Protection of Privacy

Policy and Procedures Manual

June 2015

Table of Contents

CHAPTER 1: INTRODUCTION – PROTECTION OF PRIVACY

The Government of Newfoundland and Labrador is responsible for extensive amounts of personal information. Part III of the *Access to Information and Privacy of Privacy Act* (the "*Act*") seeks to protect this personal information by limiting how personal information can be collected, used and disclosed by public bodies. The *Act* also allows individuals the right to access and correct their personal information.

Part III of the *Act* is made up of sections 61-84. For the exact wording of these sections and to view an online version of the *Act*, please visit the House of Assembly website:

http://assembly.nl.ca/Legislation/sr/statutes/a01-2.htm

The Privacy provisions of the *Act* include the following sections:

- (61) Purpose for which information may be collected
- (62) How personal information is to be collected
- (63) Accuracy of personal information
- (64) Protection of personal information
- (65) Retention of personal information
- (66) Use of personal information
- (67) Use of personal information by post-secondary educational bodies
- (68) Disclosure of personal information
- (69) Definition of consistent purposes
- (70) Disclosure for research or statistical purposes
- (71) Disclosure for archival or historical purposes
- (72) Privacy impact assessment

The right to request correction of personal information is found in section 10 of the *Act*.

These sections are also supplemented by the definitions contained in section 2 of the *Act*, particularly the definition of ***personal information*** in paragraph 2(u). See section 2.1 of this manual for information on the definition of ***personal information***.

Divisions 2 and 3 of Part III set out the process by which individuals can make a complaint to the Office of the Information and Privacy Commissioner with respect to the collection, use and disclosure of their personal information. The commissioner is given the authority to investigate complaints that personal information has been collected, used or disclosed in contravention of the *Act*, and to make recommendations with respect to those complaints. Public bodies will be required to comply with the commissioner's recommendations unless they seek a declaration from the Supreme Court, Trial Division authorizing them not to do so.

1.1 Fair Information Practices

The *ATIPP Act* privacy provisions are based on standards for privacy protection developed by the Canadian Standards Association (CSA), known as the "Fair Information Practices". The CSA is a not-for-profit organization which develops standards to address the needs of business, industry, government and consumers. The Fair Information Practices are:

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

- Identifying Purposes
  The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected;

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

- Limiting Collection
  The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means;

- Limiting Use, Disclosure and Retention
  Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes;

- Accuracy
  Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used;

- Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information;

- Openness
  An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information;

- Individual Access
  Upon request, an individual shall be informed of the existence, use and/or disclosure of his/her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate; and

- Challenging Compliance
  An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

1.2 Privacy Tools for Assessing and Aiding in Compliance

The Access to Information and Protection of Privacy Office (ATIPP Office) oversees the implementation and coordination of the *Act* within the Government of Newfoundland and Labrador, government agencies, health care bodies, educational bodies and municipalities. The ATIPP Office has developed a number of tools to help public bodies assess compliance with the privacy provisions of the *Act.* These tools, while based on legislative compliance, also incorporate the 10 privacy principles discussed in the section entitled "Fair Information Practices."

A Privacy Impact Assessment (PIA) is an internationally recognized assessment method that can be applied to proposed programs or policies to identify potential privacy issues. PIAs examine such things as whether a proposed policy or program collects more personal information than is required, as well as the sharing of personal information that is collected; the access, storage, correction and disposal of personal information; and the proposed duration of the program or policy.

Section 72 of the *Act* requires government departments (and branches of the executive government) to conduct a preliminary assessment and, where required, a PIA. Government departments (and branches of the executive government), during the development of a program or service, must:

- conduct a PIA, or

- conduct a preliminary assessment showing that a PIA is not required, and

submit the results of the preliminary assessment or the PIA to the ATIPP Office with the Department of Justice and Public Safety.

To facilitate this requirement, the ATIPP Office has developed a ***PIA Protocol***. This Protocol is a framework to assess the compliance of a project and contains three tools:

1.2.1 The Preliminary PIA Checklist (PPIA)

The PPIA is the main tool used to assess privacy compliance for government activity and is used to assess whether a PIA should be completed for a project. This tool can be completed quickly and without the need for privacy expertise.

A PPIA must be conducted, in consultation with the ATIPP Office – Department of Justice and Public Safety, for every new or substantially modified program or service developed by a government department or branch of the executive government.

The purpose of conducting a preliminary assessment is to:

- identify the types and volumes of personal information that are to be collected, used and disclosed;
- verify the legislative and policy authorities for the proposed program or service;
- clarify the roles, responsibilities and legal and policy status of the primary stakeholders, including those of other jurisdictions and the private sector;
- determine which aspects of the program or service are likely to involve privacy risks; and
- determine whether a full PIA is required to be completed by the department.

The assessment tool is flexible and adaptable to initiatives ranging in scope from simple to complex. It is intended to avoid unnecessary effort on options or processes that are fundamentally incompatible with key privacy principles.

1.2.2 Privacy Impact Assessment (PIA)

A PIA is a process to determine the impacts of a proposal on an individual's privacy and ways to mitigate or avoid any adverse effects. It is used to ensure privacy issues are fully considered at an early stage of project development, particularly when there are significant privacy risks. A PIA must be completed for projects where the PPIA indicated that a PIA was necessary and requires a team which includes members who have significant privacy expertise, technical expertise and knowledge about the project.

A PIA may be required in the following circumstances:

- a new or increased collection, use or disclosure of personal information, with or without the consent of individuals;
- a broadening of target populations;
- a shift from direct to indirect collection of personal information;
- disclosure of personal information respecting a common or integrated program or service may be permitted under paragraph 68(1)(u);
- an expansion of personal information collection for purposes of program integration, program administration or program eligibility;
- new data matching or increased sharing of personal information between programs or across institutions, jurisdictions or sectors;
- development of or a new or extended use of common personal identifiers;
- significant changes to the business processes or systems that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information; or
- the contracting out or devolution of a program or service to another level of government or the private sector.

1.2.3 The Privacy Impact Report (PIR)

A PIR is used to summarize any privacy related issues discovered during the PPIA or PIA processes. It serves as the "signoff" letter from the ATIPP Office, indicating that project has been reviewed and includes recommendations on how personal information can be better managed in the project. The ATIPP Office may follow-up with departments on recommendations resulting from the PPIA or PIA process.

A PPIA must be conducted for every new or substantially modified program or service developed by a government department or branch of the executive government.

As noted above, for every new program or service developed by a department or branch of the executive government of the province, section 72(1) of the Act requires the minister responsible for that program or service to submit to the minister responsible for the *Act*:

- a PIA for review and comment; or
- the results of a preliminary assessment showing that a PIA of the program or service is not required.

Preliminary assessments and PIAs (where required) must be conducted in accordance with the directions set out by the minister responsible for the *Act* (subsection 72(2)). As such, the ***PIA Protocol*** referenced above should be followed.

1.2.4 Role of the Information and Privacy Commissioner

Where a common or integrated program or service is being developed, the minister responsible for the program or service must also notify the commissioner at an early stage of development (subsection 72(3)).

Where the Minister responsible for the administration of the *Act* receives a PIA respecting a common or integrated program or service for which disclosure of personal information may be permitted under paragraph 68(1)(u), the minister must, during the development of that program or service, submit the PIA to the commissioner for the commissioner's review and comment (subsection 72(4)).

A "common or integrated program or service" refers to a single program or service that is provided or delivered by two or more public bodies. The program or service may have several distinct components, each of which is provided or delivered by a separate public body. These components together comprise the common program or integrated service. Each public body partner must be integral to the program or service. For example, a nursing practicum program requires the participation of both the post-secondary institution, and the health care body; the program would not function without the services of each body. Public bodies may have clients in common, but that factor alone does not make a program or service common or integrated.

1.2.5 On-site Training Sessions

For those looking for an in-depth discussion of the *Act* or for those who would like specific information about how the *Act* affects their department or public body, onsite presentations are available. These training sessions have been developed by the ATIPP Office, are presented by analysts from the ATIPP Office and include topics such as "An Introduction to Privacy"; "An Introduction to Access to Information"; "Protecting Personal Information in the Workplace"; "Privacy Plans and Maximizing Legislative Compliance"; and "Responding to Access Requests". If you are interesting in receiving training, presentations can be arranged by calling the ATIPP Office at 709-729-7072 or by contacting your Senior Privacy Analyst.

1.2.6 Online Training Module, Quizzes and Case Studies

In addition to our on-site training sessions, the ATIPP Office also offers tools and resources for those who would like a quick refresher in access and privacy compliance. The ATIPP Office, along with the Centre for Learning and Development, has developed an online

training module, short quizzes, and case studies reflecting findings and recommendations of Information and Privacy Commissioners from across the country.

Government officials are required to complete the ATIPP online training to ensure they are aware of their obligations under the Act. The online training module can be accessed through the Centre for Learning and Development online through PS Access.

The quizzes and case studies were created to illustrate the practical applications of the *Act* and are a great resource for those interested in a quick overview of access and privacy issues. Quizzes and case studies can be obtained by contacting the ATIPP Office or your Senior Privacy Analyst.

1.3 Developing Legislation and Consulting with the Commissioner

Where a department is developing legislation which might have implications for the protection of privacy (or for access to information), section 112 of the Act requires the minister responsible for the legislation to consult with the Office of the Information and Privacy Commissioner as soon as possible before, and not later than, the date on which notice to introduce the Bill in the House of Assembly is given.

The commissioner must advise the minister as to whether the proposed Bill has implications for access to information or the protection of privacy, and may comment publicly on the Bill at any time after the Bill has been made public (subsections 112(2) and (3)).

1.4 Publication Schemes (section 111)

Section 111 applies only to those public bodies that are listed in the regulations (subsection 111(6)).

A **publication scheme** is an outline of the classes of information each public body will publish or intends to publish so it may be read easily by the public.[1]

Section 111(1) of the *Act* requires the commissioner to create a standard template for the publication of information by public bodies to assist the public in identifying and locating records in the custody or under the control of public bodies.

Where a public body is listed in the regulations as being required to comply with section 111, the head of the public body must adapt the standard template developed by the commissioner and publish its own information according to that adapted template (subsection 111(2)).

[1] Report of the 2014 Statutory Review Committee at p. 323.

The published information must include:

- a description of the mandate and functions of the public body and its components (paragraph 111(3)(a));

- a description and list of the records in the custody or under the control of the public body, **including personal information banks** (paragraph 111(3)(b));

- the name, title, business address and business telephone number of the head and ATIPP coordinator of the public body (paragraph 111(3)(c)); and

- a description of the manuals used by employees of the public body in administering or carrying out the programs and activities of the public body (paragraph 111(3)(d)).

Section 111(4) requires that additional information be published with respect to "personal information banks". A personal information bank is personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. This means personal information contained in either paper or electronic file banks that relates to an individual and is organized and retrieved using a personal identifier (i.e. individual's name, employee number, social insurance number, etc.)

Not all collections of personal information will be considered to be personal information banks. The key to determining whether a group of files, which contain personal information, is a personal information bank is the way it is arranged or retrieved.

For example, collections of personal information that relate to an individual and are organized and retrievable by the person's last name or personal identifier are considered personal information banks. Collections of personal information that are organized and retrieved by an identifier that relates to a corporate body or other search field are not listed as personal information banks, even if the collections contain personal information.

A personal information bank has three key components:

1. **It contains personal information**
   This includes personal information as defined in paragraph 2(u) which means recorded information about an identifiable individual.

2. **It takes the form of a collection**
   Collection means acquiring, receiving, obtaining, gathering or compiling personal information. The collection can include various forms such as paper, electronic, pictures, video or audio. This may include applications or registrations for benefits or services, client or customer files and databases, membership lists, mailing lists and contact databases, licensing applications and certificates, program participation information and investigations, inspections, or audits.

3. **It is organized or retrievable by the name or an identifying number, symbol or other particular assigned to an individual**
   This means the information is organized or retrievable by name, MCP number, driver's license number, student identification number or some other unique identifier.

For each personal information bank maintained by a public body, subsection 111(4) requires that the following information be published:

- its name and location;
- a description of the kind of personal information and the categories of individuals whose personal information is included;
- the authority and purposes for collecting the personal information;
- the purposes for which the personal information is used or disclosed; and
- the categories of persons who use the personal information or to whom it is disclosed.

Where personal information is used or disclosed by a public body for a purpose that is not included in the information published under subsection 111(2), the head of the public body shall:

- keep a record of the purpose and either attach or link the record to the personal information; and
- update the published information to include that purpose.

Subsection 116(l) of the *Act* gives the Lieutenant-Governor in Council the authority to prescribe, by regulation, which public bodies are required to comply with all or part of section 111.

CHAPTER 2: COLLECTION OF PERSONAL INFORMATION

Part III of the *Act* serves to protect the personal information of individuals. It achieves this goal by:

- providing individuals with the ability to seek and gain access to their own personal information or requesting corrections to this information which is in the custody and control of public bodies;
- limiting the collection, use and disclosure of personal information by public bodies;
- requiring public bodies to collect personal information directly from the individuals the information is about, unless the individual, another Act or regulations or the *Act* authorizes collection from another source;
- requiring public bodies to provide notice to individuals where they are collecting personal information, including the authority for collection by the public body, the purpose for which the information is collected, and contact information for a person who can answer questions about the collection, if required;
- requiring public bodies to retain information it uses to make decisions affecting an individual for at least one year;
- requiring public bodies to take reasonable steps to ensure that adequate security and protection policies and practices are in place relating to the personal information in its custody and control;
- requiring public bodies to notify affected individuals where personal information has been stolen, lost, disposed of or disclosed without authorization and there is a significant risk of harm;
- limiting a public body's use and disclosure of personal information to the original purpose for which it was collected, for a consistent purpose, for another purpose with the individual's consent or a purpose authorized in the *Act*;
- limiting the use and disclosure of personal information to the minimum amount necessary to carry out its objective in a reasonable manner; and
- establishing a formal oversight of public bodies' handling of personal information by authorizing the Office of the Information and Privacy Commissioner to conduct audits and investigate complaints of unauthorized collection, use and disclosure of personal information.

A public body ***collects*** personal information whenever it acquires, receives, obtains, gathers, or compiles personal information and then creates a record of that personal information. This includes, but is not limited to, personal information that is:

- gathered by the public body in forms, interviews or correspondence;
- provided to the public body by another public body;
- collected by a contractor or other third party on behalf of the public body;
- in correspondence received by the public body, including unsolicited records (e.g. letters and résumés); and
- captured through print, video or audio recordings and/or through other forms of electronic media.

Under the *Act*, public bodies are only permitted to collect, use and/or disclose the minimum amount of information needed to accomplish the purpose(s) for which the information was collected, used or disclosed. For example, if only the name and telephone number of a person is required for a program, then address and social insurance number should not be collected.

To ensure that only the minimum amount of information needed is collected, used or disclosed, public bodies should:

- ensure that access to and use of personal information by employees or agents of the public body is limited to those who need the information in order to carry out their assigned duties or carry out a purpose authorized under section 66;
- conduct a PPIA or PIA on any new or substantially modified program or service;
- review their methods of collection, reasons for use and methods of disclosure to ensure that only the minimum amount of information is collected, used or disclosed; and
- provide privacy training to ensure staff understand what is meant by "minimum amount of information" and are compliant with the Act.

2.1 Personal Information Defined (paragraph 2(u))

The privacy provisions of the *Act* apply only to personal information. ***Personal information*** is defined under paragraph 2(u) as follows:

> *2 (u) **personal information** means recorded information about an identifiable individual, including*
>
> *(i) the individual's name, address or telephone number,*

(ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

(iii) the individual's age, sex, sexual orientation, marital status or family status,

(iv) an identifying number, symbol or other particular assigned to the individual,

(v) the individual's fingerprints, blood type or inheritable characteristics,

(vi) information about the individual's health care status or history, including a physical or mental disability,

(vii) information about the individual's educational, financial, criminal or employment status or history,

(viii) the opinions of a person about the individual, and

(ix) the individual's personal views or opinions, except where they are about someone else.

Personal information is information that can identify an individual (e.g. name, address, social insurance numbers). Some information on its own is sufficient to identify an individual (e.g. name) whereas in other instances, information must be combined to identify an individual (address, age and gender of the individual). Information that relates directly to and is about an individual is considered the personal information of the individual.[2]

It is important to note that while paragraph 2(u) provides examples, it is not an exhaustive list of personal information. Photographs, driver license numbers and social insurance numbers are also considered to be forms of personal information, although they are not specifically included in the definition of ***personal information***.

2.2 Purpose for Collecting Personal Information (section 61)

Section 61 limits the circumstances whereby a public body may collect personal information:

61 No personal information may be collected by or for a public body unless

[2] *Report P-2009-002*, Newfoundland and Labrador Information and Privacy Commissioner

> *(a) the collection of that information is expressly authorized by or under an Act;*
>
> *(b) that information is collected for the purposes of law enforcement; or*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body.*

Personal information should not be collected for any purposes other than those provided for under section 61. If a public body does not meet the above criteria when collecting personal information, they should not be collecting that information.

Section 61 provides that personal information may be collected ***by*** or ***for*** a public body. Collection of personal information may be carried out by the public body itself, by another public body, or by an outside organization (such as a contractor) on behalf of the public body. A public body is bound by the requirements of the *Act* whether it collects the personal information itself or authorizes another party to collect the personal information on its behalf. In such circumstances, a contractor could be considered an extension of the public body.

Public bodies should note that where an outside agent or organization is collecting personal information on behalf of a public body, the public body should have a written agreement in place to ensure the personal information is properly protected when in the custody of another party. The agreement should address such matters as use, security, retention and disclosure of the personal information. For additional information related to formalized agreements for the sharing of personal information, please contact the ATIPP Office or your departmental solicitor.

A public body must demonstrate that it is meeting the requirements set out in section 61 relating to its collection of personal information. Where the public body cannot demonstrate that it is meeting the requirements, it should revisit the policy of collecting certain personal information.[3]

2.2.1 Collection is Expressly Authorized by or under an Act (paragraph 61(a))

Paragraph 61(a) permits the collection of personal information where it is expressly authorized by or under an Act. In order for collection to be authorized under an Act, the Act must expressly state that information may be collected. It is not sufficient for an enactment to merely imply or suggest that a public body has this authority.[4]

[3] *Report P-2008-002*, Information and Privacy Commissioner of Newfoundland and Labrador
[4] *Order F2006-004*, Information and Privacy Commissioner of Alberta

2.2.2 Collected for the Purposes of Law Enforcement (paragraph 61(b))

Paragraph 61(b) provides that personal information can be collected for the purposes of law enforcement. Under paragraph 2(n), ***law enforcement*** is defined as "policing, including criminal intelligence operations; or investigations, inspections or proceedings conducted under the authority of or for the purpose of enforcing an enactment which lead or could lead to a penalty or sanction being imposed under an enactment." Any collection of personal information must meet the definition of law enforcement to be permissible under paragraph 61(b). Law enforcement is discussed further in section 2.3.2.8 of this manual, "Law Enforcement."

2.2.3 Relates Directly to and is Necessary for an Operating Program or Activity (paragraph 61(c))

Paragraph 61(c) permits a public body to collect personal information where that information relates directly to and is necessary for an operating program or activity of the public body.

Relates directly *to* means that the personal information must have a direct bearing on the program or activity.

Necessary for means that the public body must be able to demonstrate a need for the information being collected.

In assessing whether personal information is "necessary", the sensitivity of the personal information must be considered including the particular purpose for the collection and the amount of personal information collected and assessed in light of the purpose for collection.[5]

An ***operating program*** is a series of functions designed to carry out all or part of a public body's operations. An ***activity*** is an individual action designed to assist in carrying out an operating program.

2.3 How Personal Information is to be Collected (section 62)

Section 62 provides that personal information should be collected directly from the individual it is about, subject to limited exceptions. When collecting personal information, public bodies also have an obligation to notify the person from whom the information is collected of the purpose for the collection, the authority for collecting, and the contact information for someone in the public body who can answer questions regarding the collection.

[5] *Order F07-10*, Information and Privacy Commissioner of British Columbia

2.3.1 Direct Collection (subsection 62(1))

As stated in subsection 62(1), as a general rule, public bodies should collect personal information directly from the individual the information is about.

There are advantages to direct collection. First, it ensures individuals are aware of the information being collected. It also gives the public body a clear opportunity to inform the individual how the information will be used and to whom it will be disclosed.

Secondly, direct collection allows public bodies to ensure information is as accurate as possible. For example, it is unlikely that an individual would incorrectly state his/her date of birth.

The public body can collect personal information directly through:

- Interviews – This is an effective way to collect personal information. When interviewing an individual, public body employees should remember to:
    - always ask for photo identification or another suitable identifier in order to confirm an individual's identity prior to collecting his/her personal information;
    - inform the individual from whom they are collecting the information of the reason(s) for the collection; and
    - ensure that they collect only the minimum amount of personal information necessary to achieve the purpose of collection.
- Forms – This is another useful way in which public bodies can collect personal information. When using forms to collect personal information, public body employees should remember to:
    - ensure that all forms include a privacy notice. If a form does not include a privacy notice, the public body should consider revising and in the interim, should inform the individuals verbally of their privacy rights under the *Act*;
    - ensure that forms collect only the minimum amount of personal information necessary to achieve the purpose of collection; and
    - ask for photo identification when forms are submitted to verify that information is being collected from the person the information is about, where appropriate.

- Correspondence – In some instances, personal information can be collected by the public body through correspondence with individuals, other stakeholders or the general public. When a public body receives correspondence, public body employees should remember to:

    - place all incoming correspondence in the individual's file; and

    - ensure that they collect only the minimum amount of personal information necessary to achieve the purpose of collection.

- Telephone and/or Email - It is common for clients or the general public to communicate with public bodies via telephone or email. However, it is important to verify the identity of those individuals in the same manner that would be conducted in person:

    - Telephone – if discussing a file that includes personal information, or collecting personal information from that person, ensure to ask the individual identifying questions (e.g. address, full name, file number, historical questions (place of birth, last employer)). Please contact the ATIPP Office for examples.

    - Email - Personal information should not be sent over email unless the recipient's email address has been verified. Even once it is verified, personal information should only be sent using encrypted email to avoid potential breaches. For steps on how to encrypt email, visit http://www.ocio.gov.nl.ca/ocio/im/employees/pdf/OCIO_Encrytion_Steps.pdf .

2.3.2 Indirect Collection (subsection 62(1))

Even though direct collection of personal information is always preferred, section 62 provides some exceptions to direct collection.

Indirect collection means personal information is being obtained from someone other than the person the information is about. Subsection 62(1) allows indirect collection of personal information in specific circumstances.

Please note that where information is collected indirectly, the purpose of the collection must still comply with section 61 and that even where indirect collection is permitted, the personal information collected should be limited to only that information which is necessary.

In instances where indirect collection of personal information is permitted, public bodies should:

- inform individuals that indirect collection is permitted if the individual the information is about authorizes the collection. Public body employees should:

- ensure that the authorization is in writing, if possible. If authorization must be given verbally, the employee should document the conversation and send a letter to the individual confirming the authorization;

- develop and enforce **Information Sharing Agreements** that permit the transfer of personal information between the departments of public bodies and between public bodies;

- ensure that third party contractors are compliant with the *Act* by entering into formal agreements with the third parties which provide services. The formal agreement should:

    - stipulate that the third party must agree to follow and comply with the policies and procedures developed by the public body;

    - contain a detailed description of the information the third party is authorized to collect, use or disclose;

    - document the security measures used by the third party to protect the personal information in their custody or control;

    - permit the public body to review the policies and procedures of the third party related to the protection and management of personal information to verify they are consistent with those of the public body;

    - include the ability to audit compliance with the public body's policies and procedures to ensure compliance with the *Act;* and

    - be in writing.

2.3.2.1 Indirect Collection Authorized by the Individual (clause 62(1)(a)(i))

> *62(1) A public body shall collect personal information directly from the individual the information is about unless*
>
> > *(a) another method of collection is authorized by*
> >
> > > *(i) that individual, […]*

Information can be collected indirectly if the collection is authorized by the individual. Such authorization should be in writing, if possible, although verbal consent may be appropriate in certain situations. If authorizations must be given verbally, the public body should document the conversation and send a letter to the individual confirming the authorization.

When an individual is asked to authorize indirect collection of personal information under clause 62(1)(a)(i), the individual should be informed of:

- the nature of the personal information to be collected, specifically what type of information is going to be collected and how much will be collected;
- the purpose for the collection (i.e. what the personal information will be used for);
- any reasons for collecting the information indirectly;
- who is collecting the information, who will be receiving the information and any expiry date for the individual's authorization for indirect collection; and
- what the consequences may be, if any, for refusing to authorize the indirect collection.

2.3.2.2 Indirect Collection Authorized by the Commissioner (clause 62(1)(a)(ii))

> *62(1) A public body shall collect personal information directly from the individual the information is about unless*
>
> > *(a) another method of collection is authorized by*
> >
> > > *(i) the commissioner under paragraph 95(1)(c), […]*

Paragraph 95(1)(c) of the *Act* provides that the commissioner may "review and authorize the collection of personal information from sources other than the individual the information is about."

2.3.2.3 Indirect Collection Authorized by an Act or Regulation (clause 62(1)(a)(iii))

> *62(1) A public body shall collect personal information directly from the individual the information is about unless*
>
> > *(a) another method of collection is authorized by*
> >
> > > *(iii) an Act or regulation;*

When using this section, the legislation authorizing the indirect collection should describe the type of personal information to be collected. For example, the *Highway Traffic Act* permits the Registrar of Motor Vehicles to release personal information to a person or insurance company that may be liable to pay damages resulting from an accident.

2.3.2.4 Indirect Collection Authorized under Sections 68 - 71 (paragraph 62(1)(b))

> *62(1) A public body shall collect personal information directly from the individual the information is about unless*
>
> > *(b) the information may be disclosed to the public body under sections 68 to 71; […]*

Sections 68 to 71 set out the circumstances where public bodies may disclose personal information:

- Disclosure of personal information (section 68)
- Disclosure for research or statistical purposes (section 70)
- Disclosure for archival or historical purposes (section 71)

This provision allows a public body to collect personal information from another public body rather than from the individual the information is about, where the second public body is authorized to disclose the information under sections 68-71. In other words, if a public body is authorized to disclose certain personal information to another public body, the receiving public body is, in turn, authorized to collect the information and to use it for the purpose for which it was disclosed.

Where a public body is relying on paragraph 62(1)(b) to collect personal information indirectly, the public body that has the information must be satisfied that the disclosure is permitted under sections 68-71. Where such disclosure is permitted, indirect collection of personal information is authorized by the public body.[6] Furthermore, the public body receiving the information must also ensure that it is permitted to collect the information.

2.3.2.5 Determining Suitability for an Honour or Award (clause 62(1)(c)(i))

> 62 (1) *A public body shall collect personal information directly from the individual the information is about unless*
>
> > *(c) the information is collected for the purpose of*
> >
> > > *(i) determining suitability for an honour or award, including an honorary degree, scholarship, prize or bursary; […]*

A public body may collect personal information indirectly for determining the individual's suitability for an honour or award. This provision allows a public body to collect such information where it is considering granting an honour or award to an individual without the individual's knowledge. his clause of the *Act* lists some examples of honours and awards – an honorary degree, scholarship, prize or bursary – this is not an exhaustive list.

[6] *Report P-2009-002*, Newfoundland and Labrador Information and Privacy Commissioner

2.3.2.6 Proceeding before a Court or Tribunal (clause 62(1)(c)(ii))

> 62 (1) *A public body shall collect personal information directly from the individual the information is about unless*
>
> > *(c) the information is collected for the purpose of*
> >
> > *[…]*
> >
> > *(ii) an existing or anticipated proceeding before a court or a judicial or quasi-judicial tribunal, […]*

A public body may collect personal information indirectly if the information is for a proceeding before a court or tribunal. Examples of such proceedings include:

- a court proceeding in which a person is charged with a criminal offence;
- a civil proceeding (e.g. where a citizen is bringing a lawsuit against a Department);
- a hearing before the Human Rights Commission; or
- a hearing before the Labour Relations Board.

When collecting personal information for a proceeding, public bodies must ensure that the collection is limited only to the information necessary and relevant to the proceeding.

If you are unsure about whether a particular proceeding falls under this section, please consult your departmental solicitor.

2.3.2.7 Collecting a Debt or Making a Payment (clause 62(1)(c)(iii))

> 62 (1) *A public body shall collect personal information directly from the individual the information is about unless*
>
> > *(c) the information is collected for the purpose of*
> >
> > *[…]*
> >
> > *(iii) collecting a debt or fine or making a payment, […]*

Clause 62(1)(c)(iii) permits the public body to obtain personal information indirectly to enable the public body to collect a debt or make a payment.

Where a public body is collecting a debt or fine owing to it or to make a payment to an individual, it is permitted to collect information indirectly. This may be necessary, for example, where the public body cannot locate the individual or believes it would not obtain complete or accurate information from the individual, etc.

A ***debt*** is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

A ***fine*** is a monetary punishment imposed on a person who has committed an offence, including an offence under a bylaw.

A ***payment*** is a sum of money that the public body owes to an individual. Usually, this situation will arise when an individual has moved and the public body does not have a forwarding address, or where the public body is trying to verify the identity of the individual in order to make the payment.

2.3.2.8 Law Enforcement (clause 62(1)(c)(iv))

> 62 (1) *A public body shall collect personal information directly from the individual the information is about unless*
>
> > *(c) the information is collected for the purpose of*
> >
> > *[...]*
> >
> > *(iv) law enforcement;*

Indirect collection of personal information is permitted for law enforcement purposes. ***Law enforcement*** is defined in the *Act* as follows:

> *(2)(n) "law enforcement" means*
>
> > *(i) policing, including criminal intelligence operations, or*
> >
> > *(ii) investigations, inspections or proceedings conducted under the authority of or for the purpose of enforcing an enactment which lead to or could lead to a penalty or sanction being imposed under the enactment;*

In order for a public body to collect personal information indirectly under clause 62(1)(c)(iv), the public body must ensure that the activity for which they are collecting information falls within the definition of ***law enforcement*** set out in paragraph 2(n).

Where a public body is uncertain whether the activity for which they are collecting information falls within the definition of law enforcement, they should consult their departmental solicitor.

For more information on the definition of law enforcement, see section 4.8.4 of the **Access to Information Policy and Procedures Manual**.

2.3.2.9 Collection is in the Individual's Interest (paragraph 62(1)(d))

A public body is permitted to collect information indirectly where the collection of information is in the interest of an individual, pursuant to paragraph 62(1)(d), which states:

> 62(1) A public body shall collect personal information directly from the individual the information is about unless
>
> (d) collection of the information is in the interest of the individual and time or circumstances do not permit collection directly from the individual.

There are two requirements:

- collection of personal information must be in the interest of the individual who is the subject of that information; in other words, there must be some benefit to the individual resulting from the collection of personal information, and
- time or circumstances do not permit collection of the personal information directly from the individual (e.g. there is some element of urgency).

For example, where an individual is involved in a workplace accident and is rendered unconscious, the department may collect the next of kin information to notify family.

2.3.3 Notification of Collection (subsection 62(2))

Subsection 62(2) sets out the requirement for public bodies to notify individuals from whom they are collecting personal information. It also stipulates what information must be included in the notice.

> *62 (2) A public body shall tell an individual from whom it collects personal information*
>
> *(a) the purpose for collecting it;*

(b) the legal authority for collecting it; and

(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

The ***purpose*** for collecting information means the reason(s) why the information is needed by the public body and the use(s) that the public body will make of the personal information.

The ***legal authority*** for collecting information means specifically what legislation or enactment specifically permits the public body to collect information. This could be an enactment of Newfoundland and Labrador or Canada or it could be paragraph 61(c) which permits a public body to collect information where the information relates directly to and is necessary for an operating program or *activity* of the public body.

Where a public body intends to rely upon paragraph 61(c) and where the program is authorized by an enactment, regulation, bylaw or other legal resolution, the public body should cite in its notice the authority which authorizes the program.

Providing the ***contact information*** for someone who can answer individuals' questions about the collection is important. It is intended to provide individuals with a knowledgeable source of information.

The person who is given as the contact person for the public body should be:

- knowledgeable about the program for which the information is being collected;
- able to explain why the public body is collecting personal information;
- able to explain how the personal information will be used; and
- able to identify other public bodies to which the information may be disclosed.

Examples of circumstances in which notification to individuals about collection of their personal information would be required include:

- a public body is collecting personal information about an individual for the purpose of determining eligibility in a program or to receive a service; or
- personal information is collected on a client survey where that information would individually identify an individual.

Subsection 62(2) outlines the ***privacy notice*** requirement. This is the information required to be given to an individual where a public body is collecting personal information directly from that individual. Privacy notices should be in writing, where possible. Any forms used to collect personal information should contain a privacy notice.

The legal authority for the collection, required by parapgraph 62(2)(b), may be found in an Act (including the *ATIPP Act*), a regulation, a contractual agreement, court order, etc. If you are not sure if you have the legal authority to collect the information, please contact your departmental solicitor.

Where a variety of personal information is collected, the notice should state the purpose and authority for collecting all pieces of information. If there are two different purposes for collection, those purposes should be described in the privacy notice. For examples of written privacy notices, please contact the ATIPP Office.

A written privacy notice may not always be possible. For example, a public body may need to collect information on an urgent basis but the individual may live outside the area and may not have access to email or a fax machine. When a verbal notice is used, it should contain the same required information as the written privacy notice – the purpose for collection; the authority for collection; and the contact information of an employee who can answer questions about the collection of personal information.

A verbal privacy notice should be provided prior to collecting personal information. If the public body gives notice verbally, the public body should follow up with a letter confirming the verbal privacy notification.

In order to inform individuals and the general public about how their personal information is collected, used and disclosed under the *Act*, the public body should:

- use privacy notices to inform individuals when collecting personal information, of:
    - the purpose for the collection, use and disclosure of personal information;
    - the authorization for the collection, use and disclosure of personal information; and
    - the title, business address and business telephone number of an officer or an employee of the public body who can answer the individual's questions about the collection, use and disclosure of information.
- where appropriate, publicize the privacy notice by:
    - including the privacy notice on all forms that collect personal information;
    - posting the privacy notice in high traffic areas;
    - including the privacy notice in brochures developed by the public body; and/or
    - posting the privacy notice on the public body's website.

- allow employees to use a verbal privacy notice if the collection of information is deemed urgent and the individual is unable to visit the public body and is unable to access email or a fax machine.

- employees who have used a verbal privacy notice should:

    - place a note in the individual's file which describes the conversation between the employee and the individual, contains information on whether or not the individual consented to the collection, use and/or disclosure of their personal information and is dated and signed by the employee;

    - send a copy of the note to the individual through the mail so that the individual also has a record of the conversation; and

    - replace the verbal consent with formal written consent as soon as possible; and

- review the privacy notice annually, unless an event or newly enacted legislation determines that the privacy notice should be changed or updated.

2.3.4 Where Privacy Notice is not Required (subsection 62(3))

Subsection 62(3) provides limited exceptions to the requirement to give notice to individuals whose personal information is being collected.

> *62(3) Subsection (2) does not apply where*
>
> *(a) the information is about law enforcement or anything referred to in subsection 31(1) or (2); or*
>
> *(b) in the opinion of the head of the public body, complying with it would*
>
> *i) result in the collection of inaccurate information, or*
>
> *ii) defeat the purpose or prejudice the use for which the information is collected.*

This provision should only be used in specific and limited circumstances within programs. When using this exception to avoid the requirement to provide notice to individuals, public bodies should document when the provision has been used and the reasons for not notifying.

2.4 Accuracy of Personal Information (section 63)

Section 63 places the onus on public bodies to ensure the personal information they use to make a decision directly affecting an individual is accurate and complete. Section 63 states:

> *63. Where an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body shall make every reasonable effort to ensure that the information is accurate and complete.*

This requirement is limited to situations where the personal information will be used to make a decision that directly affects the individual.

A ***decision that directly affects the individual*** is one that has an impact on an individual's life or affects their rights. Examples include determining if an individual is entitled to a benefit, such as income support, or determining if an individual will be offered a job with the public service. This section only applies where a decision has been or will be made. Where no decision will be or has been made, section 63 does not apply.

The meaning of ***reasonable effort*** will depend on the circumstances and may include:

- conducting periodic checks, directly with the individual or using other authorized avenues to ensure the information is still current and valid;
- undertaking thorough reviews of applications to ensure all questions are answered completely (e.g. application for employment or income support);
- documenting when personal information is collected or received; and
- implementing processes for correcting personal information.

When collecting, using or disclosing personal information, the public body will take reasonable steps to ensure that the information is as accurate as possible.

The public body should endeavour to collect, use and disclose accurate personal information by:

- collecting, where possible, personal information directly from the individual the information is about;
- encouraging public body employees to assist individuals when they are providing information to the public body (filling out forms, waiving consent, etc.);

- encouraging public body employees to confirm the accuracy of the personal information by confirming commonly used data elements, such as: name, date of birth, home address;

- encouraging public body employees to identify the individual or authorized individual before they collect personal information;

- taking steps to update the information in their custody or control when necessary;

- documenting any inaccuracies if it is not possible for the employee using the information to make the required changes;

- deleting information that is no longer relevant or needed; and

- protecting the information in their custody or control from unauthorized access which may corrupt the information being held.

CHAPTER 3: CONSENT

In order to protect the privacy rights of individuals, public bodies should obtain an individual's consent before collecting, using or disclosing the personal information of that individual, where appropriate.

When obtaining consent from an individual, the public body should:

- ensure that the person providing consent is the person the information is about, or another person authorized to give consent, as described in section 108*;*

- strive to ensure that an individual's consent is ***informed consent***. Informed consent can be ensured by:

    - making certain that individuals understand what is being asking of them before they consent to the collection, use or disclosure of their personal information. This means that public body employees should answer all questions so that individuals are comfortable in giving their consent;

    - ensuring that consent is voluntary and that individuals, in no way, feel obligated or coerced into giving their consent;

    - encouraging English as Second Language individuals to avail of translating services (a translator could be a trusted friend or family member or a paid professional); and

    - allowing those with low literacy to ask questions and/or bring someone they trust in order to assist them.

- attempt to obtain consent in writing by:

    - using application forms that include a section describing and explaining the consent being sought by the public body; or

    - using separate consent forms when the terms of use and disclosure have changed.

- allow public body employees to obtain verbal consent in limited circumstances where written consent cannot be obtained. If a public body employee obtains consent verbally, the employee should:

    - obtain the consent at the beginning of the conversation, prior to collecting information;

- take notes on what was discussed, including the date of the discussion, and then place the notes in the individual's file;

- include all information that is included in the written consent form; and

- where possible, send a follow-up letter describing what was discussed.

- allow an individual to withdraw consent at any time. If an individual decides to withdraw consent, the public body should:

  - ensure that the withdrawal of consent is in writing, either by having the individual fill out a withdrawal of consent form developed by the public body or by accepting a letter of withdrawal from the individual;

  - explain the terms of withdrawal to the individual who has withdrawn his/her consent, (e.g. the withdrawal of consent is not retroactive);

  - explain the implications/consequences of withdrawal to the individual who has withdrawn his/her consent (e.g. the public body may no longer be able to provide a certain service, etc.); and

  - inform **all** who work with the individual's personal information (public body employees and external agencies, etc.) that the consent has been withdrawn.

CHAPTER 4: USE OF PERSONAL INFORMATION

4.1 Public Body May Use Personal Information (section 66)

A public body may use personal information for the purposes for which it was originally collected or compiled, or for other purposes with the consent of the individual. A public body may also use personal information for another purpose for which the *Act* authorizes disclosure. The purpose of the collection must be authorized under section 61 ("***Purpose for which personal information may be collected***").

Section 66 sets out the circumstances where public bodies may use personal information as follows:

> *66(1) A public body may use personal information only*
>
> *(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 69;*
>
> *(b) where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act; or*
>
> *(c) for a purpose for which that information may be disclosed to that public body under sections 68 to 71.*
>
> *(2) The use of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.*

Prior to using personal information and in order to ensure compliance with section 66, you must review the purpose for the original collection of personal information. You must only use the personal information for the purposes identified in the notice provided to the individual or for a purpose which is consistent with the notice, unless otherwise permitted within the *Act* (see section 69 of the *Act*, "***Definition of consistent purposes***").

Any use of personal information that does not meet the above criteria is not permissible under the *Act*. It is important to examine this section if you intend to use personal information for a use other than the originally intended purpose.

If a public body is permitted to use personal information for another purpose, under paragraphs 66(1)(a), (b) or (c), they should document the new use and cite the section(s) of the *Act* that allows them to use this information for a new purpose and consider updating their privacy notice. This should be done even in instances where the public body believes

that the new use is consistent with the purpose for which the personal information was originally collected.

It can sometimes be difficult to determine the difference between a ***use*** and a ***disclosure*** of personal information.

Using personal information usually means using it internally (within the department or agency) for the administration of a project or program. For example, an individual has provided specific personal information to a department and that department has collected this information for the purpose of permitting that individual to apply for a student loan. Employees in that department may use that individual's personal information for the purposes of evaluating whether or not that individual is eligible for a student loan.

Disclosing personal information means showing, sending, telling or giving someone, another department, agency or organization the personal information in question. Information is disclosed externally when provided outside the original public body (i.e. department or agency or outside the Government of Newfoundland and Labrador). To continue the example above, providing the student's name and address when requested by Canada Revenue Agency may be a valid disclosure of personal information.

4.1.1 Use for Consistent Purpose (paragraph 66(1)(a))

A public body may use information for the purpose for which it was originally collected. Examples include the administration of a program offered and managed by a public body, delivering a service or other activities that relate directly to the purpose for which information was originally collected.

The *ATIPP Act* allows personal information to be used for a ***consistent purpose***, pursuant to paragraph 66(1)(a). A ***consistent purpose*** is defined in section 69 as:

> *69 A use of personal information is consistent under section 66 or 68 with the purpose for which the information was obtained or compiled where the use*
>
> *(a) has a reasonable or direct connection to that purpose; and*
>
> *(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.*

There are no hard and fast rules as to what constitutes a use for a consistent purpose. One guideline to consider is whether a person would reasonably anticipate or expect the personal information to be used in the newly proposed way, even if this use was not spelled out at the time the personal information was originally collected.

In order for a proposed new use to have "a reasonable and direct connection" to the original purpose, there must be some logical and plausible link to the original purpose. The consistent use should grow out of or be derived from the original use; it should not be a completely unrelated or secondary use of the information. Public bodies must be conscious of, and avoid, "function creep," or the gradual widening of the use of personal information beyond the purpose for which it was originally intended.

A use or disclosure is necessary for performing the statutory duties of, or for operating a program of, the public body if the public body would be unable to carry out its program without using or disclosing the personal information in the way proposed. Where a public body is carrying out a statutory duty or legally authorized program and the use of personal information is necessary for that purpose, this may be considered a consistent purpose and therefore authorized under section 66.[7]

A consistent use or disclosure must meet both of the above conditions to be valid.

If you are unsure if a purpose can be considered a ***consistent purpose***, please consult your departmental solicitor.

4.1.2 With the Consent of the Individual (paragraph 66(1)(b))

A public body can use the personal information of an individual where the individual has identified the information and has consented to its use, pursuant to paragraph 66(1)(b).

Any consent by an individual to a proposed new use must be an informed consent. The individual should be informed of:

- the nature of personal information held by the public body about the individual which is proposed to be used;
- the proposed new use for the personal information; and
- the potential impact or consequences on the individual of his/her consent to the new use for the personal information.

If additional uses are anticipated at the time of collection, consent for the additional uses should be obtained at that time. Consent may, however, be requested later, if the new use is not proposed until after the original collection. For example:

> A public body compiles a mailing list containing names and home addresses for one of its programs. It then begins a new program and plans to use the same mailing list for this program. If the programs are unrelated, this use of the personal information is not consistent with the use for which the public

[7] *Report P-2009-002*, Newfoundland and Labrador Information and Privacy Commissioner

body originally collected it and the public body must get consent from each individual before including his/her personal information on the second mailing list.

4.1.2.1 Written Consent

Informed consent can be achieved either through written or verbal means. Written consent is the preferred method. Where written consent is being sought, notice should be provided in writing and include a description of the personal information being held, the proposed new use and the potential impact on the individual as a result of his/her consent to the new use.

4.1.2.2 Verbal Consent

There may be instances where written consent is either difficult to obtain or timeliness is an issue and verbal consent is the more expeditious option. In such a situation, verbal consent may be the better or only option. Where verbal consent is being sought, the individual should be contacted and provided with a description of the personal information being held, the proposed new use and the potential impact on the individual as a result of his/her consent to the new use. The individual should be directly asked if he or she understands this notice and whether or not he or she consents to the new use. A note should be made on the individual's file indicating the contents of the conversation, the date and time of the conversation and who spoke with the individual.

4.1.2.3 Privacy Notices

Given the difficulties with obtaining consent for alternative uses, the focus should be on creating complete privacy notices during the collection process. If possible, specific alternative uses of the personal information should be identified during the collection process, such as sharing information with other public bodies, and individuals would be provided with the opportunity to consent to those uses.

Public bodies should not use consent language that is broad, or captures extensive amounts of information across unspecified programs uses. That is, public bodies should not use language in privacy notices that results in clients agreeing to uses of their information that have not yet been decided upon. As an example, "any/all uses that the Department sees fit" should not be included on a consent form.

4.1.3 Use Consistent with Sections 68-71 (paragraph 66(1)(c))

Public bodies are permitted to use personal information that may be disclosed under sections 68, 69, 70 and 71 of the *Act*. These sections set out the circumstances where

public bodies may disclose personal information. Examples of disclosure under these sections include, but are not limited to, instances where information can be disclosed:

- for statistical purposes (s.70);
- for archival purposes (s.71); and
- to the Auditor General (s.68(1)(j)).

Paragraph 66(1)(c) allows public bodies to use the information disclosed in accordance with these sections. For a detailed description of the disclosure requirements within the *Act,* please see section 68 ("***Disclosure of Personal Information***").

4.1.4 Minimum Amount of Information to be Used (subsection 66(2))

Public bodies are required to ensure that their use of personal information is limited to the minimum amount of information necessary to accomplish its intended purpose.

> For example, if only the name and telephone number of a person is required for a program, then address and social insurance number should not be collected.

Further, access to and use of personal information by employees or agents of the public body must be limited to those who need to know the information to carry out the purpose for which the information was collected or to carry out a purpose authorized under section 66.

4.2 Use by Post-Secondary Institutions (section 67)

Section 67 sets out certain circumstances in which a post-secondary institution is permitted to use personal information in its alumni records for the purpose of its own fundraising activities.

In order to use alumni records for fundraising purposes, the personal information contained in the records must be "reasonably necessary" for the fundraising activities (subsection 67(1)).

Subsection 67(2) also requires a post-secondary institution to take the following steps in using alumni records for fundraising:

- When the individual to whom the personal information relates is first contacted for fundraising purposes, the institution must give them notice of their right to request that their personal information cease being used for fundraising purposes;

- The institution must periodically (and in the course of soliciting funds) give notice to the individual to whom the personal information relates of their right to request that their information cease being used for fundraising purposes; and

- The institution must, periodically and in a manner that is likely to come to the attention of individuals who may be solicited for funds, publish a notice of the right to request that personal information cease being used for fundraising purposes in an alumni magazine or other publication.

Where an individual requests that their personal information stop being used for fundraising, the post-secondary institution is required to comply with that request (subsection 67(3)).

Finally, any use of personal information in alumni records for fundraising purposes must be limited to the minimum amount necessary to accomplish the purpose (subsection 67(4)).

CHAPTER 5: DISCLOSURE OF PERSONAL INFORMATION

5.1 Public Body May Disclose Personal Information (section 68)

Section 68 lists the circumstances under which public bodies may disclose personal information:

68(1) A public body may disclose personal information only

(a) in accordance with Part II;

(b) where the individual the information is about has identified the information and consented to the disclosure in the manner set by the minister responsible for this Act;

(c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in section 69;

(d) for the purpose of complying with an Act or regulation of, or with a treaty, arrangement or agreement made under an Act or regulation of the province or Canada;

(e) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information;

(f) to an officer or employee of the public body or to a minister, where the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister;

(g) to the Attorney General for use in civil proceedings involving the government;

(h) for the purpose of enforcing a legal right the government of the province or a public body has against a person;

(i) for the purpose of

i) collecting a debt or fine owing by the individual the information is about to the government of the province or to a public body, or

ii) making a payment owing by the government of the province or by a public body to the individual the information is about;

(j) to the Auditor General or another person or body prescribed in the regulations for audit purposes;

(k) to a member of the House of Assembly who has been requested by the individual the information is about to assist in resolving a problem;

(l) to a representative of a bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry;

(m) to the Provincial Archives of Newfoundland and Labrador, or the archives of a public body, for archival purposes;

(n) to a public body or a law enforcement agency in Canada to assist in an investigation

i) undertaken with a view to a law enforcement proceeding, or

ii) from which a law enforcement proceeding is likely to result;

(o) where the public body is a law enforcement agency and the information is disclosed

i) to another law enforcement agency in Canada, or

ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;

(p) where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is given in the form appropriate in the circumstances to the individual the information is about;

(q) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted;

(r) in accordance with an Act of the province or Canada that authorizes or requires the disclosure;

(s) in accordance with sections 70 and 71;

(t) where the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 40;

(u) to an officer or employee of a public body or to a minister, where the information is necessary for the delivery of a common or integrated

program or service and for the performance of the duties of the officer or employee or minister to whom the information is disclosed; or

(v) to the surviving spouse or relative of a deceased individual where, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy.

(2) The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.

If a disclosure cannot be justified by this section, the personal information should not be released. Please note that the term ***disclosure*** includes disclosure of personal information to another public body. A "public body" includes another government department, a government agency, a post-secondary institution, health board, school board and municipality.

Section 68 permits disclosure; it does not require disclosure. Public bodies should consider the circumstances surrounding each request and the privacy protection objectives of the *Act* when deciding whether to disclose personal information.

5.1.1 Disclosure in Accordance with Part II (paragraph 68(1)(a))

Paragraph 68(1)(a) authorizes public bodies to disclose personal information where necessary to respond to requests for access to information or for the correction of personal information, and comply with public interest disclosure provisions in Part II of the *Act*.

For more information on responding to requests for access to information, please refer to the Access to Information Policy and Procedures Manual.

5.1.2 Disclosure with Consent of the Individual (paragraph 68(1)(b))

Paragraph 68(1)(b) permits disclosure of personal information when the individual to whom the information relates has identified the information and consented to the disclosure.

Where an individual has not provided consent to disclose their personal information and where no other provision exists to permit the disclosure, public bodies cannot disclose the information.

Consent should be clear and specific and the public body should be satisfied that:

- the consent is voluntary; and
- the consent is informed.

Informed consent means that the individual understands the effects and the consequences of the consent.

Where possible, an individual's consent should be in writing. If consent is given verbally, the public body should make a written record of the conversation and where appropriate, send a letter to the individual confirming the consent.

The individual's consent should include:

- a description of the personal information to be disclosed;
- the purpose of the disclosure;
- the recipient(s) of the disclosed information;
- the date of the consent and the period of time during which the consent remains valid; and
- the public body to which the consent is being given.

Where a public body anticipates disclosing personal information, they should seek consent to disclose at the time the personal information is collected. Where the disclosure is not anticipated, consent may be obtained at a later time, provided it is obtained before the proposed disclosure.

Generally, when seeking consent of an individual under paragraph 68(1)(b), best practice would be to notify that individual to whom their personal information may be disclosed and how that information may be used. For further information relating to consent, refer to Chapter 3 of the manual, "Consent."

5.1.3 Disclosure for Original or Consistent Purpose (paragraph 68(1)(c))

Paragraph 68(1)(c) permits a public body to disclose personal information for the purpose for which it was obtained or compiled or for a use consistent with that purpose.

The ***purpose*** means the reason for which personal information was originally collected under section 61. A public body is authorized to disclose personal information for that purpose.

Compiled refers to when certain information is created by a public body and is associated with an identifiable individual. For example, a public body assigns a unique number to an individual. This information has been compiled by the public body and is tied to that individual but was not collected from the individual.

As discussed in section 4.1.1 of this Manual, ***consistent purpose*** is defined in section 69 of the *Act*. A use is consistent with the purpose for which the information was obtained where there is a reasonable and direct connection to the original purpose **and** it is necessary for

performing the statutory duties of or for operating a legally authorized program of the public body.

In order for a proposed new use to have ***a reasonable and direct connection*** to the original purpose, there must be some logical and plausible link to the original purpose. A use or disclosure is necessary for performing the statutory duties of, or for operating a program of, the public body if the public body would be unable to carry out its program without using or disclosing the personal information in the way proposed. A consistent use or disclosure must meet both of the above conditions to be valid.

5.1.4 Disclosure to Comply with an Act or Regulation (paragraph 68(1)(d))

Paragraph 68(1)(d) permits a public body to disclose personal information in order to comply with an Act or regulation of, or with a treaty, arrangement or agreement made under an Act or regulation of the province of Newfoundland and Labrador or Canada. This provision does not apply to the legislation of other provinces, territories or countries.

This provision means that a public body can disclose information where disclosure is required by either a provincial (i.e. Newfoundland and Labrador) or federal Act or by regulation, treaty, arrangement or agreement made under an Act or regulation. The disclosure may be expressly required by the Act, regulation, treaty, arrangement or agreement. Where disclosure is not expressly required, disclosure may still be authorized under paragraph 68(1)(d) where compliance with the Act, regulation, treaty, arrangement or agreement necessarily requires the disclosure.

An ***Act*** is a statute passed by the House of Assembly of Newfoundland and Labrador or by the Parliament of Canada.

A ***regulation*** is a law made under the authority of a statute by the Lieutenant-Governor of Newfoundland and Labrador, or the Governor General in Council for Canada, a minister, etc.

A ***treaty*** is a formally concluded and ratified agreement between or among two or more independent states.

An ***arrangement*** is a settlement of mutual relations or claims between parties.

An ***agreement*** is a mutual understanding, an arrangement between parties as to a course of action, a contract. An agreement is more precise than an arrangement and is usually, although not always, in writing.

Agreements concerning the disclosure of personal information by public bodies to other organizations should include:

- a description of the personal information to be collected and/or disclosed;

- the authority for collecting, using and/or disclosing personal information;
- the purposes for which the information is to be collected, used and/or disclosed, including a restriction on any subsequent uses as well as who will have access to the information;
- a statement of all safeguards (administrative, technical and physical) required to protect the confidentiality of the information;
- a statement specifying whether information received by a public body will be subject to the provisions of the *Act* or a comparable legislation;
- a statement that the disclosure of the personal information will cease if the recipient is discovered to be improperly disclosing the information collected from the public body; and
- the names, titles and signatures of the officials in all participating public bodies who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.

Public bodies should maintain a list of all agreements, arrangements and treaties under which they disclose personal information.

5.1.5 Disclosure to Comply with Subpoena, Warrant or Order (paragraph 68(1)(e))

Paragraph 68(1)(e) permits a public body to disclose personal information for the purpose of complying with a subpoena, warrant or order issued or made by a person or body with jurisdiction to compel the production of information.

A ***subpoena*** is a document issued requiring a person's attendance as a witness at a court proceeding or hearing. A subpoena will specify the time and place when the individual is required to testify on a matter. It may also require a person to disclose information.

A ***warrant*** is a judicial order to collect information. For the purposes of paragraph 68(1)(e), this refers to personal information.

An ***order*** is an authoritative command, direction or instruction to produce something. For the purposes of paragraph 68(1)(e), this refers to personal information.

The court or tribunal must have jurisdiction in Newfoundland and Labrador in order to require a public body to disclose personal information. Courts with jurisdiction in Newfoundland and Labrador include the Supreme Court of Canada, the Provincial Court of Newfoundland and Labrador, the Newfoundland and Labrador Court of Appeal, the

Newfoundland and Labrador Supreme Court Trial Division (General), and the Newfoundland and Labrador Supreme Court Trial Division (Family).

5.1.6 Disclosure to an Officer or Employee of the Public Body or to a Minister (paragraph 68(1)(f))

Paragraph 68(1)(f) permits a public body to disclose personal information to an officer or employee of the public body or to a minister, where the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister.

Employee is defined under paragraph 2(i). It includes a person retained under a contract to perform services for the public body.

5.1.7 Disclosure to the Attorney General (paragraph 68(1)(g))

Paragraph 68(1)(g) permits a public body to disclose personal information to the Attorney General for use in civil proceedings involving the government. In order to disclose personal information under this provision, the government must be a party to or involved in the civil proceedings relevant to the potential disclosure.

5.1.8 Disclosure for Enforcing a Legal Right of a Public Body against a Person (paragraph 68(1)(h))

Paragraph 68(1)(h) permits a public body to disclose personal information for the purpose of enforcing a legal right the government of the province or a public body has against a person.

In Alberta, the commissioner considered a case where the Workers' Compensation Board disclosed a complainant's personal information to the Appeals Commission for the Workers' Compensation Board, regarding an allegation of a reasonable apprehension of bias concerning the complainant. The complainant objected to the disclosure of personal information and also to the extent of personal information disclosed. The commissioner held that the Workers' Compensation Board was authorized to disclose the personal information for enforcing a legal right.[8]

[8] *Order F2005-002*, Information and Privacy Commissioner of Alberta

5.1.9 Disclosure to Collect a Debt Owing or Make a Payment (paragraph 68(1)(i))

Clause 68(1)(i)(i) permits a public body to disclose personal information for the purpose of collecting a debt or fine owing by the individual the information is about to the government of the province or to a public body.

Clause 68(1)(i)(ii) permits a public body to disclose personal information for the purpose of making a payment owing by the government of the province or by a public body to the individual the information is about.

A ***fine*** is a monetary punishment imposed on a person who has committed an offence, including an offence under a bylaw.

A ***debt*** is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

Documentation for disclosure under this provision should be in writing and specify:

- the nature of the information to be disclosed;
- the name of the public body, person or organization receiving the information;
- any other necessary identifying information, such as a case or file number;
- the purpose of the request, including a citation of the legal authority for collecting the fine or debt; and
- the name, title and business address of the official making the decision to disclose.

This provision enables public bodies to disclose personal information in order to collect a fine or debt owed to the Government of Newfoundland and Labrador or a public body, or to make a payment owed by the Government of Newfoundland and Labrador or a public body.

Paragraph 68(1)(i) does not permit information to be disclosed by a public body for the purpose of determining whether a fine, debt or a benefit is owed. This decision should be made before the information is disclosed.

The information disclosed should be the minimum needed to collect the debt.

5.1.10 Disclosure to the Auditor General for Audit Purposes (paragraph 68(1)(j))

Paragraph 68(1)(j) permits a public body to disclose personal information to the Auditor General or another person or body prescribed in the regulations for audit purposes.

The Auditor General is appointed by the Lieutenant-Governor in Council and confirmed by a resolution of the House of Assembly. The role of the Auditor General is to audit financial statements and other accountability documents, evaluate management practices and control systems, and determine compliance with legislative and other authorities.

5.1.11 Disclosure to a Member of the House of Assembly (paragraph 68(1)(k))

Paragraph 68(1)(k) permits disclosure of personal information to a Member of the House of Assembly (MHA) to assist the person concerned to resolve a problem. This includes helping an individual to provide information to a public body; inquiring about decisions or about a service or benefit; or correcting a mistake or misunderstanding.

A ***Member of the House of Assembly*** is a person elected as a representative of a constituency within the province of Newfoundland and Labrador to represent the interests of voters in that constituency in the House of Assembly.

This provision permits disclosure only to MHAs of Newfoundland and Labrador and only to assist the person concerned to resolve a problem. In practice, MHAs may designate their constituency assistants to act on their behalf in requesting personal information under paragraph 68(1)(k).

This provision does not permit the disclosure of personal information to federal Members of Parliament or municipal representatives. These representatives may, however, obtain personal information about an individual with the individual's consent.

The purpose of disclosure under paragraph 68(1)(k) must be to assist in resolving a problem. This includes helping an individual to provide information to a public body, inquiring about decisions or about a service or benefit or correcting a mistake or misunderstanding.

A public body employee who receives this type of request from an MHA may inquire about the purpose of the request in order to confirm that the disclosure is necessary to assist in resolving a problem. **It is important to note that verbal consent given to the MHA by the person seeking assistance is sufficient for disclosure under paragraph 68(1)(k).** Although not required by the *Act*, it is suggested that MHAs obtain written consent where practical. If written consent cannot be obtained, some record (e.g. a note to the file) should be kept for verbal requests and/or consent given. The inquiry and disclosure should be recorded in writing by the public body. Where inquiries and disclosure take place verbally, the transaction should be noted on the constituent's file. The ATIPP Office has developed a form that can be used by MHAs to annotate verbal consent and which can be filed by the public bodies to document requests [Schedule 1].

Subsection 114(2) of the *Act* provides a protection from liability for MHAs who disclose information obtained from a public body under paragraph 68(1)(k) while acting in good faith on behalf of an individual.

More information on general process for constituency assistants calling a government department on behalf of a constituent for an MHA can be found on the ATIPP website at www.atipp.gov.nl.ca.

5.1.12 Disclosure to a Representative of a Bargaining Agent (paragraph 68(1)(l))

Paragraph 68(1)(l) permits a public body to disclose personal information to a representative of a bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry.

Bargaining agent refers to a union or other organization that negotiates on behalf of workers with their employers for improvements in pay, hours, benefits, and other working conditions, and that works to protect the rights of employees.

The individual must sign and date a statement of authorization or representation clearly stating to whom the information may be disclosed and for what purpose. Disclosure is limited to personal information that is necessary for the purpose of making an inquiry. The representative may receive only that personal information that the employee has specifically authorized for release.

5.1.13 Disclosure to the Provincial Archives (paragraph 68(1)(m))

Paragraph 68(1)(m) permits a public body to disclose personal information to the Provincial Archives of Newfoundland and Labrador, or the archives of a public body, for archival purposes.

This provision does not permit disclosure to private archives such as those run by a private museum or historical society.

Section 71 governs the disclosure of personal information by the Provincial Archives of Newfoundland and Labrador or the archives of a public body (see section 5.4 of this manual, “Disclosure for Archival or Historical Purposes”).

5.1.14 Disclosure to Assist Law Enforcement (paragraph 68(1)(n))

Paragraph 68(1)(n) permits a public body to disclose personal information to a public body or a law enforcement agency in Canada to assist in an investigation:

- undertaken with a view to a law enforcement proceeding, or
- from which a law enforcement proceeding is likely to result.

Law enforcement is defined under paragraph 2(n) and is discussed in sections 2.2.2 and 2.3.2.8 of this manual, "Law Enforcement."

A ***law enforcement proceeding*** is a proceeding that leads or could lead to a penalty or sanction under a statute or regulation. Law enforcement proceedings may include formal court proceedings and proceedings of administrative tribunals. The penalty or sanction can be imposed by the public body conducting the proceeding or by another body, such as a court.

When disclosing personal information under paragraph 68(1)(n), the public body should satisfy itself that

- the requesting party is a public body within the meaning of paragraph 2(x) or is a law enforcement agency;
- there is a law enforcement investigation and that the investigation has been undertaken in contemplation of a law enforcement proceeding as defined in paragraph 2(n); and
- the requesting public body or law enforcement agency can provide the legal authority for the law enforcement activity.

Under clause 68(1)(n)(ii) the disclosure of personal information must be to assist an investigation from which **a *law enforcement proceeding is likely to result*.** When disclosure is contemplated before an actual law enforcement proceeding is under way, it must be probable that a law enforcement proceeding will go forward.

A request by a law enforcement agency for personal information should be in writing and should be retained by the public body in support of any subsequent disclosure of personal information to that agency.

5.1.15 Disclosure where Public Body is Law Enforcement Agency (paragraph 68(1)(o))

Paragraph 68(1)(o) permits a public body to disclose personal information where the public body is a law enforcement agency and the information is disclosed: (i) to another law

enforcement agency in Canada; or (ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.

5.1.16 Disclosure where Compelling Circumstances Exist Affecting an Individual's Health or Safety (paragraph 68(1)(p))

Paragraph 68(1)(p) permits a public body to disclose personal information where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is given in the form most appropriate in the circumstances to the individual the information is about.

This provision permits the disclosure of the personal information of *any individual*, not only an individual who endangers health or safety or an individual whose health or safety is endangered.

The head of a public body will have to consider all the circumstances and all the information in the public body's possession about an individual when making a decision. Past behaviour of the individual is one factor that may assist in decision-making.

5.1.17 Disclosure to Contact Next of Kin of Injured, Ill or Deceased Individual (paragraph 68(1)(q))

Paragraph 68(1)(q) permits a public body to disclose personal information so that the next of kin or a friend of an injured, ill or deceased individual may be contacted.

5.1.18 Disclosure where an Act Authorizes or Requires Disclosure (paragraph 68(1)(r))

Paragraph 68(1)(r) permits a public body to disclose personal information in accordance with an Act of the province of Newfoundland and Labrador or Canada that authorizes or requires the disclosure.

Before disclosing personal information under paragraph 68(1)(r) in response to a request, a public body should ask the body requesting the information to provide their legal authority for collecting the information. A public body requesting personal information from another body should provide the disclosing body with their legal authority for collecting the information.

5.1.19 Disclosure in Accordance with Sections 70 and 71 (paragraph 68(1)(s))

Paragraph 68(1)(s) permits a public body to disclose personal information in accordance with section 70 (*research purposes*) and section 71 (*archival or historical purposes*).

Section 70 provides a public body with the authority to disclose personal information for research purposes. See section 5.3 of the manual for information on section 70, "Disclosure for Research or Statistical Purposes."

Section 71 provides the Provincial Archives of Newfoundland and Labrador or the archives of a public body with the authority to disclose personal information for archival or historical purposes. See section 5.4 of the manual for information on section 71, "Disclosure for Archival or Historical Purposes."

5.1.20 Disclosure would not be an Unreasonable Invasion of a Third Party's Privacy (paragraph 68(1)(t))

Paragraph 68(1)(t) permits a public body to disclose personal information where the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 40.

See section 4.6.5 of the **Access to Information Policy and Procedures Manual** for a detailed overview of section 40.

5.1.21 Disclosure to a Public Body for Delivery of a Common or Integrated Program (paragraph 68(1)(u))

Paragraph 68(1)(u) permits a public body to disclose personal information to an officer or employee of a public body or to a minister, where the information is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or minister to whom the information is disclosed.

A ***common or integrated program or service*** means a single program or service that is provided or delivered by two or more public bodies or a program or service that has several distinct components, each of which may be provided or delivered by a separate public body, but which together constitute the program or service.

Factors that will determine whether or not a program or service is a **common or integrated program or service** include:

- evidence of joint planning;
- a formal agreement or legislative authority for working together;

- common goals expressed by the partners; and
- evidence of collaboration or cooperation in delivery.

When public bodies are implementing such programs or services, they should:

- disclose information in non-identifiable form whenever possible;
- ensure that individuals participating in the program are notified of all the partners and of the sharing of personal information, preferably at time of collection;
- disclose personal information only to those who need to know about a particular individual;
- disclose personal information only to the extent necessary for program or service delivery; and
- ensure that personal information is not used for any other purpose.

Public bodies that intend to create a common or integrated program or service should note section 72 with respect to the obligation to conduct a Privacy Impact Assessment, to notify the commissioner early in the process of the development of the program or service, and to submit any Privacy Impact Assessment conducted to the ATIPP Office to supply to the commissioner for review and comment. These obligations are discussed in section 1.2.1 of this Manual.

5.1.22 Disclosure to Surviving Spouse or Relative of a Deceased Individual (paragraph 68(1)(v))

Paragraph 68(1)(v) permits a public body to disclose personal information to the surviving spouse or relative of a deceased individual where, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy.

Factors to consider in determining whether disclosure of a deceased individual's personal information is an unreasonable invasion of their privacy include:

- the disclosure is desirable for the purpose of subjecting the activities of the Government of Newfoundland and Labrador or a public body to public scrutiny;
- the personal information is relevant to a fair determination of the requesting individual's rights;
- the personal information was originally supplied by the requesting individual;
- the personal information was supplied in confidence;

- disclosure may endanger the physical or mental well-being of any other living member of the family;
- there are grounds to believe that another member of the family does not want the information disclosed to the relative;
- the personal information is likely to be inaccurate or unreliable;
- the information contains medical, psychological or social work case reports or data which it is reasonable to believe would prove harmful to family relationships;
- disclosure may harm the reputation of the deceased; and
- the length of time the person has been deceased.

5.1.23 Minimum Amount of Information to be Disclosed (subsection 68(2))

> *68(2) The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it was disclosed.*

Briefly, this means disclose only what you need to in order to accomplish the specific task.

For example, in responding to a subpoena, warrant or other order, the public body should provide only the personal information specifically requested in the subpoena, warrant or order. Additionally, if a public body receives a court order to release a person's address to law enforcement officials, the public body should not release the person's telephone number or health status. Where the subpoena, warrant or order is unclear, public bodies should consult their legal counsel.

5.2 Definition of Consistent Purposes (section 69)

> *69 A use of personal information is consistent under section 66 or 68 with the purposes for which the information was obtained or compiled where the use*
>
> *(a) has a reasonable and direct connection to that purpose; and*
>
> *(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.*

Sections 66 and 68 state that disclosures are permitted if they are consistent with the original purpose for which the personal information was collected.

Public bodies should determine if the disclosure of personal information:

- has a reasonable and direct connection to the purposes for which it was obtained or compiled; and

- is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

If it cannot be determined that both criteria listed above have been met, the disclosure must be justified under paragraphs 66(1)(b) or (c). This will often mean seeking the consent of the individual the information is about before proceeding with the intended disclosure.

As discussed in section 4.1.1 of this Manual, in order for a proposed new use to have **a reasonable and direct connection** to the original purpose, there must be some logical and plausible link to the original purpose. A use or disclosure is necessary for performing the statutory duties of, or for operating a program of, the public body if the public body would be unable to carry out its program without using or disclosing the personal information in the way proposed. A consistent use or disclosure must meet both of the above conditions to be valid.

5.3 Disclosure for Research or Statistical Purposes (section 70)

Section 70 permits, but does not require, a public body to disclose personal information for a purpose related to research, providing four conditions have been met:

> *70 A public body may disclose personal information for research purposes, including statistical research, only where*
>
> *(a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form;*
>
> *(b) any record linkage is not harmful to the individuals that information is about and the benefits to be derived from the record linkage are clearly in the public interest;*
>
> *(c) the head of the public body concerned has approved conditions relating to the following:*
>
> *(i) security and confidentiality,*
>
> *(ii) the removal or destruction of individual identifiers at the earliest reasonable time, and*

(iii) the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of that public body; and

(d) the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and the public body's policies and procedures relating to the confidentiality of personal information.

A ***research purpose*** means for the purpose of a systematic investigation or study of materials or sources in order to establish facts or to verify theories.

Statistical research is research based on the collection and analysis of numerical data using, in this case, quantifiable personal information to study trends and draw conclusions.

5.3.1 Individually Identifiable Information (paragraph 70(a))

Paragraph 70(a) permits a public body to disclose personal information for a research purpose, including statistical research, where the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form.

Information is ***individually identifiable*** where unique identifiers are attached to the information such that the information can identify a particular individual. Such identifiers might include an individual's name, address, telephone number, date of birth or social insurance number. In areas with a smaller population, other types of information may also allow for the identification of an individual.

A public body may disclose personal information to assist with research. This need arises when the nature of the research itself, or the records involved, makes it unfeasible to conduct the research without information that identifies individuals.

5.3.2 Record Linkage (paragraph 70(b))

Paragraph 70(b) provides limits on linking of records during a research project with respect to disclosure of personal information for a research purpose.

Record linkage is a form of data matching involving the systematic comparison of sets of information, often personal, to establish relationships among data. Within the research context, it often involves the creation of a new database allowing the statistical correlation of research variables. Record linkage can be a useful tool for quantitative analysis in research projects.

Record linkage for research purposes is the matching of sets of personal information to achieve the objectives of the research project, generally with no intention of making

decisions about the research subjects' rights or privileges. The matching is a means of linking the right information to the right people in a representative sample used in a study. This makes it distinct from the kind of record linkage for individual profiling that is used in some marketing strategies, for example.

This provision requires that any record ***linkage must not be harmful*** to the individual the information is about. In addition to the harm test, this provision inversely sets out that there must be ***benefits to be derived from the record linkage***. Therefore, the benefits must outweigh the privacy concerns with respect to any disclosure of personal information to a researcher.

5.3.3 Approval of Conditions (paragraph 70(c))

Paragraph 70(c) sets out conditions which the public body must approve in order to permit disclosure of personal information for research purposes.

Specifically, it requires the head of a public body to approve the following conditions:

- security and confidentiality;
- the removal or destruction of individual identifiers at the earliest reasonable time; and
- prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of that public body.

5.3.4 Agreement to Comply (paragraph 70(d))

Paragraph 70(d) requires that where personal information is to be disclosed for research purposes, the person to whom that information is disclosed must sign an agreement to comply with the approved conditions, the *Act* and the public body's policies and procedures relating to the confidentiality of personal information.

The public body has the **final** responsibility for administering and approving research agreements. Before releasing any information, there should be a written agreement between the public body and the researcher. The public body should be satisfied that:

- access privileges are only used for the purpose(s) stated in the agreement and are not used as a means to browse records;
- the researcher will not disclose or share personal information with any other party, except as set out in the agreement;
- the researcher will destroy any personal identifiers as soon as possible;

- the researcher will not use personal information for any purpose other than the purpose set out in the agreement; and

- there are appropriate security measures in place to protect personal information.

The public body should confirm and document that the applicant requires access to records containing personal information in individually identifiable form in order to achieve the research purpose. The personal information must be directly related to the research – this may occur where the applicant needs to see the information in personally identifiable form for their research but does not need to provide the results or analysis of their research in a personally identifiable form.

The researcher must sign a detailed research agreement that describes the nature of the research; type of personal information that will be disclosed; how it will be used; any terms and conditions for the disclosure; and the procedural safeguards that the researcher will use for its protection. Only the researcher or an authorized agent of the researcher may sign a research agreement. Research agreements should not be ongoing or open-ended, but may be renewed as required.

Some provisions to consider including in a research agreement include:

- personal information disclosed can be used only for a research purpose set out in the agreement or for which written authorization has been given by the public body;

- the names of those persons who will be given access to the personal information must be provided;

- the researcher must bind these persons, through an agreement, to adhere to the same conditions as the researcher;

- information must be kept in a secure location;

- how and when the identifiers will be removed or destroyed must be specified;

- contact with the individuals to whom the information relates is prohibited without prior written authorization from the public body;

- no use or disclosure can be made of the information in a form that identifies individuals without prior written authorization from the public body;

- information cannot be used for an administrative purpose directly affecting an individual;

- notification of the public body is required if any conditions of the agreement or any provisions of the *Act* are breached; and

- failure to meet the conditions may result in cancellation of the agreement.

The public body may want to add audit provisions to the agreement so that the security and confidentiality measures of the researcher can be reviewed.

5.4 Disclosure for Archival or Historical Purposes (section 71)

Section 71 sets out the circumstances under which the Provincial Archives of Newfoundland and Labrador or the archives of a public body may disclose personal information.

> *71 The Provincial Archives of Newfoundland and Labrador, or the archives of a public body, may disclose personal information for archival or historical purposes where*
>
> *(a) the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 40;*
>
> *(b) the disclosure is for historical research and is in accordance with section 70;*
>
> *(c) the information is about an individual who has been dead for 20 years or more; or*
>
> *(d) the information is in a record that has been in existence for 50 years or more.*

This section recognizes the unique challenges faced by the Provincial Archives or the archives of a public body in complying with both the access and privacy components of the *Act.* Many of these records contain very sensitive information. Section 71 provides four circumstances under which an archive may disclose personal information.

CHAPTER 6: REQUESTING ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

Under the *Act*, individuals have the right to access their personal information which is in the custody or control of a public body.

In order to facilitate an individual's access to his/her personal information, the public body should:

- Develop ATIPP-compliant forms and procedures to assist individuals in filing requests to access their personal information. Public bodies should offer privacy training to ensure that their employees are familiar with the forms and processes needed to file a request for access to personal information;

- Protect personal information, when a request for access is received, by determining who is authorized to access an individual's personal information and then releasing or withholding that information accordingly;

- Ensure that employees recognize that some information can be shared informally; and

- Ensure that public body employees adhere to the spirit of section 13 of the *Act*, "***Duty to Assist Applicant***." The employee shall assist the applicant by:

    - being aware that there is no fee or cost where an applicant requests access to their own personal information;

    - answering requests in a timely manner, as prescribed by the legislation;

    - organizing the information (including page numbers, etc.) before the information is released;

    - releasing information in the format requested by the applicant, if possible; and

    - explaining redactions, codes and acronyms so that the applicant is able to understand the information.

Where a request for access to personal information is made, Part III of the *Act* does not come into play. Part III governs the actions of public bodies themselves in how they collect, use and disclose personal information in the course of their administrative operations.[9]

[9] *Report A-2008-003*, Information and Privacy Commissioner of Newfoundland and Labrador

For more information on requesting access to personal information, see the Access to Information Policy and Procedures Manual.

The right to correct personal information found in the *Act* is one way to ensure that an individual's personal information is as accurate as possible.

To ensure that individuals have the ability to correct personal information, public bodies should:

- identify the information that needs to be corrected and contact the individual in order to correct the information;
- assist individuals when they are providing information to the public body;
- identify the individual or authorized person before they correct the personal information in their custody or control;
- place all documentation that accompanied the request for correction in the applicant's file;
- render a decision on whether or not to correct an individual's personal information in a timely manner, as prescribed by the *Act*;
- if the information is corrected, send the new information to all parties who were provided with the information during the one year period before the correction was requested; and
- inform the applicant that they have the right to have the public body's decision on whether or not to correct the applicant's personal information reviewed by the Office of the Information and Privacy Commissioner or the Supreme Court, Trial Division.

6.1 Right to Request Correction of Personal Information (section 10 and section 18)

Section 10 gives individuals the right to ask a public body to correct their personal information where it is inaccurate or to provide additional information where it is incomplete.

> *10(1) An individual who believes there is an error or omission in his or her personal information may request the head of the public body that has the information in its custody or under its control to correct the information.*
>
> *(2) A cost shall not be charged for a request for correction of personal information or for a service in response to that request.*

An ***error*** is mistaken or wrong information or information that does not reflect the true state of affairs.

An ***omission*** is information that is incomplete or missing or that has been overlooked.

Section 18 sets out how a public body is supposed to respond to a request for correction of personal information.

> *18(1) In a final response to a request for correction of personal information, the head of a public body shall inform the applicant in writing*
>
> *(a) whether the requested correction has been made; and*
>
> *(b) if the request is refused,*
>
> *(i) the reasons for the refusal;*
>
> *(ii) that the record has been annotated; and*
>
> *(iii) that the applicant may file a complaint with the commissioner under section 42 or appeal directly to the Trial Division under section 52, and advise the applicant of the applicable time limits and how to file a complaint or pursue an appeal.*
>
> *(2) Where no correction is made in response to a request, the head of the public body shall annotate the information with the correction that was requested but not made.*
>
> *(3) Where personal information is corrected or annotated under this section, the head of the public body shall notify a public body or a third party to whom that information has been disclosed during the one year period before the correction was requested.*
>
> *(4) Where a public body is notified under subsection (3) of a correction or annotation of personal information, the public body shall make the correction or annotation on a record of that information in its custody or under its control.*

6.1.1 Requests for Correction (section 11)

Section 11 of the *Act* applies to both requests for access and requests for correction of personal information. As such, a request for correction must be made to the public body that the person believes has custody or control of the personal information, and must:

- be in the form set by the Minister responsible for the *Act*; and
- provide sufficient details about the information to be corrected so that an employee of the public body can identify and locate it with reasonable efforts.

An individual may make a request for correction of personal information orally where they have a limited ability to read or write in English or have a disability or condition that impairs their ability to make a request (subsection 11(3)).

Requests for correction of personal information can also be submitted electronically (subsection 11(4)).

6.1.2 Making a Correction or Annotation

Section 10 requires public bodies to make corrections to an individual's personal information if the individual can demonstrate it is inaccurate or incomplete. Even if no correction or addition is made, the record must be annotated.

Not all requests for correction of personal information need to be, or should be, made under section 10. This section does not replace existing procedures under which an individual can request correction of personal information in a record; nor does section 10 prevent a public body from correcting personal information that is clearly incorrect or out of date.

6.1.3 Requests for Correction of Factual Information

When a request for factual correction is received, the public body should assess the request. If the applicant gives adequate proof that the information held by the public body is incorrect or incomplete, a correction should be made. Where proof is inadequate, the record should be annotated.

Where the public body determines a correction should be made, the public body should correct the record by clearly marking the original information as incorrect and attaching the correct information to the records.

Where the personal information is incomplete, the public body should add the additional information, provided there is adequate proof. Where there is inadequate proof to make a correction, the public body must annotate the information. This can be done by adding

explanatory notes, letters, reports or other information to the file. For example, an annotation may consist of a letter or written statement in which the applicant disputes the facts as presented or disagrees with an opinion previously expressed by the applicant or another person about the applicant.

Section 10 provides an individual with the right to *request* a correction of their personal information.

6.1.4 Request for Correction of Opinion Information

Sometimes information in a record is based on opinion. For example, a record may contain an assessment of a person's abilities, performance or other characteristics. Because opinions are subjective, they usually cannot be corrected. In these circumstances, public bodies must annotate the record with a statement that the applicant does not agree with the opinion previously given. If the opinion is based on inaccurate or incorrect information and the information is used to make a decision affecting the individual, the public body should ask the person who supplied the opinion to provide an amended opinion.

6.1.5 Include Correction or Annotation with Original File

Whenever a correction or an annotation is made, the file should be set up so that the correction or annotation will always be retrieved when the original file is retrieved.

6.1.6 Refusal to Correct Information (subsections 18(1)(b) and 18(2))

Paragraph 18(1)(b) requires that where a public body refuses to make a requested correction, the head of the public body must inform the applicant, in writing, of the following:

- the reasons for the refusal;
- that the record has been annotated; and
- that the applicant can make a complaint to the commissioner or file an appeal directly to the Trial Division, together with the time limits and procedures for making a complaint or filing an appeal.

Under subsection 18(2), where no correction is made in response to a request, the public body must annotate the information with the correction that was requested but not made.

Under subsection 42(2), an applicant has **15 business days** from the date they are notified of a public body's decision to make a complaint to the commissioner in relation to a request for correction. The same time period applies to appeals to the Trial Division under

subsection 52(2). It should be noted that where the individual appeals a decision on a request for correction directly to the Trial Division, they are not permitted to file a complaint with the commissioner as well (subsection 42(6)).

6.1.7 Duty to Inform other Public Bodies or Organizations (subsection 18(3))

If a correction or annotation is made, the public body should determine if any other public bodies or third parties have received the information in the past year, as set out in subsection 18(3). If so, the public body should inform the public bodies or third parties about the correction or annotation. The one-year period runs from the date the correction was requested.

Where a public body receives information about a correction or annotation, it is required to make the correction on their own files as well (subsection 18(4)). Individuals or organizations not covered by the *Act* cannot be compelled to correct/annotate their records but they must be notified by the public body.

As normal practice, a record should be kept on all disclosures of personal information provided to other public bodies and third parties, enabling subsequent notification of a correction or annotation to the record.

6.1.8 Correction by Other Public Body (subsection 18(4))

Subsection 18(4) requires that where a public body is notified under subsection 18(3) of a correction or annotation of personal information, the public body shall make the correction or annotation on a record of that information in its custody or under its control.

6.1.9 Timing for Making a Decision about a Correction or Annotation (section 16)

Section 16 of the *Act* requires the head of the public body to respond to a request for correction of personal information without delay and, in any event, not later than **20 business days** after receiving it, unless the time limit is extended under section 23. Where the head of the public body does not respond within the 20 business day period (or an extended period), the head is considered to have refused the request for correction. The applicant's rights to make a complaint to the commissioner or appeal to the Trial Division are triggered upon this deemed refusal.

Business day is defined in paragraph 2(b) as a day that is not a Saturday, Sunday or a holiday.

Where the head of a public body is of the view that more time is needed to respond to a request for correction, he or she may, within 15 business days of receiving the request, make an application to the commissioner for an extension under section 23. The commissioner may approve an extension where the commissioner considers it necessary and reasonable to do so in the circumstances, for the number of business days the commissioner feels is appropriate. The commissioner is required to approve or disapprove an application for an extension of time within 3 business days of receiving it (subsection 23(3)). **Public bodies should note that the time required to make an application and receive a decision from the commissioner does not suspend the 20 business day period within which they must respond to the request for correction (subsection 23(4)).**

Where the commissioner grants an extension, the head of the public body must notify the applicant in writing of the reason for the extension, that the commissioner authorized it, and the date upon which a response can be expected.

CHAPTER 7: RETENTION OF PERSONAL INFORMATION

7.1 Retain Personal Information where Used to Make Decision Affecting Individual (section 65)

Section 65 requires public bodies to keep personal information for at least one year when it is used to make a decision that directly affects an individual. This provides individuals with a reasonable opportunity to access their personal information, and request corrections, where applicable. It is important to note that the year runs from the date the information was last used, not when it was initially collected.

If an individual's personal information is used to make a decision, public bodies should place a note on file indicating the:

- details of the decision; and
- date the decision was made.

A ***decision that directly affects the individual*** is one that has an impact on an individual's life or affects his or her rights. The meaning of the term is interpreted broadly and includes decision-making processes that are internal to a public body and those which involve a more direct relationship with the public.

It is important to remember that records may hold administrative, legal, financial or archival value to a public body that requires information to be retained for longer than one year. It is the responsibility of each public body to determine how long records in their custody and/or control need to be retained.

Examples of decisions that directly affect individuals include a determination of whether someone is eligible for a government program or a decision relating to hiring an individual.

Where no decision is made about an individual, section 65 does not apply. Examples of this include receipt of an unsolicited résumé which is never considered in relation to a position or personal information collected for a survey where the results are rendered anonymous.

Subsection 65(2) also requires a public body that has custody or control of personal information that is the subject of a request for access or correction under Part II of the *Act* to retain that information for as long as necessary to allow the requester to exhaust any recourse under the *Act* that he or she may have in relation to the request.

Disposal of records containing personal information should occur in accordance with approved records retention and disposal schedules. For additional information related to the management and disposal of government records, see the *Management of Information Act* and *The Rooms Act*.

CHAPTER 8: PROTECTION OF PERSONAL INFORMATION

8.1 Protect Personal Information in Custody/Control of Public Body (section 64)

Subsection 64(1) states that a public body shall take steps that are reasonable in the circumstances to ensure that:

- Personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;
- Records containing personal information in its custody or control are protected against unauthorized copying or modification; and
- Records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.

Disposed of in a secure manner does not include the destruction of a record of personal information unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances (subsection 64(2)).

When implementing these reasonable steps to protect personal information, a public body must consider:

- the sensitivity of the information being protected;
- the potential harm of unauthorized access; and
- the format in which the information is stored, or could be transferred or transmitted (e.g. paper, usb drive, shared drive, etc.).

In order to make reasonable security arrangements, a public body must consider administrative, physical and technical safeguards.

The Information and Privacy Commissioner of British Columbia commented on what is considered ***reasonable*** for the purposes of security of personal information:

> "The reasonableness of security measure and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances."[10]

[10] *Investigation Report F06-01*, Information and Privacy Commissioner of British Columbia

Four factors to consider when determining whether a public body has instituted reasonable security measures include:

(a) the foreseeability of the privacy breach;

(b) the seriousness of potential harm;

(c) the cost of preventative measures; and

(d) relevant standards of practice.[11]

The Information and Privacy Commissioner of Alberta has stated that "an organization need not implement each and every available security measure. However, it is well established that simple log-on passwords and employee watchfulness is insufficient. Organizations should apply multiple layers and measures that give personal information adequate protection."[12]

Use of social media websites by public bodies for the purpose of communicating personal information to individuals is discouraged as there is no way to ensure that any personal information communicated on such sites is protected.[13]

8.1.1 Administrative Safeguards

Administrative safeguards provide a framework for operating and managing the work environment and should be formalized in written policies and procedures which:

- are relevant and up to date;
- deal with security, records management and information management; and
- make administrative roles and responsibilities well-defined and easy to follow.

Examples of administrative safeguards that should be included in these policies, procedures and practices are:

- ensuring organized and secure management of records containing personal information;
- limiting access to records containing personal information to authorized employees and agents who need to know this information to carry out their duties;
- ensuring that former employees turn in their employee IDs, that their access rights have been revoked and any employer-issued technology has been returned;

[11] *Report P-2008-002*, Information and Privacy Commissioner of Newfoundland and Labrador
[12] *Investigation Report F2006-IR-005*, Information and Privacy Commissioner of Alberta
[13] *Report P-2012-001*, Information and Privacy Commissioner of Newfoundland and Labrador

- training employees on privacy, safeguards and security of personal information and consequences of non-compliance;
- incorporating file check-out procedures for records containing personal information;
- outlining procedures to identify sensitive personal information and ensure secure transfer and use of that information (e.g. only transmitting sensitive personal information in a manner that ensures it will be received by the intended recipient take preventative measures to protected against interception);
- managing and auditing employee access to records containing personal information; and
- verifying an individual's identity when requesting personal information.

8.1.2 Physical Safeguards

Physical safeguards monitor and control the work environment. Most of these can be incorporated into every employee's work routine. Examples of physical safeguards include:

- storing personal information in locked filing cabinets, offices and buildings, with controls over distribution of the keys or lock combinations;
- storing personal information in secure areas where access is limited or restricted;
- logging out of or locking computers when stepping away from the work area;
- ensuring that government assets, such as laptop computers, are secured when they are out of the office and are encrypted (e.g. not left in vehicles);
- not leaving documents containing personal information on printers or fax machines;
- always using a cover sheet when faxing personal information;
- calling before sending a fax to make sure the intended recipient is able to retrieve it;
- making sure the right email address has been entered prior to sending an email;
- encrypting emails containing personal information prior to sending;
- when replying to long email threads remove any recipients who no longer need to be involved before replying;
- limiting the amount of personal information provided in emails to that which is necessary (e.g. if everyone you are emailing knows the name of the individual being discussed do not include the individual's name in the email);
- shredding any documents containing personal information prior to disposal;

- labeling files containing personal information as a reminder to store them securely; and

- card access systems, video surveillance and security guards.

8.1.3 Technical Safeguards

Technical safeguards monitor and control access to information and computer systems. Examples of security and technical safeguards include:

- role-based access controls and strong password protection to determine user authentication and authorization;

- audit features and access logs to track system access and use;

- disable infrared ports on laptops which may allow others to browse files on a laptop at a distance without touching it;

- data encryption of personal information during file transfers;

- data encryption of personal information stored on laptops and removable media devices;

- back up of files containing personal information; and

- network security protection and monitoring (e.g. firewalls, network intrusion detection).

8.1.4 Notification of Individuals

Subsections 64(3) to (9) of the *Act* provide for the mandatory notification of individuals where personal information is stolen, lost, disposed of in an inappropriate manner, or disclosed to or accessed by an unauthorized person. For more information on this requirement, see section 9.4 of this manual.

CHAPTER 9: PRIVACY BREACHES

Public bodies should make every effort to prevent privacy breaches from occurring. They should also be aware of the steps to be taken when a breach occurs. While the *Act* provides guidance in terms of a public body's obligations to protect personal information, it also requires that steps be taken once a privacy breach occurs.

The *Act* requires that affected individuals be notified where a privacy breach results in the risk of significant harm, and that the Office of the Information and Privacy Commissioner be notified of all privacy breaches.

For a summary of the steps involved in responding to a privacy breach, please see **Appendix B: Privacy Breach Protocol.**

9.1 What is a Privacy Breach?

A ***privacy breach*** occurs when there is an unauthorized collection, use, disclosure or disposal of personal information. Such activity is unauthorized if it occurs in contravention of the *Act*. The most common privacy breach happens when personal information of individuals or employees is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information is stolen or when personal information is mistakenly mailed to the wrong person.

9.2 Consequences of a Privacy Breach

Privacy breaches can cause significant harm to individuals, including:

- identity theft;
- compromising personal safety; and/or
- embarrassment or humiliation due to an individual's personal information being disclosed.

There are also consequences for the public body and its employees, including:

- the Information and Privacy Commissioner may investigate and make recommendations with respect to complaints about a potential breach;
- the Department may suffer damage to its reputation as a result of the breach;
- the Department may be obliged to devote time and resources to correct the breach; and/or
- if the breach is found to be willful, the person responsible could face a fine of $10,000 and/or a jail term of up to six months.

Section 115 is the offence provision of the Act. It is an offence to:

- willfully collect, use or disclose personal information in contravention of the *Act* or regulations;
- willfully attempt to gain or gain access to personal information in contravention of the *Act* or regulations;
- willfully make a false statement to, or mislead or attempt to mislead, the commissioner or another person performing duties or exercising powers under the *Act*;
- willfully obstruct the commissioner or another person performing duties or exercising powers under the *Act;*
- willfully destroy a record or erase information that is subject to the *Act*, or direct another person to do so, with the intent to evade a request for access; or
- willfully alter, falsify or conceal a record that is subject to the *Act*, or direct another person to do so, with the intent to evade a request for access.

9.3 Examples of a Privacy Breach

In late January 2008, computer records containing the personal information of clients of the Workplace Health, Safety and Compensation Commission (the "WHSCC"), including health information, were exposed over the Internet by an employee of a health care services provider as a result of installing a popular music-sharing program, Limewire, on a laptop that also contained client files. The service provider was under contract to the WHSCC.[14]

In 2004, the Government of Alberta outsourced the management of vehicle registries to a private company. In November of that year, prison guards asked the province to remove their home addresses from the automobile registries because at least six prison guards had received threats from gang members. One guard was told by a gang member that the registry databases had been infiltrated by insiders.[15]

In July 2005, the British Columbia Ministry of Labour sold a set of high capacity data tapes to a surplus computer equipment store. The tapes were purchased at a public auction for $101.00. The buyer turned the tapes over to a newspaper after realizing the tapes contained health and immigration records, including information on sexual abuse, HIV status and mental illness.[16]

[14] OIPC Privacy Report, P-2010-001, http://oipc.nl.ca/pdfs/P-2010-001_WHSCC.pdf
[15] "Prison Guards Protect Privacy Breach," website www.cbc.ca, November 15, 2004, www.cbc.ca/canada/edmonton/story/2004/11/15/ed prisonguards20051115.html
[16] "Health and Immigration Records sold at B.C. Auction," website www.cbc.ca, March 6, 2006, http://www.cbc.ca/news/canada/story/2006/03/06/bc-government-tapes060306.html

9.4 Four Key Steps in Responding to a Privacy Breach

The most important step you can take is to respond immediately to the breach. You should undertake steps 1, 2 and 3 below immediately following the breach and do so simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies.

Step 1: Contain the breach

You should take the following steps to limit the breach:

- Immediately contain the breach by stopping the unauthorized practice, recovering the records, shutting down the system that was breached or correcting weaknesses in physical security;

- Immediately contact your Executive, including your Minister and Deputy Minister and Director of Communications; as well as Cabinet Secretariat, where appropriate and your delegated Privacy Analyst in the ATIPP Office;

- Immediately retrieve the Privacy Breach Reporting Form, located at http://oipc.nl.ca/pdfs/PrivacyBreachIncidentReportForm.pdf. When the form is complete, submit it to the Office of the Information and Privacy Commissioner (breachreport@oipc.nl.ca) and the ATIPP Office (atippoffice@gov.nl.ca); and

- Work with your privacy/management team to provide appropriate notification as required under subsections 64(3)-(9) of the *Act* (discussed at Step 3 below) and outlined in the Privacy Breach Protocol, located at Appendix B.

Step 2: Evaluate the risks associated with the breach

To determine what other steps are necessary, you should assess the risks associated with the breach. Consider the following factors in assessing the risks:

1. **Personal information involved**

   (a) What data elements have been breached? In many cases, the risk of harm increases with an increase in the sensitivity of the data. Social insurance numbers and financial information that could be used for identity theft are examples of sensitive information.

   (b) Can the information be used for fraudulent or other harmful purposes?

2. **Cause and extent of the breach**

(a) What is the cause of the breach?

(b) Is there a risk of ongoing or further exposure of the information?

(c) What was the extent of the unauthorized collection, use or disclosure, including the number of likely affected individuals and the risk of further access, use or disclosure, including in the mass media or online?

(d) Is the information encrypted or otherwise not readily accessible?

(e) What steps have you already taken to minimize the harm?

3. Individuals affected by the breach

(a) How many individuals are affected by the breach?

(b) Who was affected by the breach? Employees, the public, contractors, individuals, service providers, or other organizations?

4. Foreseeable harm from the breach

(a) Is there any relationship between the unauthorized recipients and the data subject?

(b) What harm will come to the individuals because of the breach? Harm may include:

(i) Security risk, bodily harm (e.g. physical safety);

(ii) Damage to or loss of property;

(iii) Identity theft or fraud;

(iv) Loss of business, employment or professional opportunities;

(v) Financial loss;

(vi) Negative effects on credit record; and/or

(vii) Hurt, humiliation, or damage to reputation or relationships.

(c) What harm could result to the public body or organization because of the breach?

(i) loss of trust in the public body or organization;

(ii) loss of assets; and/or

(iii) financial exposure.

(d) What harm could result to the public because of the breach?

(i) risk to public health; and/or

(ii) risk to public safety.

Step 3: Notification

Subsection 64(3) **requires** the head of a public body that has custody or control of personal information to notify an individual where their personal information is:

- stolen;
- lost;
- disposed of, except as permitted by law; or
- disclosed to or accessed by an unauthorized person.

However, this notification requirement does **not** apply where the head of the public body reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access to personal information does not create a risk of significant harm to the affected individual(s) (subsection 64(7)).

Where a public body has received personal information from another public body for research purposes, the researcher must not notify individuals whose information has been stolen, lost, disposed of or disclosed/accessed unless the public body that disclosed the information to the researcher has first obtained the individual's consent to be contacted by the researcher (subsection 64(6)).

The key consideration in deciding whether notification to affected individuals required is whether or not the notification is necessary in order to avoid or mitigate "a risk of significant harm" to an individual whose personal information has been inappropriately collected, used or disclosed.

Review your risk assessment from Step 2 to determine if notification is required. To assist public bodies in determining when and how to notify affected individuals, refer to the Privacy Breach Protocol available on the ATIPP website at www.atipp.gov.nl.ca.

1. Notifying Affected Individuals

As noted above, a public body **must** notify affected individuals where it is necessary to avoid or mitigate "a risk of significant harm." ***Significant harm***, for the purpose of determining whether notification is necessary, is defined in subsection 64(8) and includes:

- bodily harm;
- humiliation;
- damage to reputation or relationships;
- loss of employment, business or professional opportunities;
- financial loss;
- identity theft;
- negative effects on the credit record; and
- damage to or loss of property.

Public bodies should also consider whether any contractual or legal obligations exist that require notification in the event of a breach.

Subsection 64(9) states that the factors relevant to determining whether a breach creates "a risk of significant harm" to an individual include:

- the sensitivity of the personal information; and
- the probability that the personal information has been, is being or will be misused.

Some circumstances in which the types of harm listed above may exist are as follows:

- There is generally a risk of identity theft or fraud where the type of information that was lost/stolen/accessed includes social insurance numbers, banking information or identification numbers;
- There is a risk of physical/bodily harm if the breach puts an individual at risk of stalking or harassment; or

- There may be a risk of hurt, humiliation or damage to reputation if the breach includes disciplinary records or other aspects of employment history.

2. When and How to Notify

When to Notify: Subsection 64(3) requires that individuals be notified (where required) ***at the first reasonable opportunity***. Notification of affected individuals should occur as soon as possible following the breach. However, if you have contacted law enforcement officials, you should determine from those officials if you should delay notification so as not to impede a criminal investigation.

How to Notify: The preferred method of notification is direct notification. Direct notification may be via a phone call, a letter or in person. Indirect notification, such as website information, posted notices or media, should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is unavailable. In certain cases, using multiple methods of notification may be the most effective approach.

3. Information to be Included in the Notification

Notifications should include the following pieces of information:

- date of the breach;
- description of the breach;
- description of the information inappropriately accessed, collected, used or disclosed;
- steps taken so far to mitigate the harm;
- next steps planned and any long term plans to prevent future breaches;
- steps the individual can take to further mitigate the risk of harm;
- contact information of an individual within the public body or organization who can answer questions or provide further information; and
- contact information for the Office of the Information and Privacy Commissioner, to whom individuals have the right to file a complaint regarding a breach of privacy.

The information should be general and should not 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.

4. Others to Contact

Subsection 64(4) **requires** the head of a public body to notify the Office of the Information and Privacy Commissioner where they reasonably believe that there has been a privacy breach involving the unauthorized collection, use or disclosure or personal information. The commissioner may, notwithstanding the fact that there is no risk of significant harm, recommend that the head of the public body notify affected individuals at the first reasonable opportunity (subsection 64(5)).

Regardless of the approach taken to notify individuals, public bodies should consider whether or not the following authorities or organizations should be informed of the breach:

- Police: especially if theft or another crime is suspected.
- Insurers: especially if required by contractual obligations.
- Professional or other regulatory bodies: especially if professional or regulatory standards require notification of these bodies.
- ATIPP Office: so that your Senior Privacy Analyst can provide advice or guidance in regard to the privacy breach.

Step 4: Prevention

Once immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to investigate the cause of the breach. This could include:

1. A security audit of administrative, physical and technical security measures. This is an opportunity to develop or improve adequate long-term safeguards against further breaches;
2. Review and update applicable policies to reflect the lessons learned from the investigation and regular review of policies should be implemented;
3. An audit at the end of the investigation process to ensure that the prevention plan has been fully implemented; and/or
4. Training of public body employees to ensure organizational understanding of a public body's privacy obligations under the *Act.*

Chapter 10: Privacy Complaints and the Role of the OIPC

Part III, Division 2 of the *Act* gives individuals the right to make a complaint to the Office of the Information and Privacy Commissioner (OIPC), where they believe that their personal information has been collected, used or disclosed contrary to the *Act*, as set out in subsection 73(1).

In addition to the authority to investigate complaints, the *Act* gives the commissioner the authority to conduct investigations to ensure a public body's compliance with the *Act*, and to monitor and audit the practices and procedures of a public body in carrying out their responsibility under the *Act*. These investigations and audits may be commenced by the commissioner on his or her own initiative and are not dependent on a specific complaint being made.

The Office of the Information and Privacy Commissioner can be contacted at:

The Office of the Information and Privacy Commissioner
Sir Brian Dunfield Building
3rd Floor, 2 Canada Drive
P.O. Box 13004, Station "A"
St. John's, NL A1B 3V8
Tel: (709) 729-6309
Fax: (709) 729-6500
Toll Free in Newfoundland and Labrador: 1-877-729-6309
e-mail: commissioner@oipc.nl.ca

10.1 Privacy Complaints (section 73)

Section 73(1) of the *Act* states that where an individual believes, on reasonable grounds, that his or her personal information has been collected, used or disclosed by a public body in contravention of the *Act*, he or she can file a privacy complaint with the commissioner.

A person may also file a privacy complaint with the commissioner on behalf of another individual, or group of individuals, where that individual or those individuals in the affected group have given their consent (subsection 73(2)).

In addition, the commissioner may carry out an investigation on his or her own motion where he or she believes that personal information has been collected, used or disclosed by a public body in contravention of the *Act* (subsection 73(3)).

Privacy complaints must be:

- filed in writing; and

- made within one year after the subject matter of the privacy complaint first came to the attention of the complainant or should reasonably have come to the attention of the complainant, or within such other time as the commissioner may allow.

The date on which the privacy breach occurred is not necessarily the date on which the one-year period for filing a complaint begins to run. An affected individual, if they are not notified, may have no way of knowing that their personal information has been collected, used or disclosed in a manner that is contrary to the *Act*.

> For example, if a T4 slip containing an individual's name, address, social insurance number and income information is inadvertently mailed to the wrong address in January 2015, but the error is not discovered and the affected individual is not notified until March 2015, the time period for making a privacy complaint begins to run in March 2015.

Where an individual was not notified by the public body, but should reasonably have been aware of the privacy breach in any event, the time period will begin to run on the date on which the subject matter of the breach should have come to their attention.

Once a privacy complaint is filed, the commissioner will provide a copy or summary of the complaint, including an investigation initiated on the commissioner's own motion, to the head of the public body concerned (subsection 73(5)).

10.2 Investigation of a Complaint (section 74)

In addition to the procedures set out in Part III, Division 2 of the *Act* respecting privacy complaints, the general investigative powers and duties of the commissioner set out in Part IV, Division 2 apply to privacy complaints (subsection 95(3)).

10.2.1 Informal Investigation

When a privacy complaint is made, the privacy commissioner may take steps to resolve it informally to the satisfaction of the parties (subsection 74(1)).

However, where the commissioner is unable to informally resolve the complaint within a reasonable period of time, he or she is required to conduct a formal investigation into the subject of the complaint, where he or she is satisfied that there are reasonable grounds to do so (subsection 74(2)).

Where a person has five (5) active privacy complaints with the Office of the Information and Privacy Commissioner that deal with similar or related records, the commissioner is permitted to hold additional complaints and not commence a further investigation until one of the active complaints is resolved (subsection 74(5)).

10.2.2 Refusal to Investigate (section 75)

Section 75 provides that the commissioner may, at any stage of an investigation, decide not to investigate a privacy complaint where he or she is satisfied that

- the head of a public body has responded adequately to the privacy complaint;
- the privacy complaint has been or could be more appropriately dealt with by a procedure or proceeding other than a complaint under the *Act*;
- the length of time that has elapsed between the date when the subject matter of the privacy complaint arose and the date when the privacy complaint was filed is such that a review would be likely to result in undue prejudice to a person or that a report would not serve a useful purpose; or
- the privacy complaint is trivial, frivolous, vexatious or is made in bad faith.

10.2.3 Making Representations (section 96)

A complainant and the public body to which the privacy complaint relates may be given the opportunity to make representations to the commissioner in accordance with section 96, which provides that:

- the commissioner may give a person an opportunity to make a representation during an investigation;
- an investigation may be conducted in private, and a person who make representations during an investigation is not, except to the extent they are invited by the commissioner, entitled to be present during or comment on representations made by others;
- the commissioner can decide whether representations are to be made in writing or orally; and
- representations may be made through counsel or other agent.

10.2.4 Production of Records (section 97)

Subsection 97(2) states that the commissioner has the powers, privileges and immunities that are or may be conferred on a commissioner under the *Public Inquiries Act, 2006*.

The commissioner may require a public body to produce any record in its custody or under its control where it is considered relevant to an investigation and may examine information in a record, including personal information (subsection 97(3)).

Where the commissioner requests a record in relation to an investigation, a public body is required to produce that record or a copy of it as soon as possible, and in any event, no later than 10 business days after the request is made (subsection 97(4)).

In certain circumstances, the head of a public body may require the commissioner to examine an original record, rather than provide the commissioner with a copy. Under subsection 97(5), the head of a public body require this examination where:

- the head has a reasonable basis for concern about the security of a record that is subject to solicitor-client privilege or litigation privilege;

- the head has a reasonable basis for concern about the security of another record and the commissioner agrees that there is a reasonable basis for concern; or

- it is not practicable to make a copy of the record.

The head of a public body cannot, however, place any other condition on the ability of the commissioner to access or examine a record (subsection 97(6)).

Subsection 97(1) expressly provides that the commissioner's power to compel the production of documents (under section 97) and the right of entry (under section 98) apply to a certain records listed in subsection 5(1), notwithstanding the fact that the Act does not apply to them. As such, the commissioner **does** have the authority to compel the production of and examine the following records in the course of an investigation, where they are deemed relevant:

- Personal or constituency records of an MHA (paragraph 5(1)(c));
- Records of a registered political party or caucus (paragraph 5(1)(d));
- Personal or constituency records of a minister (paragraph 5(1)(e));
- Records of a question to be used on an examination or test (paragraph 5(1)(f));
- Records containing teaching materials or research information of an employee of a post-secondary institution (paragraph 5(1)(g));
- Material placed in the custody of the Provincial Archives by or for a person other than a public body (paragraph 5(1)(h)); and
- Material placed in the archives of a public body by or for a person other than the public body (paragraph 5(1)(i)).

The commissioner **does not** have the authority to compel the production of or examine the following records in subsection 5(1):

- Records in a court file, records of a judge of the Court of Appeal, Trial Division or Provincial Court, judicial administration records or records relating to support services provided to judges of those courts (paragraph 5(1)(a));
- Notes, communications or draft decisions of a person acting in a judicial or quasi-judicial capacity (paragraph 5(1)(b));

- Records relating to a prosecution if all proceedings in respect of the prosecution have not been completed (paragraph 5(1)(j));
- Records relating to an investigation by the RNC if all matters in respect of the investigation have not been completed (paragraph 5(1)(k));
- Records relating to an investigation by the RNC that would reveal the identity of a confidential source of information or reveal information provided by that source with respect to a law enforcement matter (paragraph 5(1)(l)); and
- Records relating to an investigation by the RNC in which suspicion of guilt of an identified person is expressed but no charge was ever laid, or relating to prosecutorial consideration of that investigation (paragraph 5(1)(m)).

The commissioner's powers under section 97 and 98 also apply notwithstanding:

- Subsection 7(2) (where another Act or regulation prohibits or restricts access);
- Another Act or regulation; or
- A privilege under the law of evidence.

The commissioner's ability to examine information in a record, and a public body's requirement to produce a record to the commissioner, includes records exempt under solicitor-client privilege (section 30) or cabinet confidences (section 27).

10.2.5 Right of Entry (section 98)

The commissioner has the right:

- to enter an office of a public body and examine and make copies of a record in the custody of the public body (paragraph 98(a)); and
- to converse in private with an officer or employee of the public body (paragraph 98(b)).

As discussed above, section 98 applies notwithstanding paragraphs 5(1)(c) to (i), subsection 7(2), another Act or regulation, or a privilege under the law of evidence.

10.2.6 Admissibility of Evidence (section 99)

Subsection 99(1) states that a statement made, or answer or evidence given by a person in the course of an investigation by the commissioner under the *Act* is not admissible in evidence against a person in a court or at an inquiry or in another proceeding, and no evidence respecting a proceeding under the *Act* shall be given against a person except:

- in a prosecution for perjury;
- in a prosecution for an offence under the *Act*; or
- in an appeal to, or an application for a declaration from, the Trial Division under the *Act*, or in an appeal to the Court of Appeal respecting a matter under the *Act*.

The commissioner, and anyone acting for or under the direction of the commissioner, shall not be required to give evidence in a court or in any other proceeding about information that comes to the knowledge of the commissioner in performing duties or exercising powers under the *Act* (subsection 99(2)).

10.2.7 Privilege (section 100)

Subsection 100(1) states that where a person speaks to, supplies information to or produces a record during an investigation by the commissioner under the *Act*, what he or she says, the information supplied and the record produced are privileged in the same manner as if they were said, supplied or produced in a proceeding in a court. Section 100 is intended to protect those records that are supplied to or produced for the commissioner as part of the informal or formal complaint resolution process. In considering section 55 of the former Act (which is identical to the current subsection 100(1)), the Newfoundland and Labrador Supreme Court, Trial Division commented on the application of this privilege, and determined that:

> …the correct interpretation of section 55 is that in regard records produced during either [the commissioner's informal or formal resolution process] they are privileged from production under a later request for records to the public body involved in the prior investigation by the Commissioner. To find otherwise would not only hamper the resolution processes of the Commissioner but could also result in revealing the substance of a record the public body may have successfully claimed to be exempt from disclosure, thus defeating the purpose of the Act.[17]

The Newfoundland and Labrador Court of Appeal has also commented that the privilege "preserves the privilege over documents in the hands of the Commissioner, to the same extent as if the documents had been tendered in court…".[18]

Where a record does not contain information that was supplied to the commissioner as part of an investigation or where the document itself was not produced to the commissioner, the privilege in section 100 will not apply.

[17] McBreairty v. College of the North Atlantic, 2010 NLTD 28.
[18] Newfoundland and Labrador (Information and Privacy Commissioner) v. Newfoundland and Labrador (Attorney General), 2011 NLCA 69

Subsection 100(2) provides that solicitor-client privilege and litigation privilege are not affected by production of records to the commissioner. The fact that a record to which solicitor-client privilege or litigation privilege applies has been disclosed to the commissioner as part of an investigation will not result in the privilege being waived with respect to any other third party who makes request the information.

10.2.8 Section 8.1 of the Evidence Act

Section 101 provides that section 8.1 of the *Evidence Act* does not apply to an investigation conducted by the commissioner under the *Act*.

Section 8.1 of the *Evidence Act* restricts, in the context of a legal proceeding, the admissibility of information and records relating to the Provincial Perinatal Committee; the Child Death Review Committee under the *Fatalities Investigations Act*; a quality assurance committee of a member, as defined under the *Hospital and Nursing Home Association Act*; and a peer review committee of a member, as defined under the *Hospital and Nursing Home Association Act*.

This restriction has no applicability with respect to proceedings conducted by the commissioner.

10.2.9 Time Limit for Conducting an Investigation

The commissioner must complete a formal investigation and make a report on a privacy complaint within a time that is "as expeditious as possible in the circumstances" (subsection 74(3)).

10.3 Commissioner's Report (sections 76 and 77)

On completing an investigation into a privacy complaint, the commissioner may recommend that the head of a public body:

- stop collecting, using or disclosing personal information in contravention of the *Act* (paragraph 76(1)(a)); or
- destroy personal information that was collected in contravention of the *Act* (paragraph 76(1)(b)).

The commissioner may also make:

- a recommendation that an information practice, policy or procedure be implemented, modified, stopped or not commenced (paragraph 76(2)(a)); or

- a recommendation on the privacy aspect of the matter that is the subject of the privacy complaint (paragraph 76(2)(b)).

On completing an investigation into a privacy complaint, the commissioner is required to:

- prepare a report containing his or her findings and, where appropriate, his or her recommendations and the reasons for those recommendations (paragraph 77(1)(a)); and

- send a copy of the report to the person who filed the privacy complaint and to the head of the public body concerned (paragraph 77(1)(b)).

The report must also include information respecting the obligation of the head of the public body to notify the person who filed the privacy complaint of the head's response to the commissioner's recommendations within 10 business days of receiving them (subsection 77(2)).

10.4 Response of Public Body (section 78)

Where the commissioner issues a report and makes a recommendation in response to a privacy complaint, subsection 78(1) requires the head of a public body to

- make a decision whether or not to follow the recommendation of the commissioner in whole or in part; and

- give written notice of the decision to the commissioner and a person who was sent a copy of the report.

The head of the public body must respond to the commissioner's recommendations **not later than 10 business days** after receiving them.

Where the head of the public body does not give written notice within 10 business days after receiving the commissioner's report, the head of the public body is considered to have agreed to follow the recommendation of the commissioner (subsection 78(2)).

10.5 Application for Declaration from Court (section 79)

Where the head decides not to comply with a recommendation of the commissioner, either in whole or in part, the head must apply to the Supreme Court, Trial Division for a declaration that the public body is not required to comply with the recommendation because the collection, use or disclosure of the personal information is not in contravention of the *Act* (paragraph 79(1)(a)).

This application must be made within 10 business days of after receiving the commissioner's recommendation.

Public bodies should consult with their legal counsel when considering filing an application for a declaration under section 79.

Where the head of a public body makes an application for a declaration from the Trial Division, a copy of the application must be served on the commissioner, the minister responsible for the administration of the Act, and a person who was sent a copy of the commissioner's report within 10 business days after receiving the recommendations (paragraph 79(1)(b)).

The commissioner or the minister responsible for the administration of the *Act* may intervene in an application for a declaration by filing a notice to that effect with the Trial Division (subsection 79(2)).

10.5.1 Procedure on Application for Declaration

The practice and procedure under the Rules of the Supreme Court, 1986 providing for an expedited trial, or such adaptation of those rules as the court or judge considers appropriate in the circumstances, will apply to the application (section 81).

Solicitor-client privilege and litigation privilege of a disputed record which may contain personal information will not be affected by disclosure to the Trial Division for the purposes of an application (section 82).

The Trial Division must review the act or failure to act of the head of a public body that relates to the collection, use or disclosure of personal information as a new matter, and may receive evidence by affidavit (subsection 83(1)). This means that the Trial Division may hear evidence, and is not restricted to the same evidence that was produced during the commissioner's investigation of the privacy complaint.

Where the Trial Division exercises its powers to compel the production of documents for examination, it must take reasonable precautions to avoid disclosure of:

- any information or other material if the nature of the information or material could justify a refusal by the head of a public body to give access to a record or part of a record; or

- the existence of information, where the head of the public body is authorized to refuse to confirm or deny that the information exists under subsection 17(2).

These reasonable precautions may include, where appropriate:

- receiving representations without notice to another person,

- conducting hearings in private, and
- examining records in private (subsection 83(2)).

10.5.2 Disposition of Application

Section 84 provides that where the Trial Division hears an application for a declaration under section 79, the court may:

- grant the application, where it determines that the head of the public body is authorized to use, collect or disclose the personal information;
- order the head of the public body to stop using, collecting or disclosing the personal information, where it determines that the head of the public body is not authorized to use, collect or disclose the personal information; or
- order the head of the public body to destroy the personal information that was collected in contravention of the *Act*.

The Trial Division may also make any other order that the court considers appropriate.

10.6 Filing an Order with the Trial Division (section 80)

Under section 80, the commissioner can file an order with the Trial Division to give binding effect to his or her recommendation in certain circumstances.

Section 80(1) gives the commissioner the authority to prepare and file an order with the Trial Division where:

- the head of the public body agrees or is considered to have agreed under section 78 to comply with the commissioner's recommendation in whole or in part but fails to do so within 1 year after receipt of the recommendation; or
- the head of the public body fails to apply to the Trial Division for a declaration under section 79.

An order filed under this section shall be limited to a direction to the head of a public body either:

- to stop collecting, using or disclosing personal information in contravention of the *Act*; or

- to destroy personal information collected in contravention of the *Act* (subsection 80(2)).

The commissioner may not file an order with the Trial Division until the one-year time period in paragraph 80(1)(a) has passed (subsection 80(3)).

Where the commissioner files an order with the Trial Division, it is enforceable against the public body as if it were a judgment or order made by the court (subsection 80(4)).

10.7 Disclosure of Information (section 102)

Section 102 of the *Act* places restrictions on disclosure by the commissioner, and by the commissioner's staff, of information they obtain in performing duties or exercising powers under the *Act*.

Specifically, subsection 102(1) states that the commissioner and a person acting for or under the direction of the commissioner, shall not disclose information obtained in performing duties or exercising powers under the *Act*, except as provided in subsections 102(2) to (5).

Subsection 102(2) states that the commissioner may disclose, or may authorize a person acting for or under his or her direction to disclose, information that is necessary to:

- perform a duty or exercise a power of the commissioner under the *Act*; or
- establish the grounds for findings and recommendations contained in a report under the *Act*.

In conducting an investigation and in performing any other duty or exercising any power under the *Act*, the commissioner, and anyone acting for or under the direction of the commissioner, shall take reasonable precautions to avoid disclosing and must not disclose:

- any information or other material if the nature of the information or material could justify a refusal by a head of a public body to give access to a record or part of a record; or
- the existence of information, where the head of a public body is authorized under subsection 17(2) of the *Act* to refuse to confirm or deny that the information exists in response to a request for access to information under the *Act* (subsection 102(3)).

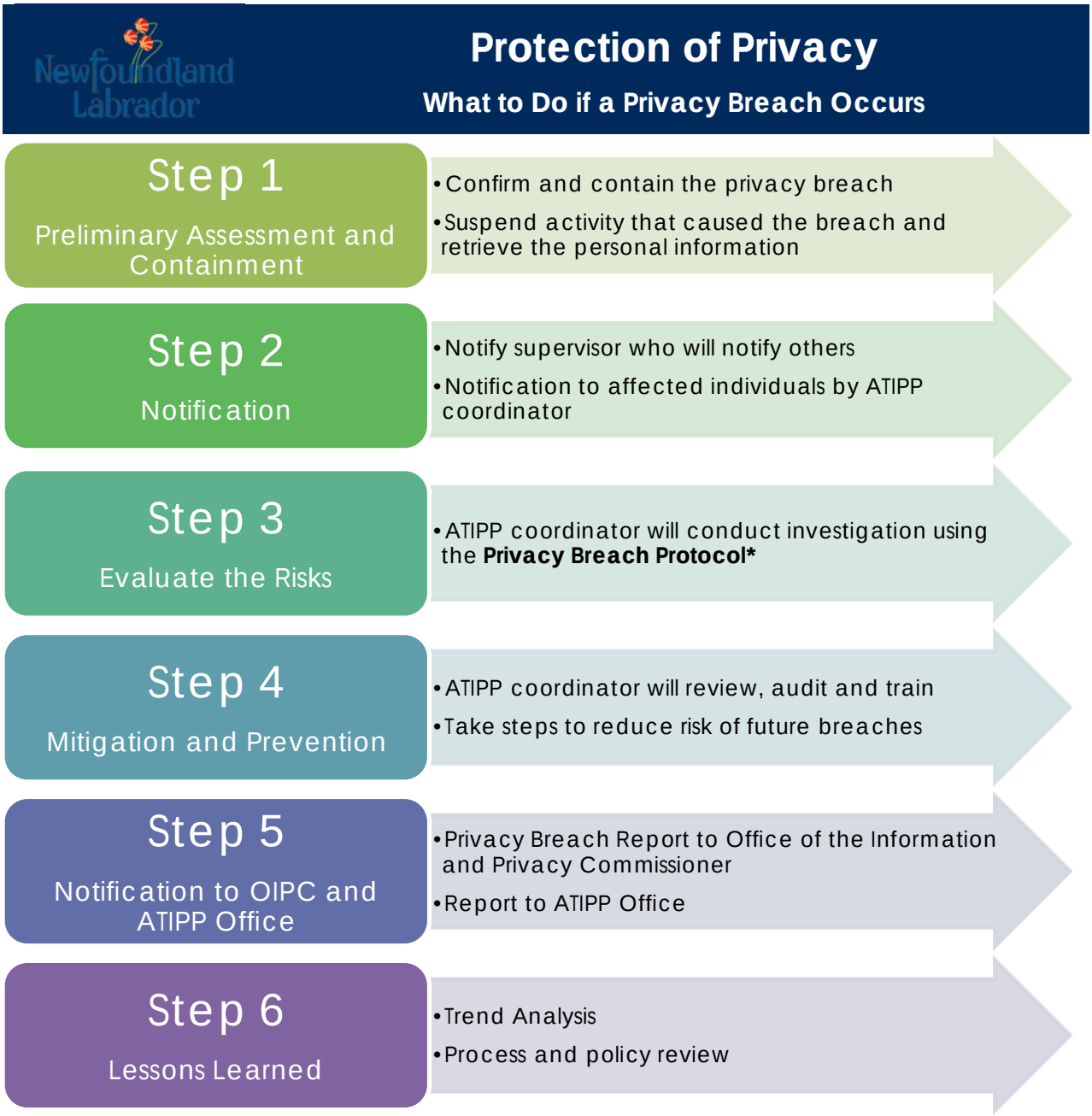
In addition, the commissioner may disclose to the Attorney General information relating to the commission of an offence under the *Act* or under any other Act of Newfoundland and Labrador or Canada where the commissioner has reason to believe an offence has been committed (subsection 102(4)).

Subsection 102(5) states that the commissioner may disclose, or may authorize a person acting for or under his or her direction to disclose, information in the course of a prosecution or an appeal referred to in subsection 99(1).

10.8 Protection from Liability (section 104)

Section 104 states that an action does not lie against the commissioner or against a person employed under him or her for anything he or she may do or report or say in the course of the exercise or performance, or intended exercise or performance, of his or her functions and duties under the *Act*, unless it is shown he or she acted in bad faith.

Appendix A: What to Do if a Privacy Breach Occurs



Many of the steps outlined above must be carried out simultaneously or in quick succession. For more information contact the ATIPP Office at (709) 729-7072 or visit: www.atipp.gov.nl.ca.

*Find the Privacy Breach Protocol at: http://www.atipp.gov.nl.ca/info/privacybreach.html and Privacy Breach Reporting Form at: http://oipc.nl.ca/pdfs/PrivacyBreachIncidentReportForm.pdf.

Appendix B: Privacy Breach Protocol

Protection of Privacy

Privacy Breach Protocol

March 2015

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*** from the ATIPP Office website and submit it to your Senior Privacy Analyst with the ATIPP Office and the Office of the Information and Privacy Commissioner (OIPC).

- 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 (729-212) 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	☐	☐

Questions to Consider	Yes	No
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	☐
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 not 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: http://www.atipp.gov.nl.ca/

Appendix C: Authorization of Representative

Proof of Authority Form

Personal information on this form is collected under the Newfoundland and Labrador *Access to Information and Protection of Privacy (ATIPP) Act, 2015* and will be used to designate an *authorized* representative to make a Personal Information Request or requests for correction of personal information on your behalf. Attach this form to the Information Request form or Request for Correction of Personal Information Form and submit as part of that request.

1. PROOF OF AUTHORITY

To Which Public Body Are You Submitting this Proof of Authority? _____

2. APPLICANT INFORMATION

Applicant Name:

Organization (*where applicable*):

Address:

_____

_____

_____ **Postal Code**: _____

Daytime Telephone #: ( )	**Facsimile #**: ( )
E-Mail:	

3. CONSENT

Pursuant to Section 108 of the *ATIPP Act*:

I, _____(*Your Name*) hereby give authorization to _____(*Name of Authorized Representative)* as my personal representative to act on my behalf, and to exercise:

	My right to access <u>all of my records</u> containing personal information
	My right to access my records, as indicated on the Access to Information Request Form (Form 1)
	My right to request correction(s) to my personal information, as indicated on the Request for Correction of Personal Information Form
Please select:	
	This consent will expire upon completion of the request.
	This consent will expire on (YYYY-MM-DD):

Applicant's Signature: _____ **Date**: _____
YYYY-MM-DD

Witness Signature: _____ **Date**: _____
YYYY-MM-DD

Note: You may revoke this Proof of Authority at any time by contacting the above public body

Personal information collected on this form is protected by the *Access to Information and Protection of Privacy Act*.

Inquiries about the use and protection of this personal information should be directed to the Access and Privacy Coordinator of the public body to whom the application is sent.

Schedule 1 –MHA Annotation of Verbal Consent

This letter should be printed on MHA Letterhead paper.

Please remove this text before printing.

Annotation of Verbal Consent File #: _____

This form is confirmation that the Honourable Member has received consent to request information from a government department or public body on behalf of the constituent.

On _____,
(Date: YYYY-MM-DD)

_____
(Name of Constituent)

provided VERBAL CONSENT for

_____
(Name of MHA)

to make a request on their behalf for the purpose of:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____ _____
Signature of MHA or MHA's Representative *Date (YYYY-MM-DD)*