favour of disclosure. These types of information include:

- Medical or psychological information;
- Information about law enforcement;
- Employment or educational history;
- Information gathered on a tax return or for the purpose of collecting a tax;
- Information about an individual's bank account or credit card;
- Job or character references; and
- Racial or ethnic origin, religious or political beliefs or associations.

These types of information should usually not be released. If you come across a situation where you think there are particularly strong or important reasons in favour of releasing this information, we encourage you to contact the ATIPP Office for assistance.

Other Information – Balancing Factors

Some personal information does not fit into either of the above categories. In such cases, you should use your discretion to balance the reasons why you would disclose the information with the reasons why you would not.

Some of the factors to consider include:

- The disclosure is desirable for subjecting a public body to public scrutiny;
- The disclosure is important for promoting health, safety or environmental protection;
- A person may be unfairly harmed by the disclosure;
- The person provided information in confidence;
- A person's reputation may be unfairly damaged; and
- The information is about someone who is deceased and an appropriate amount of time has passed.

All of these factors should be considered, but the first is particularly relevant in the context of public documents. Public documents exist, in part, to ensure that the public is fully aware of how council makes its decisions. If personal information is not sensitive and it will contribute significantly to a public discussion, it should be released.

Some examples:

- *A public document contains the name of a staff person and their duties. This information is not an unreasonable invasion of privacy and can be released.*
- *Council grants a permit to build a new house. The information on the permit can be released.*
- *Council publishes a job advertisement and receives a number of resumes in response. Those resumes should not be tabled at a public meeting.*
- *Council receives a letter from an individual stating that the Council should do a better job at picking up garbage. In this case, it may be appropriate to table a version of the letter with the name and address or other identifiable information redacted. This way, the parts of the letter that are important for public discussion will be available.*
- *Council receives a letter from a well-known engineer stating that a bridge in the community is in need of repair. In this case, it may be appropriate to table the letter in full. While the names in letters should sometimes be redacted, in this case the individual writing the letter, their reputation, and their qualifications are relevant to the discussion. We would encourage you to discuss the matter with the ATIPP Office.*

Adopted Minutes of the Council

The minutes should inform citizens about what has occurred and what decisions have been made at public council meetings. In many cases this will mean revealing personal information such as the names of individuals who have been granted permits and speakers at a public council meeting. At the beginning of public meetings, you should inform speakers that their names and opinions may be included in the minutes. You should also advise those in attendance if you intend to include their names in the minutes.

You are not required to make the minutes available as a public document until they have been adopted by Council at a subsequent meeting.

If you record a meeting to assist you in writing minutes, you may wish to destroy the recording after you have written the minutes. If an ATIPP request comes in for the recording any time before the recording is destroyed, it will be subject to an ATIPP Request.

Personal information about councillors and staff that should not be redacted

- Names
- Position, functions, salary and benefits
- Attendance or non-attendance at meeting
- Travel Expenses
- Who has introduced a motion, seconded it and how they have voted
- Opinions or other information expressed at the public council meeting

Personal information about individuals that should not be redacted

- Names of individuals in attendance (unless an individual has specifically asked not be included)
- Names of individuals who have received an honour or award (unless an individual has specifically asked not be included)
- Names and opinions of individuals who have made a presentation at a public council meeting
- Details of a contract to supply goods or services. For example, if an individual has been contracted to provide cleaning services to the town, you may reveal who has been hired and the amount of the contract
- Names and other personal information if they are necessary and relevant to the discussion at hand

Information about permits and other benefits in the minutes

If a council decides whether to approve a permit, grant, or other benefit at a public meeting, the minutes may reveal the name of the person who has been granted the permit or benefit. It should also include other pertinent information such as the address where a home will be built, the area where a development will take place, or the time, place and date of an event.

The only exception to this is if a benefit is granted which reveals sensitive personal information about a person, such as a person's income or disability. In these specific circumstances, it is inappropriate to reveal individual's names.

Sensitive personal information in the minutes

A public council meeting occurs in public. Information should not be discussed publicly if Council is not comfortable including the information in the minutes. If an issue requires councillors to discuss sensitive personal information in detail, it should be discussed in a private meeting rather than a public meeting.

Assessment Rolls

What is included on the assessment roll?

Where municipalities use an assessment role, they are required to make the roll available as a public document.

For each property, the roll should include:

- The address of a property
- The owner of the property
- The assessed value of the property
- Any other information required by the director of the Municipal Assessment Agency

Any person can inspect the roll and make copies.

The roll is also available electronically at www.maa.ca. If a person cannot come to the town office, you may wish to refer them to this website. When doing a public search, a person will receive:

- The property address
- The property types
- Whether it is occupied by the owner or a tenant
- The frontage or acreage of the property

Regulations and Municipal Plans

Regulations

Municipalities are required to make all regulations made by Council available at the town office. They should be provided without any information redacted. Regulations are sometimes referred to as by-laws or bylaws but they mean the same thing in this context.

Registered municipal plans

Municipal plans are created under the authority of the *Urban and Rural Planning Act*. They include information such as zoning, development of new areas, water use, and other information.

The full content of a certified municipal plan should be available at the town office with no redactions.

Not all municipalities have a registered municipal plan. If your municipality does not have one, there is consequently no requirement to have one available as a public document.

Opened Public Tenders

What is an opened public tender?

Under the *Public Tender Act*, municipalities must call for tenders when the value of a good or service exceeds $10,000 or when public works exceeds $20,000. This is called an opened public tender. There are some exceptions not covered here.

What should be available to the public?

Where a public tender is called, the tenders will be opened in a public place. After they are opened, the following information should be made available. This includes:

- The name of any company which has submitted a bid
- The amount of the bid

Financial Statements, Auditors Reports and Adopted Budgets

What are financial statements?

Financial Statements are statements required under section 86 of the *Municipalities Act, 1999.* Municipalities are required to prepare and adopt financial statements in accordance with accepted accounting principles.

What are auditor's reports?

Auditors Reports are reports required under section 87 of the *Municipalities Act, 1999.* Municipalities are required to appoint an auditor each year to audit the accounts and to report to council on the financial statements.

What are adopted budgets?

Adopted budgets are budgets adopted under section 77 of the *Municipalities Act, 1999.* The Act requires councils to prepare and adopt a budget each year containing estimates of revenue and expenditure of the council for the next financial year.

What must be available at the town office?

The full content of a town's financial statements, the auditor's reports and adopted budgets should be made available at the town office without redactions.

Contracts

What are contracts?

A contract is a formal and legally binding agreement between two parties. Examples include:

- An employment contract hiring a person to work as an employee of a municipality
- A contract with a company in which they agree to do road repair work on the town's behalf.

The 'parties to a contract' are the individuals or entities who have agreed to the contract. They will be listed on the first page of the contract and will also have signed the contract.

What must be available to the public?

Any contracts to which the municipality is a party must be available for viewing at the town office.

Contracts include employment contracts. In such contracts, you should not redact a person's title, functions, salary range or other remuneration. However, if the contract contains personal information that is not important for the public to know, and plays no role in public scrutiny, it should be redacted. For example, if a contract contains an individual's home address, this information should be redacted.

Orders

What is an Order?

Orders legally require a person to either stop doing something (e.g. stop causing a nuisance such as excessive noise) or to take certain action (e.g. to repair dilapidated property). Section 404 of the *Municipalities Act, 1999* allows municipalities to make orders.

What should be available to the public?

Any orders made by the town should be available at the town office without redactions, including the names of individuals who have been ordered to take action and the address of any properties involved.

Permits

What is a permit?

The *Municipalities Act, 1999*, allows municipalities to grant permission to citizens to do various activities such as building a home, modifying a home, owning a pet, operating a taxicab, etc.

The *Urban and Rural Planning Act, 2000* allows municipalities to make development regulations to ensure land is controlled and used in accordance with the municipal plan. Various types of permits may be set out in the municipal plan.

A permit is the document giving a person or business approval to do these activities.

What must be available at the town office?

All permits must be available in full without redactions.

Correspondence and other Documents Tabled at a Public Meeting

Receiving correspondence

When a person submits a letter, email or other document to council about an issue, they should be advised that their correspondence may be tabled at a public council meeting.

Personal Information in Tabled Documents

Any documents tabled at a public council meeting will become public documents.

When a piece of correspondence has been selected for tabling, you should consider whether releasing the information would be an unreasonable invasion of privacy.

As a general rule, it is appropriate to redact the name and address of a person sending a letter prior to tabling the document. That way, their personal information is protected but the content of the letter can still be discussed. However, there may be situations where releasing the name would not be an unreasonable invasion of privacy; for example, where releasing personal information is necessary for appropriate public scrutiny of the town. For more information see page 7 or section 40 of the *ATIPP Act, 2015*.

If a letter addresses a sensitive issue, it may be appropriate to provide council with a summary of the information rather than the letter itself, or to ask council to discuss the matter at a privileged meeting.

Overview of Privacy in the *ATIPP Act*

Section Two

Section

Privacy Issues

Principles of Collecting, Using and Disclosing Personal Information

Sharing Information with Councillors

Social Media, Email and Websites

Privacy Breaches

Government of Newfoundland and Labrador
ATIPP Office, Department of Justice and Public Safety

Privacy Issues

Section Overview

This section deals with privacy issues outside the context of public documents. In this section you will learn about:

- Collecting, using, accessing and disclosing personal information in documents that are NOT public documents;
- Sharing information with councillors;
- Personal information, email and social media; and
- Privacy breaches.

Principles of Collecting, Using, Accessing and Disclosing Personal Information

Municipalities should make certain information available in public documents, as set out in the first part of this Guide. However, municipalities also control a wide variety of other personal information. Some examples include:

- Resumes of job applicants;
- Staff records;
- Information on taxes paid by residents;
- Personal phone number of employees and councillors; and
- Lists of participants in various programs and their personal information.

The following is a list of principles to follow when collecting, using, accessing and disclosing personal information:

1. **You should collect the minimum amount of personal information necessary.**
    - For example, if you only need a person's email address, do not collect their home address, income level, age, etc.
2. **You should collect personal information directly from the individual the information is about.**
    - Information should not be collected from a person's friends or family members
    - For exceptions to this principle, see section 62 of *ATIPP Act*
3. **Personal Information should only be collected where legally authorized.**
    - A collection is legally authorized where:

- It is authorized by an Act;
- It is collected for law enforcement purposes; or
- It relates directly to and is necessary for an operating program or activity.

4. **Personal Information should only be used or accessed for the original purpose or for a consistent purpose.**
   - Example of a collection: collecting information in application forms to determine who will be granted a taxi operator's license.
   - Example of a consistent purpose: using the contact information in application forms to mail out information about changes to taxi regulations.
   - Example of a non-consistent purpose: using the contact information in application forms to call people asking that they volunteer for to help with an upcoming festival.

5. **Information should only be disclosed under certain specific circumstances.**

   Section 68 of the *ATIPP Act, 2015* lists all the circumstances. The most common for municipalities are:
   - Disclosing information in public documents; or
   - Disclosing information for the purpose it was obtained.

6. **When using, accessing or disclosing personal information, the use, access or disclosure should be limited to the minimum amount necessary.**
   - Example: your town holds a job competition and receives 10 applications. These applications should be shared only with those involved in the hiring process. They should not be shared with staff not involved in the hiring process or with the general public.

For each of these principles, there are some limited exceptions set out in the *ATIPP Act, 2015*. If you are considering collecting, using, accessing or disclosing personal information and you think you may need to go outside these principles, see sections 61-72 of the *ATIPP Act, 2015* or contact the ATIPP Office for assistance.

Sharing Information with Councillors

Councillors have access to all information contained in public documents, as set out in Part I of this Guide.

For other information, personal information should only be disclosed to councillors where it is necessary to carry out a purpose the municipality is trying to achieve. This includes when personal information is needed to assess a conflict of interest and when personal information is needed to inform a decision.

Personal information is needed to assess conflict of interest

Under section 207 of the *Municipalities Act, 1999*, a councillor has a conflict of interest where:

- he or she has a direct or indirect monetary interest in a matter;
- a relative has a monetary interest in the matter; or
- he or she is an officer, employee or agent of a company or association that has a monetary interest in the matter.

If a decision is being made by council involving personal information, councillors must be able to assess whether they have a conflict of interest. There may be circumstances where information is withheld from the public but given to councillors so they can assess whether they have a conflict.

Personal information is needed to make a decision

There are circumstances where sensitive personal information should be withheld from the public. For example, if there is an accusation of harassment from one employee by another, it would be inappropriate to discuss the matter openly in a public meeting. However, if the council needs to assess the situation and decide how to proceed, they will need to have the information necessary to make that decision. This may mean that they will need access to some personal information.

When personal information should be withheld from councillors

There are times when a municipality deals with sensitive personal information and councillors do not require that personal information to do their jobs.

For example, if a councillor wants general information on the number of people who owe money to the town and the amounts, the town clerk could provide the councillor with a list that does not include names.

Responsibilities of Councillors

There are times when councillors will be privy to personal information that is not available to the general public. Councillors should not disclose that personal information unless they are allowed to do so under the *ATIPP Act*, *2015*. If information is collected, used, accessed or disclosed inappropriately, an individual may make a complaint to the Office of the Information and Privacy Commissioner (OIPC).

Social Media, Email and Websites

Municipalities are increasingly using social media to provide the public with information. Many municipalities have a Facebook or Twitter page, and we encourage municipalities to use such tools to inform the public about general issues such as town events and boil water advisories.

However, social media must not be used to transmit personal information. It can be difficult to verify a person's identity, and the security of social media is not guaranteed. If you receive a message about a personal matter from social media, ask the sender to contact you by phone or through your municipality's official email address. You can reply through social media if the person is asking for general information, such as information about garbage collection.[1]

Municipalities should have an official email address. Town employees should not use their personal email addresses to communicate with residents. There may be confusion if an employee moves into a new job and continues to receive personal information relating to town business. Towns also need to be able to access records after an employee moves into another job.

A town may also share general information on a website. You should use caution when sharing any personal information on a website and ensure it is authorized under the *ATIPP Act*..

Privacy Breaches

A privacy breach occurs any time information is accessed, collected, used or disclosed in contravention of the *ATIPP Act, 2015*. Some examples of privacy breaches that could occur in the municipal context include:

- A person hacks into a municipality's computer system and obtains personal information including employees resumes;
- A town employee sends a fax containing personal information to the wrong number;
- A town employee mails a letter containing personal information to the wrong address; or
- A town councillor attends a privileged meeting about an employee dispute. The councillor takes documents about the matter home and leaves the documents on the kitchen table. The councilor's spouse sees the documents and reads all about the dispute.

All privacy breaches must be reported to the OIPC. All privacy breaches should also be reported to the ATIPP Office.

In addition, where a person's privacy is breached and there is a risk of significant harm, that person must be notified of the breach.

For more information about privacy breaches, please see Appendix B (Privacy Breach Protocol).

If you need assistance dealing with a privacy breach or have any questions, please contact the ATIPP Office.

[1] *Report P-2012-001*, Newfoundland and Labrador Information and Privacy Commissioner

Overview of Access to Information

Section Three

Section

Government of Newfoundland and Labrador
ATIPP Office, Department of Justice and Public Safety

Overview of Access to Information

Section Overview

This section provides guidance on when a formal ATIPP request is necessary as well as information about the process involved in receiving and responding to a request.

Is an ATIPP Request Required to Release Information?

If you receive a call from someone asking for information and there are no issues with releasing it, there is no need to require a formal ATIPP Request. In addition, you should not require a formal ATIPP request for those public documents set out in section 215 of the *Municipalities Act, 1999*.

If the person asking for the information prefers to make a formal ATIPP request, they have a right to do so. Some people prefer this route because it gives them a right to have the request processed under specific timelines and the ability to submit a complaint to the OIPC if they are not satisfied with the response.

Receiving an ATIPP Request

Any person or organization can make an ATIPP request to a municipality. Request forms are available from the ATIPP Office website at: http://www.atipp.gov.nl.ca/forms/.

If a request is unclear, you should contact the applicant as soon as possible for clarification.

You must note the date you receive the request, as requests must be responded to within 20 business days. A request to extend the due date may be granted by the OIPC under section 23 of the *ATIPP Act, 2015*. You must also provide records if available by day 10 or send an advisory response to the applicant in writing.

As soon as you receive a request, you must notify the ATIPP Office. The ATIPP Office tracks requests, provides you with a file numbers and can also provide assistance when you are processing a request or determining how to apply exceptions.

Duty to Assist

The *ATIPP Act, 2015* requires municipalities to assist applicants throughout the process of making an ATIPP request by:

- Making a reasonable effort to assist the applicant;
- Responding in a timely manner; and

- Conducting a thorough search so as to return as complete a set of records as possible.

The duty to assist the applicant has always been an important, underlying provision of the *ATIPP Act, 2015* and is a statutory duty that should be upheld throughout the entire request process. It requires that clear communication between the ATIPP Coordinator and applicant occur at all stages of the request; that the applicant is kept informed throughout the process; that a working relationship with the applicant is developed in order to better understand the applicant's wishes or needs; and that he or she has understanding of the process.

Exceptions to Disclosure

The *ATIPP Act, 2015* sets out a limited number of circumstances where information requested in an ATIPP request may be withheld. These are known as exceptions and are contained in sections 27-41 of the *ATIPP Act, 2015*.

Where information falls under an exception, the municipality is required to or may sever the information, however, the municipality should sever only the necessary information.

The following is a list of exceptions to access and a brief explanation of each. If you are having difficulty applying these exceptions, please consult the Access to Information and Protection of Privacy Act, the ATIPP Access Policy and Procedures Manual, or call the ATIPP Office.

Mandatory Exceptions

Five exceptions are **MANDATORY** – this means you must withhold such information whether you want to release the information or not. Two exceptions (Cabinet Confidences – section 27 and Disclosure of House of Assembly Service and Statutory Office Records – section 41) are unlikely to apply to municipalities; however, the following three mandatory exceptions may arise in requests:

Information from a Workplace Investigation (section 33) - This section requires public bodies to withhold all relevant information created or gathered about a workplace investigation. Workplace investigations typically involve events such as harassment or the conduct of an employee in a workplace. This section also requires certain information to be released where the applicant is either a witness, the person who made the complaint or the person the investigation is about.

Disclosure Harmful to Business Interests of a Third Party (section 39) – This section protects information which, if disclosed, would harm a third party's business interests. In order for information to be withheld it has to meet **all** of the following three criteria, commonly referred to as a "three-part test":

- the information would reveal third party trade secrets, or commercial, financial, labour relations, scientific or technical information of a third party;

- the information is supplied in confidence; and
- the disclosure of information would reasonably be expected to result in ***any*** of the following:
    - harm *significantly* the competitive position or interfere *significantly* with the negotiating position of a third party;
    - result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied;
    - result in undue financial loss or gain to any person or organization; or
    - reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

For information on the process of notifying third parties, please see Appendix A.

Disclosure Harmful to Personal Privacy (section 40) – This section sets out when a disclosure would be harmful to personal privacy. It sets outs:

- information that is not an unreasonable invasion of privacy;
- information that is *presumed* to be an unreasonable invasion of privacy; and
- relevant factors to consider.

If you are trying to determine if a disclosure would be an unreasonable invasion of privacy, check if the information is specifically listed in section 40(2) or 40(4) of the *ATIPP Act, 2015*. Information listed in section 40(2) should be released. Where information is listed in section 40(4), you should presume the information should not be released; however you should consider the factors listed in section 40(5) and may release the information if the factors weigh in favour of disclosure.

If you are not sure how to apply section 40, please contact the ATIPP Office for assistance.

Discretionary Exceptions

All other exceptions are **DISCRETIONARY**. This means that public bodies may apply them, but are not required to do so. However, even where you are applying a discretionary exception, you must consider whether the public interest override applies for all but two (law enforcement and health and safety). The public interest override is discussed on page 27.

Some discretionary exceptions apply to municipalities but will rarely be encountered. If you feel that one of the following discretionary exceptions applies and you need assistance on using the exception please refer to the ATIPP Access Policy and Procedures Manual or call the ATIPP Office:

- disclosure Harmful to Intergovernmental Relations or Negotiations (section 34);
- disclosure Harmful to the Financial or Economic Interests of a Public Body (section 35);
- disclosure Harmful to Conservation (section 36);
- disclosure Harmful to Individual or Public Safety (section 37); and
- disclosure Harmful to Labour Relations Interests of Public Body as Employer (section 38).

The following discretionary exceptions are more likely to be encountered by municipalities:

Local Public Body Confidences (section 28)

Municipalities can refuse to disclose information that would reveal:

- a draft resolution or bylaw;
- a draft of a private bill; or
- the substance of deliberations of a meeting held in the absence of the public, where holding such a meeting is authorized under an act.

This exception cannot be used where the information has been discussed in detail at a meeting open to the public. For example, if there was an open debate at a public meeting about a draft bylaw, that draft bylaw cannot be withheld.

This exception cannot be used where records are more than 15-years-old.

Policy Advice or Recommendations (section 29)

Section 29 gives a municipality discretion to refuse to disclose advice or recommendations prepared for the municipality. This allows a municipality to have an open and frank discussion in private about important policy issues without such discussions being made public. This can include:

- advice, proposals, recommendations, analyses or policy options;
- the contents of a formal research or audit report that is incomplete;
    - Public bodies have 65 business days upon delivery of a draft research or audit report to request edits/changes. If no edits/changes are requested within 65 days, the report cannot be considered "draft" and withheld as policy advice.

However, it is important to note that this exception does not cover factual material and other specific reports as set out in section 29(2) of the *ATIPP Act, 2015*. Furthermore, this exception cannot be used for records that are more than 15-years-old.

Legal Advice (section 30)

Section 30 allows public bodies to refuse to disclose to an applicant information that is subject to solicitor client privilege.

A document is considered to be solicitor client privileged where:

- it is a communication between a solicitor and client (including a municipality as client);
- it involves the seeking or giving of legal advice; and
- it is intended to be confidential by the parties.[2]

It is important to note that if a document was written or viewed by a lawyer but not for the purpose of giving or receiving legal advice, this exception does not apply. For example:

> *If one of your councillors is a lawyer but gives advice about how to organize an event, this exception would not apply.*

Disclosure Harmful to Law Enforcement (section 31)

A municipality may refuse to disclose information which could reasonably be expected to interfere with a law enforcement matter.

Where a municipal bylaw can lead to a penalty or sanction, actions taken by municipal enforcement officers to enforce those by laws would be considered 'law enforcement.'

> *'Law enforcement' means an investigation or inspection conducted under the authority of or for the purpose of enforcing an 'enactment which lead to or could lead to a penalty or sanction.'*

Confidential Evaluations (section 32)

Section 32 allows public bodies to refuse to disclose personal information that is an evaluation or opinion, provided in confidence for the following purposes:

- determining suitability for employment or awarding contracts;
- determining suitability for an academic program; or
- determining suitability for an honor or award.

[2] *Report A-2007-12*, Newfoundland and Labrador Information and Privacy Commissioner.

The Public Interest Override

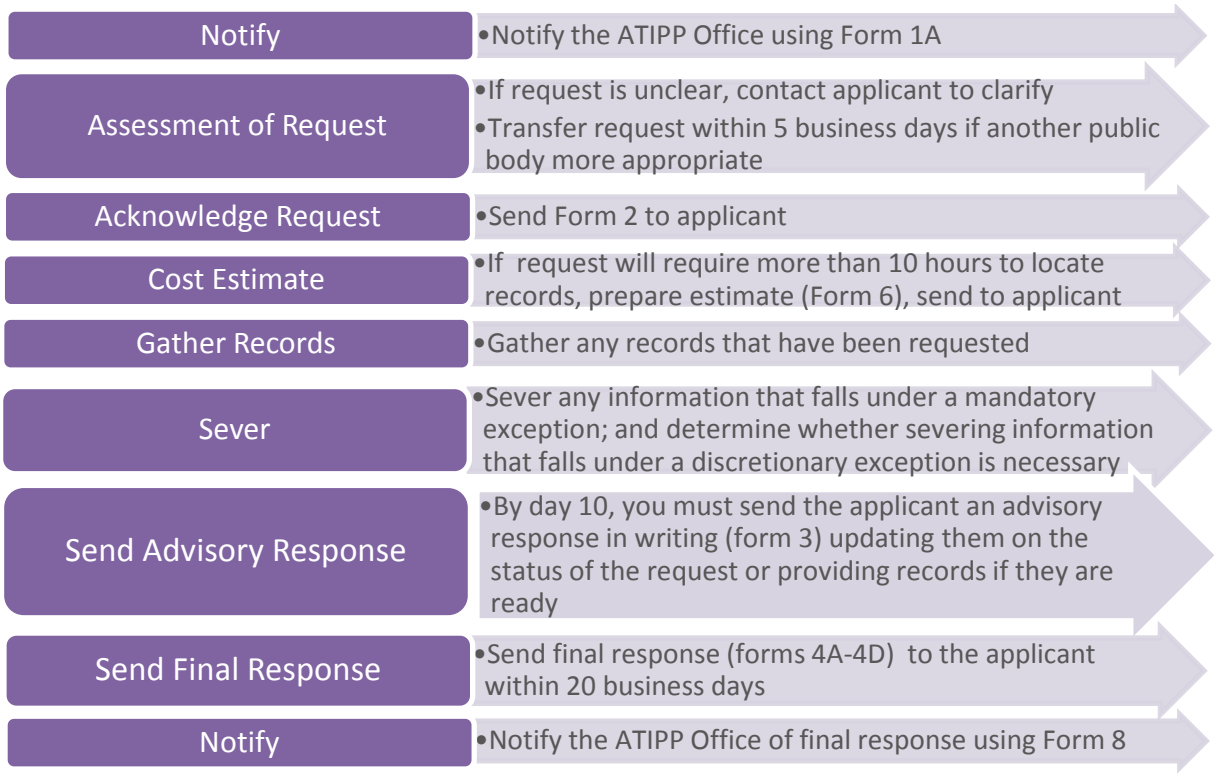
For most discretionary exceptions, the public interest override applies. This means that information cannot be withheld using these discretionary exceptions where it is clearly demonstrated that there is a public interest in releasing the information. The public interest override applies to the following discretionary exceptions:

- Local public body confidences;
- Policy advice or recommendations;
- Legal advice;
- Confidential evaluations;
- Disclosure harmful to intergovernmental relations or negotiations;
- Disclosure harmful to the financial or economic interests of a public body;
- Disclosure harmful to conservation; and
- Disclosure harmful to the labour relations interests of a public body.

The OIPC has developed guidance on applying the public interest override. The guidance is available at http://www.oipc.nl.ca/pdfs/PublicInterestOverride.pdf.

How to Process an ATIPP Request

In this section, we provide a basic procedure for various kinds of requests. If you have any questions or concerns, please consult the ATIPP Access Policy and Procedures Manual or contact the ATIPP Office. Standard forms are available for your use at www.atipp.gov.nl.ca/forms/.



Where the request contains Information that may harm a business or that may be an unreasonable invasion of privacy

The process for requests involving third party business information or a third party's personal information can be complex. See Appendix A for a flowchart on how to process this kind of request. If you have any questions, please contact the ATIPP Office.

Time Limit and Extensions

Public bodies are required to respond to ATIPP requests within 20 business days after they have been received. 'Business day' means a day that is not a Saturday, Sunday or a holiday. Even if a town office is only open part time, the 20 day requirement applies. For more information on what is considered a business day, please consult the handout found on the ATIPP Office website at http://www.atipp.gov.nl.ca/info/Timelines-BusinessDays-Handout.pdf.

Advisory Response

It is important to note that municipalities are also now required to release information by business day 10 if the record is available or provide an advisory response in writing advising the applicant of the status of the request.

Extensions

A municipality may extend the time for responding to a request by applying to the OIPC no later than 15 business days after receiving the request. Examples of reasons the OIPC may grant an extension include:

- the applicant does not give sufficient details;
- a large number of records is requested or must be searched, and responding within the 20 day time period would be unreasonable for the municipality;
- the nature of the access request is such that responding within the 20 day time period would interfere unreasonably with the operations of the municipality;
- the applicant has submitted multiple requests at the same time to the municipality and it would be unreasonable for the municipality to respond within the time period;
- you need to contact a third party about the release of their business information;
- more time is needed to consult with a third party or other public body; or
- other circumstances that may require additional time to respond to a request.

The OIPC has developed guidance on requesting a time extension which is available at http://oipc.nl.ca/pdfs/RequestingaTimeExtension.pdf.

The OIPC can be contacted by email at commissioner@oipc.nl.ca or by phone at 729-6309 or toll-free in Newfoundland and Labrador at 1-877-729-6309.

Where an extension is granted by the OIPC, you must notify the applicant using Form 5.

Access Requests for Specific Types of Information

Section Four

Section

Government of Newfoundland and Labrador
ATIPP Office, Department of Justice and Public Safety

Access Requests for Specific Types of Information

Public Documents

Part I of this Guide lists the documents which must be made available at the town office without requiring an ATIPP request. If you receive an ATIPP request for one of these documents, you should inform the applicant that the documents are already publicly available and advise the applicant how to access them.

If an applicant wishes to proceed with an ATIPP request, they may do so.

Minutes Which Have Not Yet Been Ratified

An applicant may request minutes that have not yet been ratified. When fulfilling such a request, you may want to include in your final response a statement indicating that these minutes are not the final, official record of the meeting.[3]

If you receive this kind of request, you may wish to contact the applicant advising them when the ratified minutes will be published and asking whether they wish to proceed with the request.

Recordings

Recordings of public meetings are a record of the municipality and are subject to an ATIPP request. A copy should be provided if requested. You may want to include in your final response a statement indicating that these minutes are not the final, official record of the meeting.[4]

Records Relating to Privileged Meetings

A municipality may conduct privileged meetings under the authority of section 213 of the *Municipalities Act, 1999* by passing a motion to that effect. A municipality may refuse to disclose information which would reveal the substance of deliberations at a privileged meeting. To apply this exception, you would need to show:

- an authorized privileged meeting was, in fact, properly held; and
- the disclosure of the disputed records or information would reveal the substance of deliberations of the meeting.[5]

[3] *Report A-2007-019*, Newfoundland and Labrador Information and Privacy Commissioner.
[4] *Report A-2007-019*, Newfoundland and Labrador Information and Privacy Commissioner at paragraph 34.
[5] *Report A-2008-009*, Newfoundland and Labrador Information and Privacy Commissioner.

The substance of deliberations could include information such as what was said by individuals at the meeting, what opinions were expressed, how individuals voted, and the arguments in favour of or against taking a particular action.[6] Remember that if the minutes of a privileged meeting are tabled at a public meeting, they will be available to the public under section 215 of the *Municipalities Act, 1999* once they are adopted. For this reason, you should use caution before tabling such minutes at a public meeting.

Also note that other exceptions may apply, such as disclosures harmful to personal privacy (see pages 23-26).

Property Documents

Property documents that have been registered in the Registry of Deeds may be disclosed. The Registry of Deeds is a public registry, and releasing information contained in a public registry is not an unreasonable invasion of privacy.

Sometimes, documents associated with a property are not contained in the registry of deeds, such as personal affidavits with respect to the property. If these documents are requested, you should consider whether the release of any information would be an unreasonable invasion of privacy. [7] See page 24 and Appendix A.

Crown Grants

Crown Grants are registered publicly in the Registry of Crown Titles and Records. If an ATIPP request includes a Crown Grant, and the municipality has that information, it should be disclosed.[8]

The Name of a Person who Submitted an ATIPP Request

The name of a person who submitted an ATIPP request should not be disclosed to anyone other than the ATIPP Coordinator.[9]

Complaints about another Resident

Municipalities deal with a variety of different complaints, including speeding, littering, failing to maintain property, noise, etc. Such complaints deal with individuals but can also involve third parties and, in many cases, specific properties.

If you receive a request for information relating to such a complaint, you should consider:

[6] *Report A-2008-009*, Newfoundland and Labrador Information and Privacy Commissioner at paragraph 32.
[7] *Report A-2007-012*, Newfoundland and Labrador Information and Privacy Commissioner at 81-87.
[8] *Report A-2007-012*, Newfoundland and Labrador Information and Privacy Commissioner.
[9] *Report A-2012-005*, Newfoundland and Labrador Information and Privacy Commissioner, ATIPP Act s. 12

- will disclosing the information be harmful to law enforcement? See page 26.
- will disclosing the information be harmful to personal privacy? See page 24 and Appendix A.

Depending on the details of the request, it may be appropriate to release details of the complaint but not the identity of the person making the complaint. If you need assistance in responding to such a request, please contact the ATIPP Office for assistance.

Information about Staff

Where an ATIPP request seeks information about an employee or officer of a municipality, the municipality should release information about:

- the person's position;
- the person's functions;
- the person's salary and benefits; and/or
- opinions a person gives as part of their duties as a town employee, unless those opinions are about another person.

If the request asks for other information, you should consider whether disclosing the information would be an unreasonable invasion of privacy under section 40.

Resources

SECTION FIVE

Section

Legislation

Forms

Training

Policy manuals and guides

Legal resources

Resources

Section Overview

This Guide is intended to be a general overview of access to information and privacy issues. It focuses on highlighting the most common issues faced by municipalities. The following resources may also be helpful:

Legislation

- *The Access to Information and Protection of Privacy Act, 2015*
- *The Municipalities Act, 1999*

Forms

The ATIPP Office has developed a number of forms for responding to requests. These forms are available at www.atipp.gov.nl.ca/forms/. The forms can be modified as required.

Training

The ATIPP Office offers training to all new ATIPP Coordinators. To set up a training session, please call the ATIPP Office at 729-7072 or toll-free at 1-877-895-8891 or email atippoffice@gov.nl.ca.

Policy Manuals and Guides

- Protection of Privacy Policy and Procedures Manual
- Access Policy and Procedures Manual
- Municipal Council Handbook 2014

Other Resources

The Office of the Information and Privacy Commissioner (OIPC) – This office oversees the *ATIPP Act, 2015* in Newfoundland and Labrador; individuals can make a complaint to the OIPC regarding a decision of a municipality relating to an ATIPP request or if they believe the municipality has inappropriately collected, used, accessed or disclosed their personal information.

Appendix A - Notifying Third Parties About Requests for their Personal Information or Business Information

Step 1 – Assess the Information

No Notification Required When:

- You have decided not to disclose (e.g. will redact information).
- You determine that the information clearly:
  - does not meet the three-part test for third party business information; or
  - is not an unreasonable invasion of privacy

No need to proceed further.

Notification Required

In some cases, there will be factors in favour of disclosure and factors against disclosure. If you weigh these factors and decide to disclose, you must notify third parties. Determine whether you:

- intend to disclose the information (not sure but think you will disclose) - **go to step 2A**
- have decided to disclose the information – **go to step 2B**

Proceed to Step 2A or 2B as appropriate.

Step 2A: Notification where you intend to release

- Make every reasonable effort to notify third party
- Ask if the third party will consent to the release
- Provide a timeframe for third party to response
- Your time limit of 20 days continues to run throughout this process. Contact OIPC to request extension if necessary.

Proceed to Step 3A or 3B as appropriate.

Step 2B: Notification where you have decided to release

- Notify third party that they have 15 business day to file a complaint or appeal (form 7)
- Do not release information yet
- Wait 15 business days. Confirm with the OIPC whether the third party filed a complaint or appealed the decision:

If they did not:	If they did:
Release records	**Proceed to step 4**

Step 3A: Third Party Consents

Provide the information to the Applicant.

Request closed

Step 3B: Third Party does not Consent/Respond

Decide to redact	Decide to release
No need to proceed further	**Go to step 2B**

Step 4: Third party files complaint or appeals decision

- Advise the applicant of status of any complaints or appeals by a third party
- Wait until final decision is made by OIPC or Court:

OIPC/Court agrees with third party	OIPC/Court agrees with municipality*
Do not release records	**Release records**

**If OIPC agrees with municipality, ensure third party hasn't appealed with decision with the Court before releasing records*

Appendix B
Protection of Privacy

Privacy Breach Protocol

March 2015

Government of Newfoundland and Labrador
ATIPP Office, Department of Justice and Public Safety

TABLE OF CONTENTS

1. Introduction

The **Access to Information and Protection of Privacy (ATIPP) Office** has created the *Privacy Breach Protocol* to assist you in making key decisions when dealing with a privacy breach.

Each public body that collects, uses and discloses personal information is responsible for handling personal information in its custody or control. Where individual(s) are affected by a privacy breach, the public body must consider whether notification of the affected individuals is appropriate.

This protocol will guide you through decision-making steps setting out how to respond to a privacy breach:

- **Contain the Breach**
- **Evaluate the Risks**
- **Notify Affected Individuals (if appropriate)**
- **Prevent Future Breaches**

2. Privacy Breach Defined

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 the *Access to Information and Protection of Privacy Act* ("ATIPP Act").

The most common privacy breaches occur when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information is stolen or personal information is mistakenly provided to the wrong person.

3. Responding to a Privacy Breach

Step 1: Contain the Breach

You should take immediate action to contain the breach:

- **Contain the breach** – Immediately stop the unauthorized practice, recover the records, and shut or correct weaknesses in physical security. If the breach is unauthorized access to an IT asset, such as a computer, server or network, you MUST shut down the affected asset and contact the OCIO (or your IT representative) immediately.
- **Immediately contact your supervisor who will advise your departmental Executive,** including Minister and Deputy Minister; Communications Director; as well as Cabinet Secretariat, where appropriate; and your delegated Privacy Analyst in the ATIPP Office.

- **Download the *Privacy Breach Reporting Form*** and submit it to your Senior Privacy Analyst with the ATIPP Office and to the Office of the Information and Privacy Commissioner(OIPC). The form can be found on the OIPC's website at www.oipc.nl.ca.

- If there is a risk of criminal harm, you should **immediately contact the RNC or RCMP**.

Step 2: Evaluate the Risks

Evaluating potential risks to affected individuals is important in order to understand the scope of the breach and how it may affect those individuals whose information was subject to a breach. In order to evaluate the potential risks, consider the following:

Personal Information Involved

- What types of information are involved in the breach? Generally, the more sensitive the information, the higher the risk.
- Can the information be used for fraudulent or otherwise harmful purposes? (Social Insurance Numbers and financial information, for example, can be used for identity theft).

Cause and Extent of the Breach

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- How much information was collected, used or disclosed without authorization?
- How many individuals are likely to receive or have access to the information that was breached?
- Is the information protected by encryption or other means rendering it not readily accessible?
- What steps have already been taken to minimize the harm?

Individuals Affected by the Breach

- How many individuals are directly affected by the breach?
- Who was affected by the breach: employees, citizens, clients, other public bodies?

Foreseeable Harm from the Breach

- Is there any relationship between the unauthorized recipients and the information involved in the breach?
- What is the risk of harm to **affected individuals** as a result of the breach?
    - security risk (e.g. physical safety)
    - identity theft or fraud
    - loss of business or employment
    - hurt, humiliation, damage to reputation or relationships
- What is the risk of harm to the **public body** as a result of the breach?
    - loss of trust in the public body or organization
    - loss of assets
    - financial exposure
    - contractual and/or other legal obligations (contact your solicitor)
- What is the risk of harm to the **public at large** because of the breach?
    - risk to public health
    - risk to public safety

Step 3: Notification

A key consideration in deciding whether notification is necessary should be the mitigation of harm to any individuals whose personal information has been inappropriately collected, used or disclosed as a result of the breach.

Notify the ATIPP Office and the OIPC

When a privacy breach occurs, you must notify and submit a privacy breach reporting form to:

- The ATIPP Office - send to the Senior Privacy Analyst assigned to your public body. If you are unsure who the Senior Privacy Analyst assigned to your public body is, please send the form to the ATIPP Office by email (ATIPPOffice@gov.nl.ca); fax (729-2226) or contact the Office by phone (729-7072 or 1-877-895-8891).
- The OIPC - send the report by email (commissioner@oipc.nl.ca); fax (729-6500) or contact the Office by phone (729-6309 or 1-877-279-6309)

Notify Affected Individuals (if required or appropriate)

If there is a risk of significant harm cause by the breach, you are required to notify the individuals affected. When determining if notification is required or appropriate, consider the questions below:

Questions to Consider	Yes	No
Contractual and/or legal obligations Do you have contractual and/or legal obligations to notify affected individuals in the case of a privacy breach or loss of data?	☐	☐
Sensitivity of personal information breached Would a reasonable person consider the information breached to be sensitive? Some examples include:		
Medical information	☐	☐
Allegations relating to a crime	☐	☐
Criminal record	☐	☐
Employment or educational history	☐	☐
Risk of identity theft Is there a reasonable risk of identity theft or other fraud for affected individuals? Please check all applicable personal identifiers involved in the privacy breach:		
Social Insurance Number (SIN)	☐	☐
Driver's License Number	☐	☐
Medicare Plan Number (MCP)	☐	☐
Other Identifying Number (Please specify) _____	☐	☐
Credit or Debit Card Number	☐	☐
Other Information that could be used for fraudulent purposes (Please specify) _____	☐	☐
Risk of physical harm Is there a reasonable risk of physical harm, stalking or harassment for affected individuals?	☐	☐
Risk of hurt, humiliation, damage to reputation Is there a reasonable risk of hurt, humiliation or damage to the reputation of affected individuals? *Risk to reputation may be a concern if the breach includes mental health records, medical records or disciplinary records.*	☐	☐

Notifying Affected Individuals

As mentioned above, notification of affected individuals must occur if there is risk of significant harm. Some considerations in determining whether to notify individuals affected by the breach include:

- Contractual and/or other legal obligations requiring notification
- Sensitivity of the personal information breached
- Risks of identity theft or fraud (usually due to the type of information lost, such as Social Insurance Number and/or financial information)
- Physical harm (if the loss puts an individual at risk of being stalked or harassed)
- Risk of hurt, humiliation or damage to reputation (i.e. disciplinary or medical records)

When and How to Notify

When: If notification is to take place, it should occur as soon as possible following the breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed so criminal investigation is not impeded.

How: The preferred method of notification is direct (i.e. by phone, letter or in person) to affected individuals. Indirect notification (i.e. website information, posted notices, media) should generally occur only where direct notification could cause further harm, is cost prohibitive and/or there is insufficient contact information. Using multiple methods of notification in certain cases may be the most effective approach depending on the circumstances surrounding the breach (e.g. the availability of contact information for those affected and the sensitivity of the personal information).

The tables below set out factors to consider in deciding how to notify the affected individuals.

Considerations Favoring DIRECT Notification	Check if Applicable
The identities of the affected individuals are known	☐
Current contact information for the affected individuals is available/can be obtained	☐
Affected individuals require detailed information in order to properly protect themselves from harm resulting from the breach	☐

Considerations Favoring DIRECT Notification	Check if Applicable
Affected individuals may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	☐

Considerations Favoring INDIRECT Notification	Check if Applicable
The number of affected individuals is large making direct notification impractical	☐
Direct notification could compound the harm to the individual resulting from the breach	☐

What to Include in the Notification

The information in the notification should assist the affected individual in reducing or preventing harm that could be caused by the breach. It should include the information below:

Information Required in the Notification	Check if Included
Date of the breach	☐
General description of the breach	☐
Description of the information: Provide an overview of the information that was inappropriately accessed, collected, used or disclosed. *The information should be general and should <u>not</u> include the personal information that was breached. For example, you can say that the individual's date of birth was inappropriately disclosed, but you would not state the individual's actual date of birth in the notification.*	☐
Steps taken so far to control or reduce the harm	☐
Future steps planned to prevent further privacy breaches	☐

Steps the individual can take: Provide information detailing how individuals can protect themselves in light of the breach (e.g. contact credit reporting agencies to set up a credit watch, explain how to change a personal health number or driver's licence number)	☐
Organization contact information for further assistance: Provide contact information for someone within your organization who can answer questions, provide additional information and offer assistance to affected individuals	☐
Information and Privacy Commissioner: Provide OIPC contact information and notify individuals of their right to make a complaint to the OIPC	☐

Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

Additional Notifications to Consider	Check if Applicable
Law Enforcement if theft or other crime is suspected Law enforcement may request a temporary delay in notifying individuals for investigative purposes. It is important to discuss these matters with your Privacy Analyst and departmental solicitor.	☐
Professional or regulatory bodies You should contact any professional or regulatory bodies, if they require notification.	☐
OCIO / IT Staff If the breach was a data breach or the result of an information technology failure, you must contact the OCIO or your appropriate IT support staff. Additional contact with third parties may be required to ensure correction or repair of a technical issue.	☐

Step 4: Prevent Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, you should:

- thoroughly investigate the cause of the breach -- this could require a security audit of both physical and technical security;
- develop or improve, as necessary, adequate long term safeguards against further breaches;
- review your policies and update them to reflect the lessons learned from the investigation;
- audit at the end of the process to ensure that the prevention plan has been fully implemented; and,
- train all staff to know the organization's privacy obligations under the *ATIPP Act.*

4. ATIPP Office Contact Information

If you have any questions regarding this document, or privacy in general, please contact us:

Access to Information and Protection of Privacy Office

Department of Justice and Public Safety

4th Floor, East Block, Confederation Building

P.O. Box 8700

St. John's, NL

A1B 4J6

Tel: (709) 729-7072

Fax: (709) 729 -2129

Toll Free: 1-877-895-8891

Website: www.atipp.gov.nl.ca/