CHAPTER 2

PART 2 - PROTECTION OF PRIVACY

DIVISION 1 APPLICATION OF THIS ACT

Section 10 – Non-application to personal health information

DIVISION 2 PRIVACY IMPACT ASSESSMENT

Section 11 – Privacy Impact assessment

DIVISION 3 COLLECTION OF PERSONAL INFORMATION

Section 12 – Prohibition – collection

Section 13 – Employee to report suspected unauthorized collection

Section 14 – Response to report of suspected unauthorized collection

Section 15 – Collection only if authorized

Section 16 – Direct collection unless indirect collection authorized

Section 17 – Notice of direct collection

Section 18 – Personal information received by public body without request

DIVISION 4 USE OF PERSONAL INFORMATION

DIVISON 5 DISCLOSURE OF PERSONAL INFORMATION

DIVISION 6 SPECIALIZED SERVICES AND DATA-LINKING

DIVISION 7 PROTECTING PERSONAL INFORMATION

DIVISION 8 ACCESSING AND CORRECTING PERSONAL INFORMATION

DIVISION 9 PRIVACY COMPLAINTS

CHAPTER 2 OVERVIEW

Chapter 2 of the manual provides an interpretation of **Part 2 PROTECTION OF PRIVACY** of the *Access to Information and Protection of Privacy (ATIPP) Act*.

This chapter will discuss:

- collection of personal information;
- use of personal information;
- disclosure of personal information;
- privacy Breaches; and
- privacy Impact Assessments.

UNDERSTANDING PROGRAM, ACTIVITY AND SERVICE

WHAT IS A PROGRAM?

Programs are established through legislation for each department and are provided with a mandate and budget under the *Financial Administration Act (FAA)* and *Yukon Act*.

The Financial Administration Manual written under the FAA, provides the following definition of a program:

> "*Program means that part of a vote identified as a program and which reflects government policy and is comprised of activities designed to accomplish a specified objective or set of objectives.*"

As defined in the Yukon *Financial Administration Act*, "Vote" means that part of an appropriation act identified as a vote and authorizing the payment of a specified amount from the consolidated revenue fund for specified purposes. For more information, see page 4 of the Yukon *Financial Administration Act*.

Identifying Program and Activities

The Department of Finance identifies departments, programs and activities using a systematic numbering system commonly referred to as **coding**. Coding is broken down to the department code, the vote or budget, the program, the activity and sub-ledgers that signify common financial services.

For example:

551-XXXXXX

55 is the department code

55**1**-XXXXXX or 55**2**-XXXXXX

1 or **2** signifies the vote (Operations and Maintenance budget [1], or Capital Budget [2]). See the section highlighted in yellow on the following page.

The next 6 digits signify the program

551-**XX**XXXX

And the activity or elements

551-XX**XXXX**

Using the Department of Highways and Public Works as an example, here is the 19/20 budget for Information and Communications Technology – a **PROGRAM** of the department. ICT is commonly referred to as a division, but it is a program from the perspective of Finance. As an example, here is a budget document from Information and Communications Technology program (ICT) with the PROGRAM identified.

MINISTERIAL BODY

HIGHWAYS AND PUBLIC WORKS

PROGRAM

INFORMATION AND COMMUNICATIONS TECHNOLOGY

PROGRAM MANDATE

- To provide leadership, advice and centralized network, software and telecommunications services to the Government of Yukon in support of their evolving use of computer and communications technologies.
- To provide leadership in the management, storage and protection of the government's information assets, and to facilitate public access to government records while protecting the privacy of individuals.
- To develop and manage essential information and communications technology infrastructure including a Yukon-wide mobile radio service for government use.

PROGRAM SUMMARY ($000s)	2019-20 ESTIMATE	*Comparable* 2018-19 FORECAST	*Comparable* 2018-19 ESTIMATE	*Comparable* 2017-18 ACTUAL
Amounts included in the Appropriation				
Operation and Maintenance (Vote 55-1)				
Planning and Administration	**910**	800	900	1,014
Technology Infrastructure and Operations	**9,769**	9,024	9,024	8,507
Service Innovation and Support	**536**	241	529	550
E-Services	**1,901**	1,639	1,351	886
Corporate Information Management	**1,596**	1,490	1,490	1,330
Service Agreements	**5,321**	5,036	5,036	4,330
Information Management	**2,030**	1,573	1,573	1,398
	22,063	19,803	19,903	18,015

WHAT IS AN ACTIVITY?

An **ACTIVITY** is a function of the program. They are identified in the budget under the PROGRAM SUMMARY section. Note activities may be identified on both an operations and maintenance (O&M) budget document and capital budget document.

The Financial Administration Manual written under the FAA, provides the following definition of an activity and element:

> "*Activity means a sub-division of a program which is a focus for program planning and the setting of objectives, and is the lowest presented for debate in the Committee-of-the Whole of the Legislative Assembly*"
>
> "*Element means a sub-division of an activity designed to attain the objectives of that activity*"

ACTIVITIES

PROGRAM SUMMARY ($000s)

	2019-20 ESTIMATE	Comparable 2018-19 FORECAST	Comparable 2018-19 ESTIMATE	Comparable 2017-18 ACTUAL
Amounts included in the Appropriation				
Operation and Maintenance (Vote 55-1)				
Planning and Administration	**910**	800	900	1,014
Technology Infrastructure and Operations	**9,769**	9,024	9,024	8,507
Service Innovation and Support	**536**	241	529	550
E-Services	**1,901**	1,639	1,351	886
Corporate Information Management	**1,596**	1,490	1,490	1,330
Service Agreements	**5,321**	5,036	5,036	4,330
Information Management	**2,030**	1,573	1,573	1,398
	22,063	19,803	19,903	18,015

WHAT IS A SERVICE?

SERVICES are functions of the ministerial body that are provided internally to government and externally to the public for the purpose of fulfilling the **program mandate**. Below is a high-level overview of services provided by the Corporate Information Management (CIM) branch of ICT.

Depending on the budget, a service may be the equivalent of the department's element, or it may be broken down further to list all of the minute functions of each activity listed below.

Program: Information and Communications Technology (Division)

Activity: Corporate Information Management (Unit)

Mandate: To provide leadership in the management, storage and protection of the government's information assets and to facilitate public access to government records while protecting the privacy of individuals

Services: ATIPP Office, Information Management

For example:

ATIPP Office

The Access to Information and Protection of Privacy (ATIPP) Office provides corporate services as the central ATIPP service to the public and public bodies which includes:

- Operating the shared central ATIPP services
- Receiving and administering access requests
- Develop and make available corporate policies, standards and guidelines for public bodies to assist with compliance under the *ATIPP Act*
- Responding to general questions related to the *ATIPP Act*
- Report on ATIPP activities

UNDERSTANDING SIGNIFICANT HARM

There are 3 sections of the Act in Part 2 that ensure employees are reporting any suspected unauthorized collection (section 12), unauthorized use (section 19) and unauthorized disclosure (section 23) of personal information.

What is personal information?

Section 1 Definitions of the ATIPP Act provides a NON-EXHAUSTIVE definition of personal information to guide Designated Privacy Officers (DPO), Designated Access Officers (DAO), Heads and employees of public bodies in the application of the Act.

The definition is not finite, due to the nature of how personal information is used with advances in technology and the variety of programs, activities and services of a public body. Personal information may be affected by context.

In some cases, an individual's name and mailing address may involve low risk if a breach occurred, however depending on the other information or the breadth of the breach and other personal information involved, it may become more significant.

What is "SIGNIFICANT HARM"?

Section 1 Definitions of the ATIPP Act provides the following definition for significant harm:

"SIGNIFICANT HARM" means in respect of a privacy breach, bodily harm, personal humiliation, reputational or relationship damage, loss of employment, business or professional opportunities, financial loss, negative effects on a credit rating, or damage to or loss of property, or any other similar type of harm.

Note that the definition for "SIGNIFICANT HARM" is a 3 part definition that also applies to other Parts of the Act.

Designated Privacy Officers (DPO) are tasked with understanding their program areas and working closely with program employees in order to assess reports for suspected privacy breaches. DPOs need to have a clear understanding of each program's legislation, including Yukon or federal legislation, any paramountcy provisions and agreements in order to make an assessment under this Part of the Act.

When assessing and reporting suspected breaches, Designated Privacy Officers must use all available resources, including the provisions in this Act, the ATIPP Regulations and ATIPP Protocols, issued by the ATIPP Office.

For more on Designated Privacy Officers, please see Chapter 4 of the manual.

PART 2

DIVISION 1 – APPLICATION OF THIS PART

SECTION 10 Non-application to personal health information

Application: Ministerial Public Bodies defined or prescribed as Custodians under the Health Information Privacy and Management Act (HIPMA)

This provision in the Act clarifies the non-application of this Part to personal health information held by a custodian in relation to its functions as a custodian, and clarifies exemptions to non-application. For example, the requirement for ministerial public bodies to complete privacy impact assessments.

"PUBLIC BODY" means a ministerial body, or a statutory body or an entity prescribed through ATIPP Regulations as a public body. (See the ATIPP Regulations and **section 1** of the Act for definitions)

> **10(1)** This part, except for section 11, does not apply to personal health information held by a public body, or by a program or activity of a public body, under its authority and in relation to its function as a custodian.

Subsection 10(1) of the Act **does not** apply to personal health information (PHI) held by a public body in relation to its functions as a custodian. While the *Health Information Privacy and Management Act* (HIPMA) includes persons and groups other than those listed below as custodians of personal health information, **the *ATIPP Act* applies only to public bodies**.

Public bodies, or programs or activities of public bodies, that are also custodians under HIPMA include:

- Department of Health and Social Services,
- Emergency Medical Services (as a program of the Department of Community Services),
- and
- Yukon Hospital Corporation.

Unless prescribed through HIPMA Regulations, no other public body is a custodian.

Despite this Act not applying to the personal health information held by above named public bodies in their capacity as a custodian, **these public bodies are still required to complete privacy impact assessments (PIAs) in accordance with provision 11 of this Act**. The rationale for this requirement is that the ATIPP Act has more stringent requirements than HIPMA in respect of required PIAs, and higher standards should be consistently applied across ministerial public bodies.

For more on Privacy Impact Assessments, see the next section of this chapter.

"CUSTODIAN" has the same meaning as in the *Health Information Privacy and Management* Act and includes an agent (as defined in that Act) of a custodian.

HIPMA section 1 defines a **CUSTODIAN** as a person (other than a person who is prescribed not to be a custodian) who is:

- the Department of Health and Social Services (HSS),
- the operator of a hospital or health facility,
- a health care provider, (HIPMA defines **HEALTH CARE** and **HEALTH CARE PROVIDER**)
- a prescribed branch, operation or program of a Yukon First Nation,
- the Minister of the Department of Health and Social Services,
- a person who, in another province
    - performs functions substantially similar to the functions performed by a health care provider, and
    - is, in the performance of those functions, subject to an enactment, of Canada or a province, that governs the collection, use and disclosure of personal information or personal health information, or
- a prescribed person (HIPMA defines **PERSON**).

HIPMA, section 1, defines **AGENT** of a custodian as a person (other than a person who is prescribed not to be an agent of the custodian) who acts for or on behalf of the custodian in respect of personal health information, including for greater certainty such a person who is:

- an employee of the custodian,
- a person who performs a service for the custodian under a contract or agency relationship with the custodian,
- an appointee, volunteer or student,
- an insurer or liability protection provider,
- an information manager,
- if the custodian is a corporation, an officer or director of the corporation, or
- a prescribed person.

HIPMA provides the following definition of **"HEALTH INFORMATION"** of an individual: identifying information of the individual, in unrecorded or recorded form, that relates to the individual's health or the provision of health care to the individual, payments for health care, the donation by the individual of any body part, tissue or bodily substance of the individual, is derived from the testing, including genetic testing, or examination of any body part, tissue or bodily substance of the individual, or is prescribed under HIPMA Regulations.

"PERSONAL INFORMATION"

> **10(2)** For greater certainty, despite a public body, or a program or activity of a public body, having the authority to act as a custodian, this Part applies to all personal information, other than personal health information, held by the public body or program or activity of the public body.

Subsection 10(2) clarifies that this Act **does apply** to any personal information, other than personal health information (PHI) that is held by one of the above named custodians. This Part applies to all personal information, other than personal health information, held by the public body or program or activity of the public body.

HIPMA, **section 10 Mixed Records**, states that if a record contains both personal health information and personal information of the same individual, the information is deemed to be personal health information of the individual.

HIPMA's *General Health Regulation (O.I.C. 2016/159)*, **section 10 Act does not apply**, provides a list of activities exempt from application of *HIPMA*, which are then subject to the ATIPP Act.

- Determining eligibility for employment, continuing employment or fitness to work for or with the Department [10(1)(a)];
- Administering disability benefits or a disability management program of or for employees of the Department [10(1)(b)];
- Assessing the qualifications of an actual or potential service provider to the Department;
- Making, processing, assessing or otherwise dealing with a claim or anticipated claim made under the *Workers' Compensation Act* [10(1)(c)], and
- Any matter arising under the *Occupational Health and Safety Act* in relation to any worker, as defined in the *Act*, in the course of work for or with the Department [10(1)(d)]

Section 12 of HIPMA states the Act does not apply to a record containing both personal health information that also contains information of the following types:

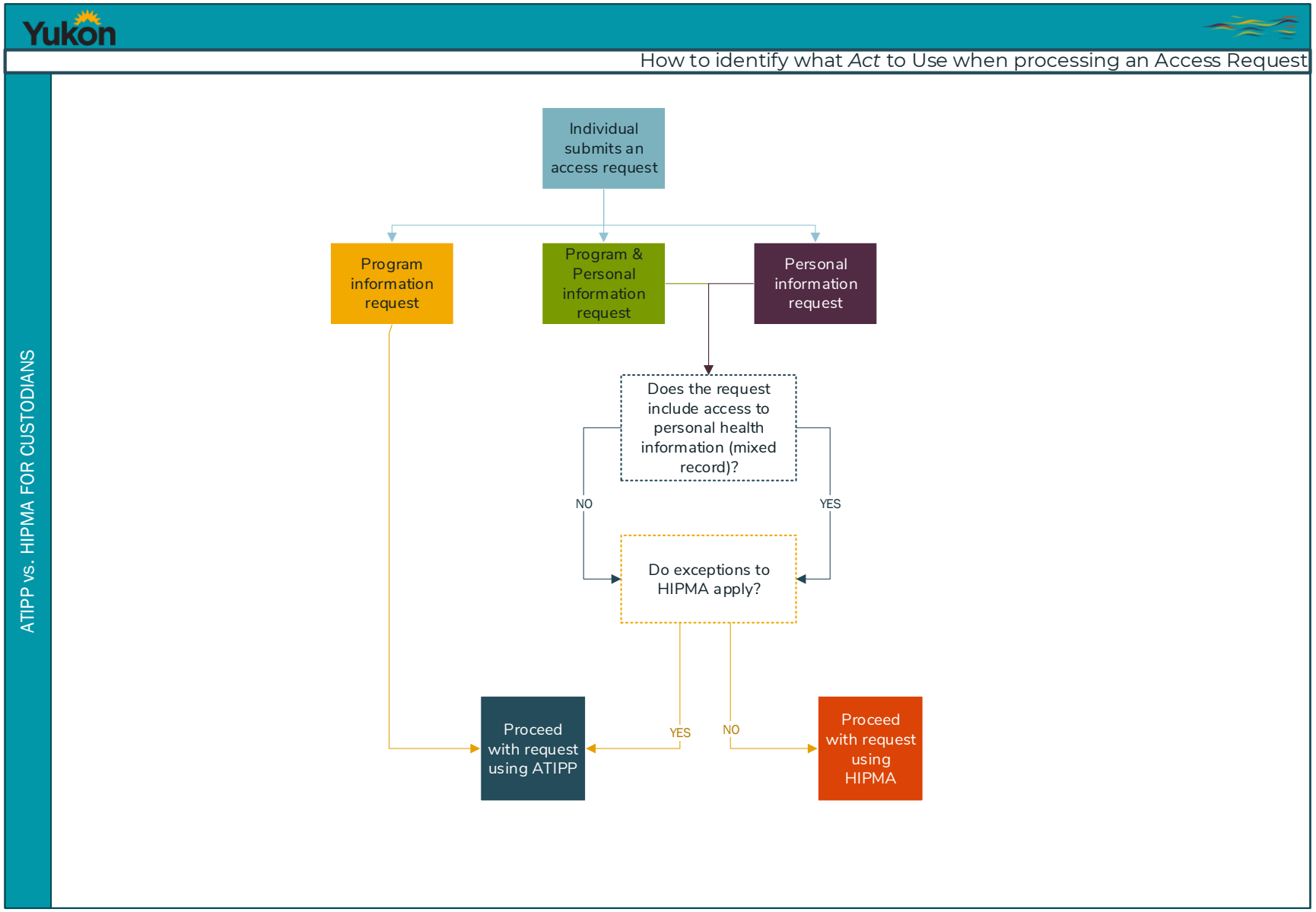
Information to which access is prohibited:

- Section 67 (Cabinet information),
- Section 68 (Confidential information from another government) or
- Section 71 (Personnel assessment conducted by or for public body) of the *ATIPP Act*.

Information to which access may be denied:

- Section 72 (Information related to law enforcement),
- Section 73 (Information subject to legal privilege),
- Section 74 (Policy advice and recommendations),
- Section 75 (Disclosure harmful to economic or financial interests of public body) and
- Section 76 (Disclosure harmful to intergovernmental relations) of the *ATIPP Act*.

FIGURE 1.1 NON-APPLICATION OF ACT



PART 2

DIVISION 2 PRIVACY IMPACT ASSESSMENT

SECTION 11 Privacy Impact Assessment

Application: Ministerial Public Bodies

Section **11** clarifies that the requirement to conduct a **"PRIVACY IMPACT ASSESSMENT" (PIA)** is specific to certain activities of ministerial bodies. This provision is limited to ministerial public bodies because smaller public bodies may not have the necessary resources or expertise to complete PIAs routinely. It is best practice for all public bodies to complete PIAs.

A PIA is a documented process for evaluating the collection, use and disclosure of personal information to identify and mitigate potential privacy risks.

Prior to the introduction of this section, PIAs were required to be conducted by all government departments in accordance with policy written under the General Administration Manual in 2016.

PIAs require updating when significant changes occur that impact the original privacy risks. The public body will amend the original PIA as changes to the intiative are implemented over time, in accordance with the ATIPP Protocols issued by the ATIPP Office.

Despite this Act not applying to the personal health information held by ministerial public bodies in their capacity as custodian, **these public bodies are still required to complete privacy impact assessments (PIAs) in accordance with this provision the Act**.

> **11(1)** The head of a public body that is a ministerial body must, in accordance with the regulations (see ATIPP Regulations), if any, conduct a privacy impact assessment of each of the following before the public body carries it out or provides it:
>
> **11(1)(a)** a proposed program or activity,
>
> **11(1)(b)** a proposed specialized service,
>
> **11(1)(c)** a proposed data-linking activity,
>
> **11(1)(d)** a proposed information management service, or
>
> **11(1)(e)** a significant change to an existing process.

Subsection **11(2)** provides the review requirements for public bodies conducting PIAs. This provision requires the ministerial public body to provide a copy of the PIA to the Access and Privacy Officer (ATIPP Office) and in certain cases to the Information and Privacy Commissioner (IPC).

11(2)(a) The head of a ministerial public body is required to provide a copy of all PIAs to the Access and Privacy Officer;

11(2)(b) in the case of a specialized service or data linking activity, the Information Privacy Commissioner.

SPECIALIZED SERVICES (INTEGRATED SERVICES/PERSONAL IDENTITY SERVICES) AND DATA LINKING ACTIVITIES

An**"INTEGRATED SERVICE"** is a service that will enable public bodies and partner agencies to collaboratively provide integrated services. Under the ATIPP Act, the Commissioner in Executive Council (Cabinet) can prescribe the purpose of an integrated service.

A **"PERSONAL IDENTITY SERVICE"** is a service to enable public bodies to provide client-centered services. The Commissioner in Executive Council (Cabinet) may approve a personal identity service by prescribing, along with the standards below, the public body that will act as the personal identity manager.

A "**DATA LINKING ACTIVITY**" means a data-linking activity approved under this section and involves involves linking of data from different sources to analyze and predict complex patterns of activity. Requiring a regulation for data-linking activities is one such measure to ensure purposes are prescribed before such methods and technologies are employed.

In regards to a specialized service or data linking activity, the Commissioner in Executive Council (Cabinet) may prescribe the following through regulation:

- Each service that will be provided,
- The types of personal information collected, used or disclosed,
- The terms and conditions that must be included, and
- If consent of an individual is required, the way in which consent must be given and withdrawn.

THE ROLE OF THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

Subsection 3 states the OIPC may provide recommendations to the head of the public body that conducted the PIA in respect of the proposal or change that is subject to it.

Subsection 4 provides the process for heads of public bodies to receive comments from the OIPC and the process for responding.

11(4) If the head of a public body receives a recommendation under subsection (3), the head has 30 days before carrying out the recommendation or provides the proposal or change to which the recommendation relates to:

11(4)(a) decide whether to accept of reject the recommendation and

11(4)(b) provide a notice of their decision to the OIPC. If the head does not provide this notice, the head is considered to have rejected the recommendation under subsection 5.

To give the OIPC time to formally review and comment, public bodies should provide the PIA to the OPIC at least 60 business days before implementing the proposed new or changed practice or system.

The public body should advise the OIPC of the project well in advance of implementation.

THE ROLE OF THE ATIPP OFFICE

PIA Reviews

The ATIPP Office provides services to review PIAs. The ATIPP Office will provide feedback, comments and recommendations to allow the head or delegated program manager to:

- make recommended changes to the PIA to strengthen and improve outcomes,
- revise the PIA draft to incorporate risk mitigations, and
- determine whether identified risks to privacy are acceptable.

The ATIPP Office has a service standard of 30 business days to review the first draft of your

PIA, so be sure to keep this in mind with your timelines.

The PIA will outline privacy risks to allow the head or delegated program manager to make a reasoned and informed final decisions under this provision. The final decision on whether and how to go forward with a project or initiative, rests solely with the public body responsible for the initiative.

For more on the PIA Process, please see the PIA Guidance document issued by the ATIPP Office and the ATIPP Protocols.

ACCESS TO INFORMATION REGISTRY

All PIAs are required to be submitted to the ATIPP Office.

Once the ATIPP Office receives the PIA, a summary of the PIA will be drawn from the description of the initiative and made public through the **Access to Information Registry**.

"ACCESS TO INFORMATION REGISTRY" means the registry established under subsection 85(1).

PART 2

DIVISION 3 - COLLECTION OF PERSONAL INFORMATION

SECTION 12 Prohibition - collection

This provision prohibits a public body from collecting personal information other than as authorized under this Part of the Act. As part of this prohibition, the public body must also ensure that it limits its collection of personal information to only the minimum collection amount necessary to fulfil the purposes for its collection.

> **12** A public body must not collect personal information
>
> **12(a)** except as provided under this Division; and
>
> **12(b)** beyond the amount that is reasonably necessary to carry out the purpose for which the personal information is collected.

Subsection (a) restricts the amount of personal information that can be collected by a public body. A public body is prohibited from collecting personal information other than "as authorized" under this Part of the Act.

"PERSONAL INFORMATION" is defined as recorded information about an identifiable individual and includes any type of information that would make it possible to identify one specific individual. This definition is non-exhaustive, but its paragraphs provide illustrative examples of different types of personal information that are caught by this expression. This definition is subject to **section 3**. This means that those types of information set out in provision 3 are not to be considered "personal information" for the purpose of this Act. The result of these two provisions, read together, is that wherever this Act uses the expression "personal information", that term does not include those types of information set out in section 3 even though such types of information would be, without this exception in provision 3, caught by this non-exhaustive definition of this expression.

"COLLECTION" of personal information, includes gathering or obtaining the personal information but does not include the use, disclosure or management of the personal information. This definition clearly defines the activities that, if undertaken in relation to personal information, are considered to be, or not be, a collection of personal information.

Appropriate **authorization for the collection of personal information** is further defined in **sections 15 and 16** of this Act. For example, public bodies can only collect personal information if an act authorizes the collection, if the information is for law enforcement, or if the information is necessary for operating a program or activity of the public body.

Subsection (b) clarifies that, as part of the restriction on the amount of personal information that a public body can collect, the public body must ensure that it limits its collection of personal information to only the minimum amount necessary to fulfill the purpose for its collection. Any collection beyond this minimum amount is "**unauthorized collection**."

The personal information must relate directly to and be necessary for an operating program or activity of the public body. The collected personal information cannot be for a prospective program or activity that does not currently exist, meaning that personal information must not be collected "just in case" it may be useful in the future.

SECTION 13 Employee to report suspected unauthorized collection

This section requires all **employees** of a public body to report any **unauthorized collection** of personal information to the public body's designated **privacy officer (DPO)**. The reporting of an instance such as this, must happen as soon as possible after the unauthorized collection has been discovered.

> **13** If an employee of a public body reasonably believes that an unauthorized collection of personal information by the public body has occurred or is occurring, the employee must, without delay, report the suspected unauthorized collection to the designated privacy officer for the public body.

An **"EMPLOYEE"** of a public body includes any individual who is:

- directly employed by the public body, or another public body that provides a service to the public body in question (appointed to their position in the public service under the *Public Service Act)*;
- a principal, vice-principal or teacher, or technical support staff, of the public body appointed to their position under the *Education Act*;
- a contractor or other service provider to the public body (whether or not they are compensated);
- a director or officer of the public body.

This substantive but non-exhaustive definition provides clarity in respect of who is an employee for the purposes of the ATIPP Act.

This definition makes it clear that if a person who is working under a contract for a public body (for example casual workers who do not meet the definition of an employee under the *Public Service Act*), or a person volunteering for a public body will be, for the purpose of this Act, considered as an employee of that public body.

Examples of "unauthorized collection"

If a public body collects personal information for a prospective program or activity that does not currently exist, that public body has over-collected information. Personal information must not be collected "just in case", or because it might be useful in the future. Personal information collected for the purpose of operating a program or activity of a public body and must **relate directly to and be necessary** for that program or activity. Public bodies are limited to collecting the minimum amount of personal information necessary to meet the stated purpose. Public bodies should not be collecting information on behalf of another public body for ease of disclosure.

Over-collection of personal information is considered to be an "unauthorized collection", but is not considered to be a privacy breach under this Act. A **"PRIVACY BREACH"** includes the unauthorized use, disclosure or disposal of, personal information, but does not include an unauthorized collection of the information. Although not a breach, employees are required to report suspected unauthorized collection under **section 13** of the *Act*. For more about how privacy breaches are handled, see the Privacy Breach Procedures guidance document issued by the ATIPP Office.

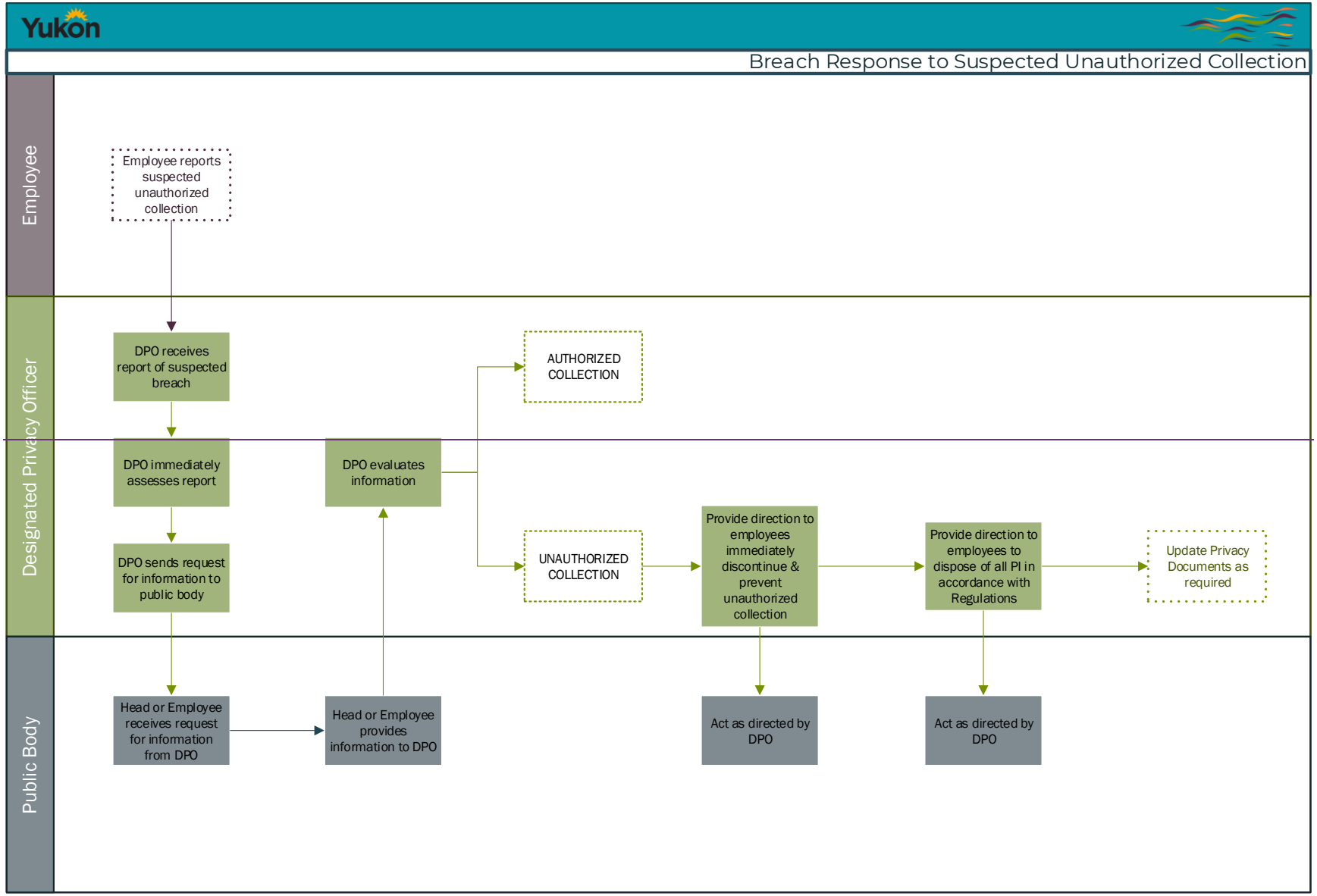
The Designated Privacy Officer (DPO) of a public body is designated by the head to ensure that the public body is accountable regarding the administration of privacy matters. This position is responsible for assessing and responding to any report of suspected unauthorized collection of personal information and suspected privacy breaches. For more about the role and responsibilities of DPOs, see the DPO Toolkit issued by the ATIPP Office.

Review of collection practices

A public body should regularly review their collection practices to ensure that any collection of personal information is authorized by **section 15**. Such a review should verify that there is:

- authority for the collection of personal information;
- discontinue the collection of personal information that does not meet the criteria set out in **section 15** and amend forms and other collection documents, contracts, agreements, policies and procedures that require the collection of this personal information;
- confirm that a process is in place to ensure that all new or modified collections of personal information meet the criteria set out in **section 15** and ensure that the minimum personal information necessary to meet program needs is collected;
- ensure that information that is needed only for subsets of clients is collected only from the clients that fit the subset criteria;
- verify that procedures are in place to ensure that any unsolicited personal information that is received by a public body is dealt with in accordance with section 18 of the ATIPP Act and disposed of in accordance with the ATIPP Regulations.

This review could be carried out by the program areas having custody or control over personal information with the advice of the ATIPP Office.


Yukon
Breach Response to Suspected Unauthorized Collection
Employee
Designated Privacy Officer
Public Body
Employee reports suspected unauthorized collection
DPO receives report of suspected breach
DPO immediately assesses report
DPO sends request for information to public body
Head or Employee receives request for information from DPO
Head or Employee provides information to DPO
DPO evaluates information
AUTHORIZED COLLECTION
UNAUTHORIZED COLLECTION
Provide direction to employees immediately discontinue & prevent unauthorized collection
Act as directed by DPO
Provide direction to employees to dispose of all PI in accordance with Regulations
Act as directed by DPO
Update Privacy Documents as required

SECTION 14 Response to report of suspected unauthorized collection

This provision details how a report of unauthorized collection is to be administered by outlining the responsibilities of the employee's response to the Designated Privacy Officer (DPO) in order for a determination to be made regarding the collection. This provision provides the DPO with the authority to decide whether the collection is valid and recommend actions to resolve the matter, including destroying the information in accordance with ATIPP Regulations. Please the ATIPP Regulations for more information.

"DESIGNATED PRIVACY OFFICER" (DPO) of a public body, means the employee designated under paragraph **87(1)(a)** as the designated privacy officer for the public body. Each public body has only one Designated Privacy Officer to ensure that accountability is maintained in respect of administration of privacy matters. For more on designated officers, please see **Chapter 4**.

> **14(1)** Without delay after receiving a report made under section 13, a Designated Privacy Officer must assess the report.

Subsection 1 states that when a designated privacy officer receives a report of suspected unauthorized collection of personal information, they must immediately assess the report.

> **14(2)** For the purpose of an assessment under subsection (1), the designated privacy officer for a public body may request from the head or an employee of the public body any information that the designated privacy officer considers necessary to conduct their assessment.

Subsection 2 authorizes the Designated Privacy Officer to request any information necessary to conduct an assessment regarding a possible unauthorized collection of personal information from the head or employee of public body.

Assessing a report of unauthorized collection may include reviewing the public body's privacy compliance documents including Personal Information Maps (PIM), Privacy Impact Assessments (PIA), Information Management Service Agreements (IMSA), Service Level Agreements (SLA), Information Sharing Agreements (ISA) and Research Agreements.

In order to confirm the unauthorized collection, DPO's may request assistance from their IT team.

DPOs for ministerial bodies may also request assistance from their departmental Information Technology (IT) unit/branch or Government of Yukon's Corporate Information Communications Technology (ICT) program.

> **14(3)** Without delay after receiving a request under subsection (2), the head or employee who received the request must, if they hold the information requested, provide it to the designated privacy officer for the public body.

Subsection 3 states that upon receiving a request for information, the head or employees of a public body **must** respond to their privacy officer *without delay* if they hold the information requested.

> **14(4)** If, after conducting their assessment, a designated privacy officer determines that an unauthorized collection has occurred or is occurring, the designated privacy officer must, without delay,
>
> **14(4)(a)** take the action, or direct any employee of the public body to take the action, that the designated privacy officer considers necessary to immediately discontinue or prevent the unauthorized collection; and
>
> **14(4)(b)** subject to paragraph 22(b), dispose of all personal information, in accordance with the regulations, that was collected by means of the unauthorized collection. Please see ATIPP Regulations.

Subsection 4 authorizes the Designated Privacy Officer to decide whether the reported unauthorized collection is occuring and to recommend actions to resolve the matter, including destroying the personal information in accordance with the ATIPP Regulations (please refer to the ATIPP Regulations for more information). The DPO must make this decision *without delay*, or immediately after making the determination.

The DPO's determination as to whether or not the collection of personal information is authorized will be based on consideration of:

- the purpose(s) of the collection (valid purposes are set out in **section 15**), and
- if the public body collected information indirectly, the circumstances under which the indirect collection occurred (valid circumstances for the indirect collection of personal information are set out in **section 16**).

SECTION 15 - Collection only if authorized

This provision identifies the purposes for which personal information can be collected by a public body. Public bodies cannot collect personal information unless the collection is authorized. This section clarifies *when* personal information can be collected by a public body.

Direct collection of personal information is authorized if:

> **15(a)** the collection is authorized or required under an Act of the Legislature or of Parliament;
>
> **15(b)** it is required for law enforcement purposes;

> **15(c)** collection as it is required for carrying out, evaluating, planning or providing a particular service;

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 have a demonstrable need for the information.

Subsection (c) splits the authority for collection between providing and planning for a program or activities, including specialized service, data-linking activity or information management service. This allows the ministerial public body to make the distinction between planning for a new or significant change to an existing program, activity, system or service and implementation.

PIAs are a useful tool that assist ministerial public bodies to ensure privacy is incorporated into the new endeavour, and should be completedduring the planning phase of an initiative.

> **15(c)(i)** carrying out or evaluating a program or activity of the public body, or a data-linking activity in respect of which the public body is a partner
>
> **15(c)(ii)** providing or evaluating a specialized service in respect of which the public body is the personal identity manager or a partner, or

Subsection (c)(iii) provides a distinct authority for ministerial public bodies that are planning new or changes to existing programs or activities, including specialized service, data-linking activity or information management service that requires a privacy impact assessment and input from the Commissioner.

> **15(c)(iii)(A)** planning a proposed program or activity of the public body,
>
> **15(c)(iii)(B)** planning a proposed specialized service in respect of which the public body is the personal identity manager or a partner; or
>
> **15(c)(iii)(C)** planning a proposed data-linking activity in respect of which the public body is a partner; or
>
> **15(d)** the collection is for a prescribed purpose other than a purpose referred to in paragraphs (a) to (c) and the individual consents, in the prescribed manner, to that collection.

Subsection (d) provides the authority for an 'other' purpose prescribed through ATIPP Regulations that gives the public body the ability to acquire consent from individuals to directly collect their personal information.

SECTION 16 - Direct collection unless indirect collection authorized

This section provides for the specifically authorized circumstances in which a public body may indirectly collect personal information of an individual**.** Any collection of personal information outside the valid purposes and/or circumstances set out in **sections 15 and 16** of this Act will be considered to be an unauthorized collection.

Indirect collection is authorized if:

> **16(1)** A public body authorized under section 15 to collect the personal information of an individual must collect it directly from the individual except if authorized under subsection (2) to collect it from another source.

Subsection 2 provides the authority for which a public body may collect the personal information of an individual from a source other than the individual only if:

> **16(2)(a)** the individual consents, in the prescribed manner, to the public body's collection from another source;

To use **subsection (2)(a)**, the public body is required to act in the manner prescribed through ATIPP Regulations. Please see the ATIPP Regulations for more information.

If an individual authorizes a public body to collect personal information from another public body or from a custodian under the *Health Information Privacy Management Act*, the written authorization for the collection is often included in the same form as the authority for the other body or custodian to disclose the necessary information to the first public body. As a result, the authorization format should take into consideration the disclosure (and possibly the consent) requirements of the ATIPP Act and HIPMA if the disclosing public body is a custodian under that Act.

> **16(2)(b)** one of the following applies:
>
> **16(2)(b)(i)** the source is another public body that disclosed the personal information to the public body in accordance with section 25 or 26,

This provision can be used when indirectly collecting personal information from another public body, including instances listed in **16(2)(d)**. **Subsection 2(d)** is intended for the indirect collection from non-public bodies. However, an indirect collection about the supervision or discipline of an employee under subsection **(2)(d)(vii)** should use the authority **(2)(d)** to ensure the notification requirement is triggered.

> **16(2)(b)(ii)** the source is another public body that redirected the personal information to the public body in accordance with subsection 18(2),

This provision addresses instances whereby an activity or service receives information that it did not solicit, for example when the wrong public body receives a grant application and forwards it to the correct public body.

> **16(2)(b)(iii)** the source is a reputable public source, and the public body is collecting the personal information from that source for the purpose of making a decision that directly affects an individual,

"REPUTABLE PUBLIC SOURCE" means a source specified in a ministerial order made under **subsection 126(1)**. A source is authorized by a ministerial public order, after a 60-day public consultation. This provision provides the government the flexibility to regulate the indirect collection of personal information in the digital era.

The Minister is not required to specify any sources even after a consultation period; rather, inclusion of this tool allows the flexibility to decide, at a later date, that a particular source is a reputable source for which a public body may indirectly collect personal information for the purposes of making a decision affecting an individual.

> **16(2)(b)(iv)** the source is a source that contains publicly available information, and the public body is collecting the personal information from that source for a purpose other than the purpose of making a decision directly affecting an individual;

"PUBLICLY AVAILABLE INFORMATION" means personal information that is contained in a public registry, contained in a magazine, book, newspaper or other similar type of publication that is generally available to the public in print or electronic format, whether by purchase or otherwise, or of a type or class of personal information prescribed as publicly available information.

"PUBLIC REGISTRY" means a registry (other than a court registry), register, roll, list or other thing that (a) is established or maintained under an Act, (b) contains personal information, and (c) is prescribed as a public registry.

For more on public registries, see **Chapter 3**, Division 2 Open Access Information.

Most of this information would be readily available in a public or specialized library. Other public sources include information that is made available to the public at large in any medium. The information may not be routinely made available; it may be the type of information that can be made available on demand, for example, through a search of a database or making a request for a public record, as in the case of certain classes of court records. The information may be made available free or for a fee. Examples include information in reports of charitable organizations, announcements of honours or awards granted by or through a public body, copies of speeches or speaking notes when the speeches are given at a public event, and information available on the Internet.

Care should be taken when relying on personal information that is collected from the Internet and the credibility of the source of the information should be considered.

Not included under this provision is information of a more private character, such as information based on personal acquaintance, friendship or observation that may be provided by members of a governing board or employees; information that could only be gathered through surveillance or from private sources; next-of-kin information and names of parents of students.

Subsection (c) authorizes the collection from another source if an act or its regulations state the information can be indirectly collected. This subsection also allows for the Information and Privacy Commissioner to authorize indirect collection.

> **16(2)(c)(i)** authorized or required under an Act of the Legislature or of Parliament, or

For example, the *Workers' Compensation Act* authorizes collection of medical information from a physician about an individual who was involved in a work-related accident.

> **16(2)(c)(ii)** approved by the commissioner under paragraph 111(1)(a) (after a request from the public body); or

Subsection (d) subject to subsection (3), the public body determines that the collection from another source is necessary for the purpose of

> **16(2)(d)(i)** collecting a debt or fine that is owing to the Government of Yukon or a public body from the individual,

This provision allows a public body to contact any person or organization, or to use publicly available information to assist in the collection of money owed to the public body or government. When public bodies face the problem of not being able to locate those owing money, or when they believe they would not obtain accurate information needed to collect the debt from the individual debtor, they are permitted to collect personal information from other sources.

This provision allows a representative of either the territorial government, as a whole, or any individual public body to contact any person or organization or to use publicly available information (e.g. on the Internet) that may be able to help in the collection of money owed to the public body or the government. This may include finding the home or work location or telephone number of the individual who owes money.

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 under an enactment.

> **16(2)(d)(ii)** making a payment to the individual from the Government of Yukon or a public body,

This provision allows a public body to contact any person or organization, or to use publicly available information to assist the public body to make a payment to the individual.

> **16(2)(d)(iii)** determining the individual's eligibility to receive a benefit from a program or activity of a public body, and the information is used only to process an application made by or on behalf of the individual,

This provision allows a public body to approach several different sources or information, other than the individual, to determine whether the individual is eligible to receive a benefit from a program or activity of a public body. This collection of information only takes place in the course of processing an application from the individual or from their representative.

For example, to verify their income for low-income housing or other income-tested program, or verify educational prerequisites for a post-secondary program.

It is good practice to inform the individual about whom information is being collected that information from a variety of sources will be collected to document that particular application. This collection of information can take place only in the course of processing an application from the individual, or from his or her representative.

Public bodies should not take the further step of asking an individual to authorize indirect collection unless they are prepared to change their procedures for determining eligibility, if an individual refuses to authorize the indirect collection.

Authorization from the individual is not necessary if the requirements of section 16(d)(iii) are fulfilled.

> **16(2)(d)(iv)** verifying the individual's eligibility to continue to receive a benefit from a program or activity of a public body,

This provision allows for cases where an individual has already qualified for a program, benefit, or service and the public body needs to check that the individual is still eligible.

Many programs operated by public bodies have eligibility criteria that must be met in order for an individual to participate in them or receive a benefit or service. This may require the public body to approach several different sources of information besides the individual to determine whether the criteria or qualifications are met. For example, a public body may perform random checks on the income and assets of individuals on social assistance or in low-income housing to verify that an individual remains eligible for the program and verification of educational prerequisites for a post-secondary program.

As with the previous provision, it is a good business practice to inform the individual about whom the information may be collected that verification of continuing eligibility may occur without notice. This is especially the case if the individual could incur any penalty for receiving a benefit for which he or she has become ineligible.

> **16(2)(d)(v)** determining the individual's eligibility to receive an honour or award, including a scholarship, bursary or honorary degree,

This provision allows a public body to seek references and other relevant personal information about an individual being considered for an honour or award such as honorary degrees, scholarships, prizes and bursaries.

The nature of some awards is such that the potential recipients do not have to apply for the award and may not be aware that they are being considered. Scholarships and bursaries are often awarded on the basis of academic achievement and recommendations by faculty members. Honorary degrees are usually awarded in recognition of a person's contribution to a community or sector of society. Prizes may be awarded on the basis of athletic or scholastic achievements.

Any information collected should be *directly related* to the criteria for granting the honour or award. As a best practice, public bodies should develop criteria for an award in advance of the collection of personal information and make those criteria publically available. Once the individual has been informed about the honour or award, his or her personal information should only be disclosed with consent, unless another exception for disclosure applies.

> **16(2)(d)(vi)** administering a program or plan for the benefit or management of employees of the Government of Yukon or a public body,

This provision permits Government of Yukon as an employer, to indirectly collect information in managing human resources such as managing salaries, benefits, leave management and training and development. It allows government departments (ministerial public bodies) to collect personal information about an employee or prospective employee from other departments for the purpose of managing or administering personnel of Government of Yukon.

Management of personnel refers to aspects of the management of human resources of a public body that relate to the duties and responsibilities of employees. This includes staffing requirements, job classification or compensation, recruitment and selection, salary, benefits, hours and conditions of work, leave management, performance review, training and development, occupational health and safety, and separation and layoff. For Government of Yukon, the term includes the government-wide network managed through the Public Service Commission (PSC). It *does not* include the management of consultant, professional or independent contractor contracts.

Administration of personnel comprises all aspects of a public body's internal management, other than personnel management, necessary to support the delivery of programs and services. Administration includes business planning, financial, material, contracts, property, information, and risk management.

This provision also allows public bodies to collect information about employees or prospective employees from third parties. Any collection under this provision **must** be for the purpose of management or administration of the personnel of the public body collecting the information. Employees should be informed in a general way as to how personnel information about them is collected and from what sources they can expect this information to be derived. They should also be aware of the purposes for which various types of information are used and of their rights under the Act.

Examples include: the collection of references for prospective employees, determination of qualifications, performance for secondment, training opportunities and the provision of pay and benefit services by one public body for other public bodies.

This provision refers to official personnel activities and does not permit the collection of personnel-related information by individual officials for purposes other than official duties relating to the management and administration of personnel within a public body.

The indirect collection authorized in this provision does not apply to other internal activities of public bodies, such as Corporate Challenge events and United Way campaigns. Personal information of employees not related to managing or administering personnel should be collected directly from the individuals in compliance with notification provisions in **section 17**.

> **16(2)(d)(vii)** supervising or disciplining an employee (other than a service provider) of a public body or terminating an employment relationship between an employee (other than a service provider) and a public body,

This provision permits Government of Yukon, as an employer, to indirectly collect information in managing employees' performance. If information is indirectly collected, employees are required to be notified in accordance with **section 17(4)**.

16(2)(d)(viii) providing legal services to the Government of Yukon or a public body,

This provision allows lawyers representing Government of Yukon to collect information required in providing legal advice. The information may be required for day-to-day provision of legal services, or in preparation for a proceeding before a court or tribunal. It may be desirable for legal enquiries be made in confidence., The individual concerned may not be able to provide the required information. In these circumstances the public body's legal representatives, or others providing legal services, can collect information indirectly, or ask an employee to do so on their behalf.

16(2)(d)(ix) an existing or anticipated proceeding to which the Government of Yukon or a public body is, or is expected to be, a party

This provision allows lawyers representing Government of Yukon to collect information required in preparation for a proceeding.

"PROCEEDING" means (a) in respect of a court, a civil or criminal proceeding, or (b) in respect of an adjudicator, the hearing of a matter over which the adjudicator is authorized under an Act of the Legislature or of Parliament to preside.

This definition sets out the 2 different types of proceedings that are relevant to the scope of this Act. Paragraph (a) refers to judicial proceedings and paragraph (b) covers what is commonly referred to as quasi-judicial proceedings (proceedings conducted by an adjudicator in accordance with their power to do so under an act).

16(2)(d)(x) a law enforcement matter,

This provision allows the indirect collection for law enforcement activities. The law enforcement body must ensure that there is specific authority to investigate and that the investigation could lead to a penalty or sanction imposed under a statute or regulation.

"LAW ENFORCEMENT" means (a) policing, including criminal or security intelligence operations, (b) a police, security intelligence, criminal or regulatory investigation, including the complaint that initiates the investigation, that leads or could lead to a penalty or sanction being imposed, or (c) a proceeding that leads or could lead to a penalty or sanction being imposed.

During an investigation, a substantial portion of personal information about the individual under investigation is collected from other sources. Reasons for this include the fact that investigators may not wish to alert the individual concerned that an investigation is taking place, the individual would not provide accurate information, or the individual might alter or destroy evidence.

Disclosure of personal information by private-sector organizations in Yukon is governed by the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*.

Law enforcement bodies should not collect excessive amounts of personal information. One of the situations where this is likely to occur is in the use of surveillance. Visit the ATIPP website on Yukon.ca for more information on disclosure of video surveillance to law enforcement.

> **16(2)(d)(xi)** placing an individual into the custody, or under the supervision, of an employee of a correctional facility, penal facility or other similar type of custodial institution,

This provision permits correctional authorities to seek out information, using a variety of sources, about an individual under their control or supervision.

> **16(2)(d)(xii)** making a decision in respect of the provision of health care to an individual who is lawfully detained in a correctional facility, penal facility or other similar type of custodial institution,

This provision permits correctional authorities to seek out information, using a variety of sources, about an individual under their control or supervision, including the collection of health information to provide health care.

> **16(2)(d)(xiii)** preventing or reducing a serious threat to public health or safety, or protecting the health or safety of an individual,

This provision allows the collection of information to prevent and protect the health and safety of an individual. This authority can be used in the event of a civil emergency or to receive information about a client, if they could pose a significant risk to the health and safety of staff.

For more on emergencies, see the ATIPP website on Yukon.ca for guidance on privacy during an emergency.

This provision allows emergency services personnel, as well as other employees of a public body, to collect information needed to deal with an emergency situation. This can happen when

- the individual is not able to provide the information directly; or
- direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person.

Examples of such emergency situations include cases were an injured person is not able to respond to questions about medication or an accident or fire situation when a delay in collecting information about a person's actions could result in death or severe complications. Under this provision, a public body can collect indirectly only the information required to deal with the emergency (minimum amount necessary).

> **16(2)(d)(xiv)** enforcing a maintenance order under the *Maintenance Enforcement Act* to which the individual is subject,

This provision permits a public body to collect personal information for the purpose of enforcing maintenance orders. Section 6 of the *Maintenance Enforcement Act* authorizes the Director or designate to collect specific types of information for the purposes of enforcement. Only the specific information listed in the Act can be disclosed to the Director or designate by a public body.

> **16(2)(d)(xv)** facilitating the sheriff's performance of a service under the *Judicature Act* for a public body in respect of a process, writ, warrant or other similar type of document in which the individual is named,

This provision allows the Sheriff's Office to collect information required to serve legal documents under the *Judicature Act*.

> **16(2)(d)(xvi)** providing a specialized service to the individual in respect of which the public body is the personal identity manager or a partner,

This provision allows for the collection of information by a partner agency if they are participating in an approved integrated service (see **section 27**) or an approved personal identity service (see **section 28**).

> **16(2)(d)(xvii)** carrying out a data-linking activity in respect of which the public body is a partner, or

This provision allows for the collection of information to fulfill an approved data-linking activity in accordance with **section 29**.

> **16(2)(d)(xviii)** carrying out a specific research purpose, including a statistical research purpose, for which the personal information is used and disclosed only as non-identifying information.

This provision allows for the collection of identifiable information if the use and disclosure is non-identifiable. For example, providing identifiable information that is processed by a system that will remove the identifiers to allow for the data to be used in a manner that will not identify anyone.

Subsection 3 establishes criteria that a public body must consider when determining if it is necessary to collect information from another source (other than the individual). These criteria will help ensure that programs or activities are designed to collect information directly from individuals.

16(3) In determining under paragraph (2)(d) whether it is necessary to collect personal information from a source other than the individual whose information is to be collected, the public body must consider whether collection directly from the individual would

16(3)(a) defeat or prejudice the purpose of the collection;

16(3)(b) result in the collection of inaccurate personal information; or

16(3)(c) delay the public body,

16(3)(c)(i) in carrying out a program or activity for the benefit of the individual, or

16(3)(c)(ii) in providing a specialized service or benefit to the individual.

Subsection 4 clarifies that a program or activity must satisfy the rules established in **section 15** in order for a public body to indirectly collect personal information.

SECTION 17 - Notice of direct collection

This provision requires a public body to notify individuals when their personal information is collected directly by a public body and stipulates what information should be contained in the notice.

Public bodies should undertake a regular review of their collection documents to determine which ones require the inclusion of collection notices. Collection notices should be included on all print and electronic forms used to collect personal information directly.

Subsection 1 is a provision that sets out rules that a public body must follow when it is required to collect personal information directly from an individual. The notification requirement allows an individual to know the purpose of the collection of personal information and how the information will be used. It requires any pubic body that collects personal information directly from an individual to provide NOTICE OF DIRECT COLLECTION to the individual.

Examples of cases where collection of personal information requires notification under this provision include: collection of personal information for enrolment in a program, to receive a service or to apply for a benefit, collection of personal information on a client survey and collection of personal information on a course evaluation form.

> **17(1)** Subject to subsection (3), a public body that collects personal information directly from an individual must provide a notice to the individual in accordance with subsection (2).

Subsection 2 outlines that notifications may be given in many ways. For example:

- printed on a collection form;
- presented in a pop-up window linked to an online form;
- displayed on a notice hung on the wall or placed on a service counter; or
- given orally, for example, during a phone call.

Regardless of the manner in which notification is provided, all three parts of the notice must be provided to the individual.

The notice should be provided at the time that the personal information is being collected, before it is collected.

For example, notice should be given to individuals at the beginning of an interview when an individual is being asked to provide his or her own personal information. If the interview is being recorded, it is good practice to record the notice at the beginning of the tape.

When a notification is given orally, either in person or over the telephone, it is a good practice to refer the individual to a written copy of the notice or to provide a printed copy either at the counter or later by mail, and to retain a record that the notice was given. When individuals are applying for and participating in extensive and complementary programs, it may be convenient and effective to place a notice explaining all collections of personal information relating to the programs in a publication about the programs, or to explain orally.

> **17(2)** A notice to an individual under subsection (1) must specify:
>
> **17(2)(a)** the purpose of the collection of their personal information;
>
> **17(2)(b)** the business contact information of the employee of the public body who is responsible for answering the individual's questions about the collection; and
>
> **17(2)(c)** the public body's legal authority for the collection.

The purpose of a collection means the reason(s) the information is needed and the use(s) that the public body will make of the personal information. The legal authority for collection may be a specific provision in an enactment of Yukon or Canada that expressly authorizes collection of the personal information, or **section 15(c)(i)** of the ATIPP Act, which authorizes collection of personal information that is *directly related to and necessary for* operating program of a public body.

The notice should be given at the time that the personal information is being collected. The individual should be able to decide whether or not to provide their personal information, before the collection occurs and understand the how services may be impacted or not provided in the event they refuse to provide personal information.

If a public body relies on **section 15(c)(i)** of the *ATIPP Act*, it is important to also provide the authority for the program for which the personal information is being collected. The program itself may be authorized by a Yukon or Federal Act, or a regulation under an act, or legal resolution of a public body establishing a program that falls within its mandate under an act.

Identifying someone to answer the individual's questions about the collection is intended to provide the individual with a knowledgeable source of information. The person cited should be familiar with the program, and be able to explain why the personal information is being collected and how it will be used by, and disclosed to, other bodies.

Examples of cases where collection of personal information requires notification under this provision include: collection of personal information for enrolment in a program, to receive a service or to apply for a benefit, collection of personal information on a client survey and collection of individually identifying information on a course evaluation form.

When collection of personal information is carried out by one public body for or on behalf of another public body, this must be done under a written agreement. The agreement should state the reasons for collecting information through an agent, the specific authority for the collection, and the purposes for which the personal information will be used or disclosed. Any use or disclosure of the personal information must be authorized under the ATIPP Act.

Where a public body would be permitted to collect personal information indirectly but chooses to collect directly from the individual the information is about, notification is still mandatory, even if it would not be required had the public body collected the information indirectly.

For assistance with creating a collection notice, see the ATIPP Office document: Collection Notice Checklist.

Subsection 3 provides that the requirements for collecting personal information directly and giving notice may be set aside if, in the opinion of the head of the public body, compliance with these provisions could reasonably be expected to result in the collection of information that would not be accurate or would prejudice the collection.

> **17(3)** A public body is not required to provide a notice under subsection (1) if
>
> **17(3)(a)** subject to subsection (4), the public body is authorized to collect personal information from a source other than the individual in accordance with subsection 16(2);

17(3)(b) the purpose of the collection relates to a law enforcement matter; or

17(3)(c) the head of the public body is satisfied that providing the notice would

17(3)(c)(ii) defeat or prejudice the purpose of the collection, or

17(3)(c)(ii) result in the collection of inaccurate information.

Subsection 3 provides that the requirements for collecting personal information directly and giving notice may be set aside if, in the opinion of the head of the public body, compliance with these provisions could reasonably be expected to result in the collection of inaccurate information. This provision should be used only in limited circumstances within programs, and public bodies should maintain documentation of when the provision has been used and the reasons for using it.

Inaccurate information is incorrect, incomplete or misleading information. This provision recognizes that in certain limited circumstances, such as the conduct of some surveys seeking opinions and in some psychological testing, there may be difficulty in getting accurate information if individuals are informed in advance of the reasons for the collection. In some cases, notifying individuals of the purpose of a survey would lead to responses that would distort the results.

Subsection 4 requires a public body to notify an affected employee if their personal information is being indirectly collected for the purpose of discipline or termination. The head of the public body has the discretion not to provide notice if the head is satisfied that it would compromise information or the specific matter.

17(4) A public body that collects personal information about an employee for a purpose described in subparagraph 16(2)(d)(vii) must provide a notice to the employee about the collection that contains the information described in subsection (2), unless the head of the public body is satisfied that by providing the notice

17(4)(a) the availability or accuracy of the personal information would be compromised; or

17(4)(b) a matter relating to the supervision, discipline or termination of the employee would be compromised.

When electing to use this discretionary provision, heads should ensure that they are documenting their decision.

SECTION 18 Personal information received by public body without request

This section describes when unwanted personal information is received by the public body. For example, the public body receives personal information without requesting it, and or the personal information does not relate to the program or activity administered by the public body.

> **18(1)** A public body is not considered to have collected an individual's personal information if:
>
> **18(1)(a)** the public body receives personal information without having requested it
>
> **18(1)(b)** the personal information does not relate to a program or activity of the public body
>
> **18(1)(c)** the public body takes no action in respect of the personal information except to review all or part of it and
>
> **18(1)(c)(i)** dispose of it in accordance with the regulations;
>
> **18(1)(c)(ii)** return it to the sender, or;
>
> **18(1)(c)(iii)** redirect it in accordance with subsection (2)

Subsection 1 clarifies that any unsolicited information that is sent to a public body is not considered to have been collected; therefore, the rules of the Act do not apply to this information.

This provision is required as public bodies can only collect information if it is *necessary*. If a public body collects information that is not necessary, this is considered an 'unauthorized collection' of personal information that is prohibited under **section 12**.

Subsection 2 outlines how a public body that receives any unsolicited information, is obligated to take action in respect of it by, returning it; forwarding it to where it was intended; or destroying it.

For more information on disposing of information, see the ATIPP Regulations.

> **18(2)** If, after review of all or a part of the personal information referred to in subsection (1), the public body determines that the personal information relates to a program or activity, or a specialized service or data-linking activity, of another public body, the public body may redirect the personal information to the other public body.
>
> **18(3)** For greater certainty upon receiving unsolicited personal information and redirecting it:
>
> **18(3)(a)** a public body that receives personal information in accordance with paragraphs (1)(a) and (b) is not considered to have collected the personal information; and

18(3)(b) a redirection under subsection (2) is not considered to be a use or disclosure of personal information.

DIVISION 4 – Use of Personal Information

SECTION 19 Prohibition- Use

This section of the Act lists the only circumstances under which a public body **must not** use personal information. This section also defines how a public body may use personal information only for the purpose for which the information was collected, compiled or for a use consistent with that purpose.

"USE", in respect to personal information, includes accessing, adapting, compiling, copying, modifying, organizing or reviewing the personal information but does not include collecting, disclosing or managing the personal information.

The PURPOSE means the purpose for which the information was collected under **section 19**. A public body can use the information for that purpose. Typical purposes include the administration of a particular program, the delivery of a service and other directly related activities. A public body may make use of personal information it has gathered, created or manipulated for the specific purposes for which it is permitted to collect or compile it.

A CONSISTENT PURPOSE is one that has a reasonable and direct connection to the original purpose and is necessary for performing the statutory duties of, or for operating a legally authorized program of the public body that uses the information.

CONSISTENT USE is a use that has a reasonable and direct connection to the original purpose of collection and that is necessary for performing the statutory duties of the public body.

> **19** A public body must not use personal information
>
> **19(a)** except as provided under this Division;
>
> **19(b)** beyond the amount that is reasonably necessary for the public body to carry out the purpose to which the use relates; and
>
> **19(c)** subject to paragraph 22(b), for longer than the period of time that is reasonably necessary to carry out the purpose to which the use relates.

This provision prohibits a public body from using personal information other than as authorized under this Part of the Act. As part of this prohibition, the public body must also ensure that it limits its use of personal information to only the minimum amount necessary to fulfill the purpose for its collection.

SECTION 20 Employee to report suspected unauthorized use

This provision requires employees to report suspected unauthorized uses of personal information as a privacy breach to their public body's privacy officer. The *Act* requires public bodies to implement security measures designed to prevent privacy breaches in respect of the personal information that they hold.

"DESIGNATED PRIVACY OFFICER", of a public body, means the employee designated under paragraph 87(1)(a) as a designated access officer for the public body.

"HOLD", in respect of information, means to have custody or control of the information.

"USE", in respect of personal information, includes accessing, adapting, compiling, copying, modifying, organizing or reviewing the personal information but does not include collecting, disclosing or managing the personal information.

> **20** For greater certainty, if an employee of a public body reasonably believes that an unauthorized use of personal information held by the public body has occurred or is occurring, the employee must, without delay, report the suspected unauthorized use as a privacy breach in accordance with section 31.

"PRIVACY BREACH", in respect of personal information, means the theft or loss of, or unauthorized use, disclosure or disposal of, the personal information.

SECURITY refers to protecting or guarding the personal information from unauthorized access or disclosure, theft or other danger. Security includes administrative, physical and technology measures. These may require locked filing cabinets, computer controls and access codes, restricted work areas, and encryption or encoding of data, depending on the sensitivity of classification of the information involved and the threat and/or risk associated with it.

Section 38 of the *Act* requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction in accordance with ATIPP Regulations. Reasonable security arrangements may also include security policies**.** Please see the ATIPP Regulations for more information.

SECTION 21 Use only if authorized

This section of the *Act* lists the only circumstances under which a public body may use personal information.

The purpose of collection is described in the collection statement provided to the individual when the information is collected directly (see **section 17**). When the information is not

collected directly, or when it is compiled from several sources, the purpose should be stated in the written policy or procedure dealing with the program.

> **21** A public body may use the personal information of an individual that it collects under Division 3 only if
>
> **21(a)** the use is for the purpose for which the personal information was collected;
>
> **21(b)(ii)** is necessary for the public body to carry out a program or activity, or to perform a statutory duty;

These provisions can be cited for the disclosure in the event that a public body would not be able to carry out its program without the use of the information.

> **21(c)** the use is for the purpose for which the personal information was disclosed under section 25 or 26 by another public body or partner agency to the public body;

This provision allows for the disclosure of information only if authorized or for research purposes.

> **21(d)** the use is necessary for the public body
>
> **21(d)(i)** to prevent or reduce a serious threat to public health or safety, or
>
> **21(d)(ii)** to protect the health or safety of an individual; or

Subsection (d) allows for a public body to disclose information to prevent and protect the health of an individual or public. This authority can be used in the event of a civil emergency or to inform staff about a client that could pose a significant risk to their health and safety.

> **21(e)** the individual consents, in the prescribed manner, to the use of their personal information for a purpose other than the purpose for which it was collected.

Subsection (e) allows for a public body to use an individual's personal information, provided the individual has consented in accordance with ATIPP Regulations. Please see the ATIPP Regulations for more information.**SECTION 22 Accuracy and retention of personal information used for decision-making**

This section of the Act states that if a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must make every reasonable effort to ensure that the information is accurate and complete. Public bodies are also required to retain the personal information for <u>at least one year</u> after using it so that the individual has an opportunity to obtain access to it. This provision cannot be used by a public body to dispose or

destroy records in the absence of a Records Schedule, or to override a disposition time limit in an existing schedule. (See section 2 of the Archives Act)

> **22** If a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must
>
> **22(a)** before making the decision, take reasonable measures to ensure that the personal information is accurate and complete; and
>
> **22(b)** retain the personal information in a manner that ensures that the individual may, for at least one year after the decision is made, access the information used by the public body to make the decision.

A decision that directly affects the individual is one that has an impact on an individual's life or affects their 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.

Examples of decisions that directly affect an individual include:

- a determination as to whether or not someone is entitled to income assistance or a student loan,
- a decision on hiring an individual or on admission to a course or program, and
- a determination regarding eligibility for subsidized housing or library services.

A public body makes every reasonable effort to identify practicable means to ensure that personal information used to make a particular decision affecting the individual is accurate and complete.

ACCURATE means careful, precise, lacking errors.

COMPLETE means including every necessary item or element; without omissions or deficiencies; not lacking in any element or particular. Personal information is complete when all the information necessary to make the decision, and only the information that will be used for that purpose, is collected.

Generally, if a public body collects personal information directly, it is likely to meet the requirement of making every reasonable effort to ensure that information is accurate and complete. This is especially so if the individual has signed a statement indicating that the information is accurate and complete. However, the burden of making every reasonable effort is higher when the consequences of a decision are greater.

Public bodies should have adequate procedures in place to properly verify the accuracy and completeness of any personal information crucial to an application, transaction or action at the time the information is provided.

Programs that use personal information systems for delivery of programs should embed systematic processes for updating personal information that is used on a regular or continuous basis. Other methods of maintaining accuracy include:

- periodically auditing files with accuracy and completeness as one of the criteria tested;
- ensuring limited access to information for the purpose of making corrections; and
- establishing cross-referencing and validation checks within the software of automated systems that identify anomalies in data.

Privacy requirements should be integrated into routine information and systems operations for the program as a whole. Maintaining ongoing accuracy will be more challenging for programs that involve a lengthy review or approval process or an ongoing relationship with an individual. The accuracy requirements of the Act should be considered in the management of programs of this kind.

This provision also requires public bodies to retain personal information for **at least one year** after using it to make a decision that affects an individual, so that the individual has a reasonable opportunity to obtain access to it.

This retention requirement is intended to permit individuals to review and request correction of information about them before disposition (transfer to Yukon Archives or destruction) of that information takes place. It is not necessary to retain personal information when no decision will be or has been made about the individual. This retention requirement only applies to personal information that is required for decision-making purposes.

NOTE: Ministerial public bodies are only authorized to dispose or destroy information once it meets the disposition under a Records Schedule as approved by the Territorial Archivist under the *Archives Act*.

RETAIN means to maintain custody or control of the personal information. **Subsection 22(b)** does not prevent public bodies from storing personal information in another location, such as the Corporate Records Centre, if the public body can retrieve the personal information in response to a request for access to it.

PART 2

DIVISION 5 – DISCLOSURE OF PERSONAL INFORMATION

SECTION 23 Prohibition-Disclosure

This section of the Act lists the only circumstances under which public bodies may disclose personal information. Disclosure of personal information may occur only in the specific circumstances outlined in section 23. Public bodies should look at the circumstances surrounding each request and the privacy protection objectives of the Act when deciding whether to disclose personal information. Disclosure should be limited to only the minimum amount necessary to fulfil the purpose for its disclosure.

"DISCLOSURE" of information, includes revealing or otherwise making the information known to a person other than the person who holds the information but does not include the collection, use or management of the information.

> **23** A public body must not disclose personal information
>
> **23(a)** except as provided under this Division; and
>
> **23(b)** beyond the amount that is reasonably necessary to carry out the purpose for the disclosure.

This provision prohibits a public body from disclosing personal information other than as authorized under this Part of the Act. As part of this prohibition the public body must also ensure that it limits its disclosure of personal information to only the minimum amount necessary to fulfill the purpose for its disclosure.

SECTION 24 Employee to report suspected unauthorized disclosure

This provision requires employees to report suspected unauthorized disclosures of personal information as a privacy breach to the Designated Privacy Officer for the public body.

UNAUTHORIZED DISCLOSURE of personal information means disclosure of, production of or the provision of access to personal information to which this Act applies, if that disclosure, production or access is not authorized by this Act.

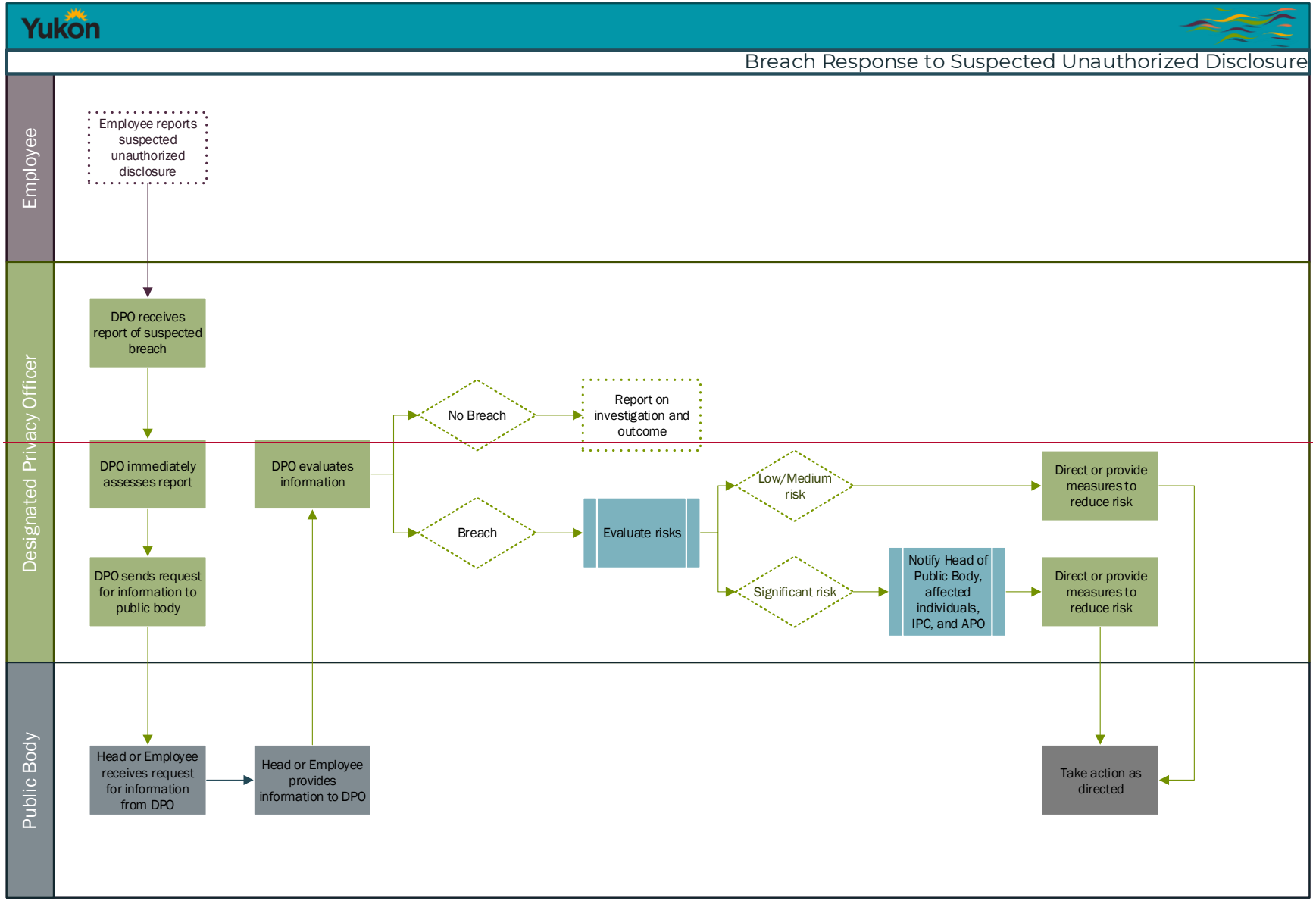
The ATIPP Act states that public bodies must have appropriate administrative controls in place to ensure that personal information is disclosed only to authorized persons. When developing a new program, activity or service, public bodies should consider whether personal information will need to be disclosed, and ensure the disclosure is authorized under the Act. Public bodies should also regularly review their disclosure policies and practices to ensure that they continue

to meet the requirements of the Act. Where it is found that disclosures are not authorized, practices should be altered to meet legal requirements or discontinued.

> **24** For greater certainty, if an employee of a public body reasonably believes that an unauthorized disclosure of personal information held by the public body has occurred or is occurring, the employee must, without delay, report the suspected unauthorized disclosure as a privacy breach in accordance with section 31.

Privacy tools such as Personal Information Maps (PIM) and Privacy Impact Assessments (PIA) can assist Designated Privacy Officers to assess whether a breach has occurred due to unauthorized disclosure.

~~FIGURE 5.1 Unauthorized Disclosure~~



SECTION 25 Disclosure only if authorized

This section clearly identifies the circumstances for which a public body may disclose personal information of an individual.

> **Section 25** A public body may disclose the personal information of an individual that it collects under Division 3 only if
>
> **25(a)** the disclosure is for the purpose for which the personal information was collected;
>
> **25(b)** the disclosure is of a type described in paragraph 70(4)(c), (d) or (e);

This provision details all the types of disclosure of a third party's personal information that is not considered to be an unreasonable invasion of the third party's personal information:

- A disclosure to which the third party consents in writing;
- The disclosure of information of a type of information referred to in paragraph 25(g);
- The disclosure is for a use that is directly connected to the purpose for which the personal information was collected, and is necessary for the following: A public body to carry out a program or activity, or a public body or partner agency to perform a statutory duty.

> **25(c)** the disclosure is for a use that
>
> **25(c)(i)** is directly connected to the purpose for which the personal information was collected, and
>
> **25(c)(ii)** is necessary for
>
> **25(c)(ii)(A)** a public body to carry out a program or activity, or
>
> **25(c)(ii)(B)** a public body or partner agency to perform a statutory duty;
>
> **25(d)** the individual consents, in the prescribed manner, to the disclosure of their personal information for a purpose other than the purpose for which it was collected;

Subsection (d) permits disclosure of an individual's personal information when the individual has identified the information and consented, in the manner prescribed in ATIPP Regulations, to the disclosure. Please see the ATIPP Regulations for more information.

As a best practice and where appropriate, a form or other document requesting consent should: indicate the original purpose of the collection and how the information is to be used and for which consent is being provided. The notice should indicate:

- Consent is voluntary and may be revoked,
- Any limitations, consequences or implications that may result from revocation (consequences that may result from refusal to consent),
- The time period during which the consent remains valid.

Examples of consent to disclosure include:

- Consent to have references provided in support of job applications;
- Consent to provide information to the Canada Revenue Agency in order to obtain income verification from that source; and
- Consent to the use of photographs for promotional purposes.

When an individual copies (carbon copy or "cc"s) other parties on a letter or e-mail, this is not consent for the responder to disclose personal information to the parties who were copied.

When the person concerned has not indicated any consent to disclose of their personal information, and no other provision exists to permit disclosure, public bodies cannot disclose the information. A public body must not penalize the individual by denying the benefit or service for which the personal information was originally collected.

Note: Consent to a disclosure may be given by a representative acting on behalf of an individual in accordance with the conditions set out in **section 118**.

> **25(e)** the disclosure is in accordance with
>
> **25(e)(i)** a provision of an enactment (other than this Act) that authorizes or requires the disclosure,
>
> **25(e)(ii)** a provision of an Act of Parliament, or a provision of a regulation made under such an Act, that authorizes or requires the disclosure,
>
> **25(e)(iii)** an arrangement or agreement that

Disclosure to **comply with an enactment of Yukon or Canada** means disclosure of personal information as *required* by either territorial or federal legislation. There must be a direct relationship between complying with the enactment and the disclosure of the personal information.

Disclosure to **comply with a treaty, arrangement, or agreement made under an enactment** of Yukon or Canada means disclosure of personal information as *required* by the treaty, arrangement or agreement. The enactment must provide authority for the provision in the treaty, arrangement or agreement, and that provision must specifically authorize disclosure of the personal information.

Public bodies should maintain a list of all agreements, arrangements and treaties, as applicable, under which they disclose personal information using a Personal Information Map (PIM). Public bodies should include information disclosed under agreements, arrangements and treaties in the relevant Personal Information Map.

> **25(e)(iii)(A)** is authorized to be made or entered into under an Act of the Legislature (other than this Act) or of Parliament, and
>
> **25(e)(iii)(B)** authorizes or requires the disclosure, or

Under these provisions, disclosure is permitted if it is either required or authorized by an enactment of Yukon or Canada. If disclosure of personal information is authorized – but not required – by an enactment, the head of the public body has more discretion as to whether or not to disclose the information.

If a public body is relying upon section 25(e)(iii)(A)-(B) as authority to disclose personal information, it must ensure that the disclosure is strictly in compliance with the enactment that authorizes the disclosure.

Some acts require other bodies to disclose personal information to a particular public body for the purposes of the (collecting) public body's program. For example, an act may compel a public body that has possession of personal, financial or health-related information about a client or potential client to provide that information or record to another public body to carry out a task, duty or function relating directly to the client or potential client.

Before disclosing personal information under section 25(e)(iii)(A)-(B) 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.

> **25(iv)** section 26 or Part 3;

See **section 26** Information used for research purpose or **Chapter 3** for Part 3, Access to Information.

> **25(f)** the head of the public body is satisfied that the disclosure is necessary to prevent or reduce a serious threat to public health or safety, or to protect the health or safety of an individual;
>
> **25(g)** the personal information being disclosed
>
> **25(g)(i)** is about the physical or mental health of an individual who has been deceased for more than 50 years,
>
> **25(g)(ii)** is the personal information of an individual who has been deceased for more than 25 years, other than information about their physical or mental health,

25(g)(iii) is contained in a record that has been in existence for 100 years or more, or

25(g)(iv) is publicly available information;

25(h) the disclosure

25(h)(i) is to the individual,

Subsection 25(h)(i) allows disclosure to the individual and identifies specific authorities to whom information can be disclosed. This is required as it allows information to be disclosed without requiring an individual to put in an access request for their information.

25(h)(ii) is to the archivist appointed under the *Archives Act* for the purpose of the performance of their duties under that Act,

Subsection 25(h)(ii) allows disclosure to the archivists for the purpose of administration of the Yukon Archives.

25(h)(iii) is for the Attorney General for their use

25(h)(iii)(A) in a proceeding to which the Attorney General or a public body is a party, or

Subsection 25(h)(iii) allows disclosure to be used in a proceeding involving the Attorney General or a public body.

"ATTORNEY GENERAL" means the minister who is the Attorney General of Yukon under section 3 of the Department of Justice Act and includes a lawyer, agent or delegate acting for or on behalf of the Attorney General. (See **section 1** definitions.)

"PROCEEDING" is defined as a court, civil or criminal proceeding; or a hearing by an adjudicator as authorized under an Act of the Legislature or Parliament. (See **section 1** definitions.)

25(h)(iii)(B) in providing legal services to a public body,

This provision allows disclosure when a public body is seeking legal advice.

25(h)(iv) is to an auditor for the purposes of an audit authorized or required under an Act of the Legislature or of Parliament,

This provision allows disclosure to an auditor to perform an audit.

"AUDITOR" means (a) the individual appointed by Parliament as the Auditor General of Canada, (b) the individual appointed under the Financial Administration Act as the internal auditor, or (c) any other person prescribed as an auditor.

> **25(h)(v)** is to the chief medical officer of health, a medical officer of health or a health officer appointed under the *Public Health and Safety Act* for the purpose of the performance of their duties under that Act,

This provision allows disclosure to the Chief Medical Officer of Health to fulfill its mandate.

Note that section 2.1(2) of the *Public Health and Safety Act*, states **subsection 17(1)** of the *ATIPP Act* does not apply to personal information collected by the Minister or the chief medical officer of health *if the information is collected during and in relation to a health emergency*, and if at the time of the collection it would be unreasonable in all of the circumstances to require the Minister or the chief medical officer of health to comply with subsection 17(1). In order to utilize this clause, a health emergency must be declared through an order issued under the Act, and collection notification must be weighed at the time of collection.

> **25(h)(vi)** is to a coroner appointed under the *Coroners Act* for the purpose of the performance of their duties under that Act,

This provision allows disclosure to the Coroner to fulfill its mandate under the *Coroners Act*.

> **25(h)(vii)** is to the Public Guardian and Trustee appointed under the Public Guardian and Trustee Act for the purpose of the performance of their duties under that Act,

This provision allows disclosure to the Public Guardian and Trustee to fulfill its mandate under the *Public Guardian and Trustee Act*.

> **25(h)(viii)** is to the Director of Statistics designated under the *Statistics Act* for the purpose of the performance of their duties under that Act,

This provision allows disclosure to the Director of Statistics to fulfill its mandate under the *Statistics Act*.

> **25(h)(ix)** is to an employee of a correctional facility, penal facility or other similar type of custodial institution in which the individual is lawfully detained, for the purpose of
>
> **25(h)(ix)(A)** placing the individual into the custody of the employee,
>
> **25(h)(ix)(B)** supervising the individual within the facility or institution,
>
> **25(h)(ix)(C)** making a decision in respect of the provision of health care to the individual while they are lawfully detained, or
>
> **25(h)(ix)(D)** the release, conditional release, discharge or conditional discharge of the individual from custody in accordance with an Act of the Legislature or of Parliament,

These provisions allow disclosure about an inmate to the correctional institution in specific circumstances such as supervision and/or health care purposes.

> **25(h)(x)** is to an employee, officer or director of a professional or occupational regulatory body for the purpose of a licensing, registration, insurance or disciplinary matter to which the individual is subject,

This provision allows disclosure of information to a regulatory body which has jurisdiction over specific matters listed. An example would be disclosing employment-related information about a nurse working for the Department of Justice (ministerial public body) and in respect of who the Yukon Registered Nurses Association require information to investigate. However, like the other disclosure provisions, this is discretionary and the Department of Justice has control over how much information would be disclosed, if any.

> **25(h)(xi)** is to a public body or law enforcement agency in Canada to assist in an investigation
>
> **25(h)(xi)(A)** undertaken with a view to a law enforcement proceeding, or
>
> **25(h)(xi)(B)** from which a law enforcement proceeding is likely to result,

These provisions allow disclosure for a law enforcement proceeding, including a proceeding that reasonably may occur. **"PROCEEDING"** is defined as a court, civil or criminal proceeding; or a hearing by an adjudicator as authorized under an Act of the Legislature or Parliament. (See **section 1** definitions.)

> **25(h)(xii)** is made by a public body that is a law enforcement agency

These provisions allow disclosure from a law enforcement agency to another law enforcement agency in Canada or another country.

> **25(h)(xii)(A)** to another law enforcement agency in Canada, or
>
> **25(h)(xii)(B)** to a law enforcement agency in a foreign country under an arrangement, an agreement, a treaty or legislative authority,
>
> **25(h)(xiii)** is to another public body for the purpose of carrying out a specific research purpose, including a statistical research purpose, for which the personal information is used only as non-identifying information,

This provision allows the disclosure of personal information if it will be used to make non-identifiable information. This will enable the government to perform data analysis or analytics with non-identifiable information.

> **25(h)(xiv)** is to the head or an employee of the public body and is necessary for the performance of the duties of the head or the employee, or

Subsection 25(h)(xiv) allows disclosure to the head or employee of the public body of information that is necessary to perform a duty.

NOTE: This disclosure can only be within the public body, not between public bodies.

The persons to whom the information is disclosed should be able to prove a need to know, or handle the personal information in order to do their jobs. The following are some examples of cases where disclosure might be necessary for the performance of an employee's duties.

- Human Resources may require access to the résumés of applicants in order to carry out the recruitment function
- Where there is a formal process within a public body to do so, an employee may need to report non-compliance (e.g. an alleged contravention of the Government of Yukon's Oath of Office and Oath of Allegiance - codes of conduct and ethics).
- Service counter staff may need to be informed if a client has a history of acting violently when interacting with departmental staff and if there is a need for extra security when the individual approaches the office.
- A counsellor may require access to student records to provide assistance, at the request of a teacher, to a student who is not doing well in school.
- The head of a local public body may require information to prepare a report for the governing body.
- A Minister may need background information about an issue and the people he or she is meeting with in order to understand the problem and their needs.

25(h)(xv) is to the commissioner; or

This provision allows disclosure to the Information and Privacy Commissioner (IPC). Information could be disclosed during an investigation, own motion investigation or an audit (for example, the Commissioner can audit the identity management service **in section 28**).

25(i) the disclosure is for the purpose of

25(i)(i) collecting a debt or fine owing to the Government of Yukon or a public body from the individual,

This provision allows a public body to disclose personal information to assist in the collection of money owed to the public body or the government.

25(i)(ii) making a payment to the individual from the Government of Yukon or a public body,

This provision allows a public body to disclose personal information to assist in making a payment to an individual.

25(i)(iii) determining the individual's eligibility to receive a benefit from a program or activity of a public body, and the information is used only to process an application made by or on behalf of the individual,

This provision allows a public body to disclose information to assist another public body assess whether an individual meets eligibility criteria. This disclosure of information can only take place in the course of the other public body processing an application from the individual, or from his or her representative. For example, a public body may verify the income for low-income housing or other income-tested programs and verify educational prerequisites for a post-secondary program.

> **25(i)(iv)** verifying the individual's eligibility to continue to receive a benefit from a program or activity of a public body,

This provision allows for cases where an individual has already qualified for a program, benefit, or service and another public body needs to check that the individual is still eligible. For example, a public body may perform random checks on the income and assets of individuals on social assistance or in low-income housing to verify that an individual remains eligible for the program.

> **25(i)(v)** determining the individual's eligibility to receive an honour or award, including a scholarship, bursary or honorary degree,

This provision allows disclosure to another public body seeking references and other relevant personal information about someone being considered for an honour or award such as honorary degrees, scholarships, prizes and bursaries.

> **25(i)(vi)** if the individual is injured or ill, contacting a relative of the individual or any other person whom it would be reasonable to contact in the circumstances,

This provision allows a public body to contact an individual in the event of a serious injury or illness.

> **25(i)(vii)** informing a representative or relative of a deceased individual, or any other person whom it would be reasonable to inform in the circumstances, of the individual's death,

This provision allows a public body to contact an individual in the event of a death.

> **25(i)(viii)** identifying a deceased individual,

This provision allows disclosure to identify a deceased individual.

> **25(i)(ix)** administering a program or plan for the benefit or management of employees of the Government of Yukon or a public body,

This provision permits the Government of Yukon, acting in an employment capacity, to disclose information in the management of human resources.

Examples include managing salaries, benefits, leave management, and training and development.

> **25(i)(x)** supervising or disciplining an employee (other than a service provider) of a public body or terminating an employment relationship between an employee (other than a service provider) and a public body,

This provision permits Government of Yukon, acting in an employment capacity, to disclose information in the management of employee's performance.

An example includes disclosing information to the Labour Relations Branch in the Public Service Commission (PSC) to receive advice on labour matters.

> **25(i)(xi)** providing legal services to the Government of Yukon or a public body,

This provision allows disclosure of information to receive legal advice.

> **25(i)(xii)** an existing or anticipated proceeding to which the Government of Yukon or a public body is, or is expected to be, a party,

This provision allows disclosure of information to lawyers representing Government of Yukon in preparation for a proceeding. **"PROCEEDING"** is defined as a court, civil or criminal proceeding; or a hearing by an adjudicator as authorized under an Act of the Legislature or Parliament. (See **section 1** definitions.)

> **25(i)(xiii)** complying with
>
> **25(i)(xiii)(A)** a subpoena, warrant or order issued or made by a court, an adjudicator or another person or body with jurisdiction to compel the production of records, or
>
> **25(i)(xiii)(B)** a rule of court relating to the production of records,

Subsection (i)(xiii) allows disclosure of information to comply with a court order (including subpoena or warrant).

These provisions permit personal information to be disclosed in order to comply with legal processes that require the production of information. These processes include the use of a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Yukon to compel the production of information, or with a rule of court binding in Yukon that relates to the production of information.

> **25(i)(xiv)** enforcing a maintenance order under the *Maintenance Enforcement Act* to which the individual is subject,

This provision allows permits a public body to disclose personal information to enforce a maintenance order. "MAINTENANCE ORDER" is defined under the *Maintenance Enforcement Act*, section 1 Interpretation and Application.

> **25(i)(xv)** facilitating the sheriff's performance of a service under the *Judicature Act* for a public body in respect of a process, writ, warrant or other similar type of document in which the individual is named,

This provision allows the Sheriff's Office to disclose information required to serve legal documents under the *Judicature Act*.

> **25(i)(xvi)** providing a specialized service to the individual in respect of which the public body is the personal identity manager or a partner, or

This provision allows disclosure of information to a partner agency if they are participating in an approved integrated service (see **section 27**) or an approved personal identity service (see **section 28**).

> **25(i)(xvii)** carrying out a data-linking activity in respect of which the public body is a partner.

This provision allows for disclosure of information to fulfill an approved data-linking activity in accordance with **section 29**.

"DATA LINKING" means the combination of personal information contained in a dataset with personal information contained in another dataset for a purpose other than (a) the purpose for which the personal information in each dataset was collected, and (b) a purpose that is consistent with a purpose referred to in paragraph (a).

SECTION 26 Research agreement required if identifying information used for research

These provisions allow disclosure of personal information to a researcher who is conducting research work that uses personal information in an identifying manner. The conduct of the research must be in accordance with the criteria established in this provision.

For a research purpose to be authorized, a written agreement must be signed by the researcher and public body identifying the parts of this Act and protocols that apply and any other conditions the public body requires.

This provision also specifies that if the researcher needs to contact an individual or individuals whose personal information is disclosed, the researcher may request the Information and Privacy Commissioner (IPC) to review the agreement before signing it. The agreement will reflect Commissioner's additional conditions related to this request.

The *ATIPP Act* does not expressly prohibit disclosure of information other than personal information for a research purpose under a confidentiality agreement. Public bodies should seek legal advice as to whether disclosure could expose the body to the risk of legal action. For example, confidential third party business information for a research purpose.

"PERSONAL UNIQUE IDENTIFER", of an individual, means an identifier that (a) is assigned to the individual, and (b) uniquely identifies the individual in relation to a public body.

The identifiers might be an individual's name, address, and telephone number, date of birth or social insurance number. Small population cells or contextual information may also allow for the identification of an individual. The Yukon Bureau of Statistics uses the threshold of 10 or less individuals to restrict information that may identify individuals.

Section 26 of the Act enables a public body to disclose personal information for a research purpose, including statistical research, only if: the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the Commissioner.

> **26(1)** A public body may disclose personal information to a person or another public body (referred to in this section as the "researcher") for a research purpose, including a statistical research purpose, that could not reasonably be carried out through the use of non-identifying information only if the researcher and the public body have entered into a written agreement that
>
> **26(1)(a)** describes the research purpose and research work to be undertaken by the researcher; and
>
> **26(1)(b)** contains the following conditions, with any necessary modifications, in relation to the research purpose and research work:
>
> **26(1)(b)(i)** the researcher must not, subject to subsection (3), use the personal information to contact the individual,
>
> **26(1)(b)(ii)** the researcher must use, disclose and manage the personal information in accordance with each term and condition of the agreement and each of the following, which must be specifically referred to in the agreement:
>
> **26(1)(b)(ii)(A)** each provision of this Act that is applicable to the research purpose and research work,
>
> **26(1)(b)(ii)(B)** each protocol that is applicable to the research purpose and research work,
>
> **26(1)(b)(iii)** the researcher must not, without authorization from the public body, use the personal information for any purpose other than the research purpose and research work described in the agreement,

> **26(1)(b)(iv)** the researcher must not disclose any of the personal information to another person except an employee or agent of the researcher who is working for or on behalf of the researcher in undertaking the research work described in the agreement,
>
> **26(1)(b)(v)** as soon as practicable after completing their research work, the researcher must dispose of the personal information in accordance with the regulations. Please see *ATIPP Act Regulations* for more information.

The first part of this provision allows public bodies to disclose personal information for research in circumstances where the research cannot be completed without access to the information in individually identifiable form. The onus is on the public body to have a general understanding of the research methods and the specifics of the proposed project in order to determine whether identifiable information is truly needed to accomplish the research.

The second part of the provision allows public bodies to disclose personal information for research if the Information and Privacy Commissioner has approved the research purpose. Approval by the Information and Privacy Commissioner ensures that the research purpose is subjected to impartial scrutiny.

The researcher must submit the research proposal to either the public body or the Commissioner in writing, clearly explaining the nature of the research, the information involved and the reason for the request. A detailed proposal enables the public body or Commissioner to evaluate the necessity for identifiable information, any potential harm to individuals, the academic credentials, skill and reputation of the researcher, and proposed security for the records containing the information.

> **26(2)** A researcher is responsible in respect of, and liable for, the performance of all duties and responsibilities under an agreement entered into under subsection (1), including those performed on the researcher's behalf by an employee or agent of the researcher.
>
> **26(3)** Before a researcher enters into an agreement under subsection (1)
>
> **26(3)(a)** the researcher may request that the commissioner approve conditions on which the researcher may contact an individual or individuals whose personal information is disclosed to the researcher; and
>
> **26(3)(b)** the commissioner may approve the request and substitute, for the condition referred to in subparagraph (1)(b)(i), conditions relating to the following matters as specified by the commissioner:
>
> **26(3)(b)(i)** the manner in which the researcher is permitted to contact an individual,

26(3)(b)(ii) the information that the researcher is required to provide to an individual with whom they make contact,

26(3)(b)(iii) any other condition that the commissioner considers warranted in the circumstances.

For more on research proposals and agreements, visit the ATIPP site on Yukon.ca.

PART 2

DIVISION 6 SPECIALIZED SERVICES AND DATA-LINKING

Section 27 Integrated Service

This provision provides Cabinet with the power to approve an integrated service through the making of a regulation that sets out the components of the service (for example, partners and types of personal information).

An **"INTEGRATED SERVICE"** is a service that will enable public bodies and partner agencies to collaboratively provide integrated services. Under the ATIPP Act, Cabinet can prescribe the purpose of an integrated service, along with the standards below.

> **27** The Commissioner in Executive Council may, for the purpose of enabling public bodies and partner agencies to collaboratively provide integrated services, approve an integrated service by prescribing
>
> **27(a)** the purpose of the integrated service;
>
> **27(b)** each service that may be provided as a part of the integrated service;
>
> **27(c)** each public body, program or activity of a public body, or partner agency that is a partner in the provision of the integrated service;
>
> **27(d)** the types of personal information that may be collected, used or disclosed by a partner for the purpose of providing the integrated service;
>
> **27(e)** the terms and conditions that must be included in an agreement between the partners in respect of their collaborative provision of the integrated service; and
>
> **27(f)** if consent from an individual is to be required before the integrated service may be provided to them, the manner in which consent must be given and may be withdrawn.

This provision provides government with the flexibility to deliver services using a 'one government' model. There is a requirement for a privacy impact assessment to be completed and submitted to the Information and Privacy Commissioner (IPC) for review prior to launching this service **(section 11)**.

SECTION 28 Personal Identity Service

These provisions enable government to create an approved personal identity service. This service will allow citizens to access more services online through a government account and web portal.

This provision provides Cabinet with the power to approve a personal identity service through the making of a regulation that sets out the components of the service (for example, partners and types of personal information).

A **"PERSONAL IDENTITY SERVICE**" approved under this provision, is a service to enable public bodies to provide client-centered services.

"PERSONAL IDENTITY MANAGER" means the public body prescribed under paragraph 28(1)(b) as the personal identity manager.

"PARTNER", in respect of a specialized service or a data-linking activity, means each public body, program or activity of a public body, or partner agency that is prescribed as a partner in the provision of the specialized service or the carrying out of the data-linking activity.

"PARTNER AGENCY" means (a) a government institution subject to the *Privacy Act* (Canada), (b) an organization operating in Yukon that is subject to the *Personal Information and Electronic Documents Act* (Canada), (c) a public body, a government institution or an institution, as defined under an Act of a provincial legislature that has substantially the same effect as this Act, (d) a custodian, (e) a First Nation government and its employees, or (f) an entity prescribed as a partner agency.

"CUSTODIAN" has the same meaning as the *Health Information Privacy Management Act*. For more on custodians, see **section 10**.

"FIRST NATION GOVERNMENT" means (a) a governing body established under the constitution of a Yukon First Nation, (b) the council of a band recognized under the Indian Act (Canada), or (c) an entity prescribed as a First Nation Government.

There is a requirement for a privacy impact assessment to be completed and submitted to the Commissioner for review prior to launching this service (see **section 11**).

> **28(1)** The Commissioner in Executive Council may, for the purpose of enabling public bodies to provide client-centered services, approve a personal identity service by prescribing
>
> **28(1)(a)** subject to subsection (2), each service that may be provided as a part of the personal identity service;
>
> **28(1)(b)** a public body as the personal identity manager;
>
> **28(1)(c)** each public body, program or activity of a public body, or partner agency that is a partner in the provision of the personal identity service;

28(1)(d) the types of personal information that may be collected, used or disclosed by a partner for the purpose of providing the personal identity service (referred to in this section as "personal identity information");

28(1)(e) the terms and conditions that must be included in an agreement between the personal identity manager and the partners in respect of the provision of the personal identity service; and

28(1)(f) if consent from an individual is to be required before the personal identity service is provided to them, the manner in which consent must be given and may be withdrawn.

Subsection (2) provides restrictions for the types of services that are authorized for the personal identity service.

28(2) A personal identity service approved under subsection (1) may include only the following types of services:

28(2)(a) identification of an individual;

28(2)(b) verification of the identity of an individual;

28(2)(c) updating the personal identity information of an individual;

28(2)(d) issuance of a physical or electronic credential to an individual;

28(2)(e) management of the personal identity information associated with a physical or electronic credential;

28(2)(f) a service of a similar type prescribed as a type of service that may be provided as part of a personal identity service.

SECTION 29 Data-linking activity

This provision provides Cabinet with the power to approve a data-linking activity through ~~the~~ making of a regulation that sets out the components of the activity (for example, purpose, details, each participant and types of personal information).

"DATA LINKING" means the combination of personal information contained in dataset with personal information contained in another dataset for a purpose other than (a) the purpose for which the dataset was collected, and (b) a purpose that is consistent with a purpose referred to in paragraph a.

"DATASET" means a grouping of data in which all or most of the data (a) is held by a public body, (b) consists of facts, (c) is not the product of analysis or interpretation, (d) is not a document referred to in section 9 of the *Archives Act*, and (e) has not, except for its grouping, been organized, adapted or modified.

The Archives Act, section 9 Acquisition of documents under conditions, includes private (non government) documents acquired by the archives by gift, bequest, loan or purchase.

A **"DATA LINKING ACTIVITY"** means a data-linking activity approved under this section and involves involves linking of data from different sources to analyze and predict complex patterns of activity. Requiring a regulation for data-linking activities is one such measure to ensure purposes are prescribed before such methods and technologies are employed.

> **29** The Commissioner in Executive Council may approve the carrying out of a data-linking activity by one or more public bodies or partner agencies by prescribing
>
> **29(a)** the purpose of the data-linking activity;
>
> **29(b)** the details of the data-linking activity;
>
> **29(c)** each public body, program or activity of a public body, or partner agency that is a partner in the carrying out of the data-linking activity;
>
> **29(d)** the types of personal information that may be collected, used or disclosed by a partner for the purpose of carrying out the data-linking activity; and
>
> **29(e)** the terms and conditions to be included in an agreement between the partners in respect of carrying out the data-linking activity.

"PARTNER", in respect of a specialized service or a data-linking activity, means each public body, program or activity of a public body, or partner agency that is prescribed as a partner in the provision of the specialized service or the carrying out of the data-linking activity.

"PARTNER AGENCY" means (a) a government institution subject to the *Privacy Act (Canada)*, (b) an organization operating in Yukon that is subject to the *Personal Information and Electronic Documents Act* (Canada), (c) a public body, a government institution or an institution, as defined under an Act of a provincial legislature that has substantially the same effect as this Act, (d) a custodian, (e) a First Nation government and its employees, or (f) an entity prescribed as a partner agency.

"CUSTODIAN" has the same meaning as the *Health Information Privacy Management Act*. For more on custodians, see **section 10**.

“FIRST NATION GOVERNMENT” means (a) a governing body established under the constitution of a Yukon First Nation, (b) the council of a band recognized under the Indian Act (Canada), or (c) an entity prescribed as a First Nation Government.

PART 2

DIVISON 7 PROTECTING PERSONAL INFORMATION

SECTION 30 Securing personal information against privacy breach

This provision requires the head of a public body to secure personal information in accordance with ATIPP Regulations. Please see the ATIPP Regulations for more information.

> **30** The head of a public body must protect personal information held by the public body by securely managing the personal information in accordance with the regulations. Please refer to the *ATIPP Act Regulations* for more information.

"HEAD", of a public body, means a ministerial body (Government of Yukon department, corporation or directorate); or a statutory body or entity (non-statutory body) prescribed through ATIPP Regulations. Public bodies include **"EMPLOYEES"** and **"SERVICE PROVIDERS"**.

"MANAGE", in respect of personal information, includes retaining, storing, transferring, transmitting or disposing of the personal information but does not include collecting, using or disclosing the personal information.

SECTION 31 Employee to report suspected privacy breach

This provision requires an employee of a public body to report a suspected privacy breach to the Designated Privacy Officer (DPO) for the public body.

"DESIGNATED PRIVACY OFFICER", of a public body, means the employee designated under paragraph 87(1)(a) as the designated privacy officer for the public body.

"PRIVACY BREACH", in respect of personal information, means the theft or loss of, or unauthorized use, disclosure or disposal of, the personal information.

> **31** If an employee of a public body reasonably believes that a privacy breach in respect of personal information held by the public body has occurred or is occurring, the employee must, without delay, report the suspected privacy breach to the designated privacy officer for the public body.

When an employee discovers or suspects that a privacy breach has occurred, they should take all known or practicable steps to reduce or stop the breach. This is the process known as containment.

CONTAINMENT means the act, process, or means of keeping something within limits. Examples of containment are:

- Immediately recovering the information and having the recipient confirm in writing that no copies of the information have been made, the information was not and will not be communicated and any and all copies have been securely destroyed;
- Shutting down the system that was breached;
- Revoking or changing a computer access code;

Once containment measures are in place, employees are required under this part of the Act to immediately report the suspected breach to their Designated Privacy Officer. It is important for the employee not to panic and not to discuss the breach with any other employee or party unless directed by their Designated Privacy Officer.

For more information on reporting, please see the Privacy Breach Procedures document issued by the ATIPP Office and ATIPP Protocols.

SECTION 32 Response to report of suspected privacy breach

This provision sets out the duties of a public body's Designated Privacy Officer (DPO) when they receive a report of a suspected privacy breach. This provision also includes factors for the privacy officer to consider when assessing whether a '*risk of significant harm*' exists.

"SIGNIFICANT HARM" means in respect of a privacy breach, bodily harm, personal humiliation, reputational or relationship damage, loss of employment, business or professional opportunities, financial loss, negative effects on a credit rating, or damage to or loss of property, or any other similar type of harm.

If the Designated Privacy Officer determines that a 'risk of significant harm' exists, they are required to report the privacy breach to the:

(1) head of the public body;

(2) Information and Privacy Commissioner (IPC); and

(3) affected individual(s).

"AFFECTED INDIVIDUAL", in respect of a privacy breach, means an individual whose personal information is personal information in respect of which a privacy breach has occurred or is occurring.

If the public body is a **"MINISTERIAL BODY"**, the Designated Privacy Officer is also required to report the privacy breach to the Access and Privacy Officer (ATIPP Office). This requirement will assist in developing centralized expertise related to identifying systemic issues that may be mitigated government wide.

On receiving a report, the Commissioner may make recommendations to the head of the public body, upon which the head has 30 days to respond.

32(1) In this section "affected individual", in respect of a privacy breach, means an individual whose personal information is personal information in respect of which a privacy breach has occurred or is occurring.

32(2) Without delay after receiving a report made under section 31, the designated privacy officer must assess the report.

32(3) For the purpose of an assessment under subsection (2), the designated privacy officer for a public body may request from the head or an employee of the public body any information that the designated privacy officer considers necessary to conduct their assessment.

32(4) Without delay after receiving a request under subsection (3), the head or employee who received the request must, if they hold the information requested, provide it to the designated privacy officer.

32(5) If, after conducting their assessment under subsection (2), a designated privacy officer determines that a privacy breach has occurred or is occurring, the designated privacy officer must, without delay, determine, in accordance with subsection (6), whether there is a risk of significant harm to affected individuals due to the privacy breach.

32(6) In making a determination under subsection (5), the designated privacy officer must consider the following factors in relation to the privacy breach to which the determination relates:

32(6)(a) the sensitivity of the personal information in respect of which the privacy breach has occurred or is occurring;

32(6)(b) the probability that the personal information is, has been or will be used or disclosed in an unauthorized manner;

32(6)(c) how much time elapsed between the occurrence of the privacy breach and the determination that it occurred;

32(6)(d) the number of affected individuals;

32(6)(e) the type of relationship, if any, between affected individuals and any person who may have used, or to whom may have been disclosed, the personal information in respect of which the privacy breach has occurred or is occurring;

32(6)(f) the measures, if any, that the public body has implemented or is implementing to reduce the risk of significant harm to the affected individuals;

32(6)(g) if the personal information has been lost, stolen or disposed of, whether or not any of the personal information has been recovered;

32(6)(h) any other information that is relevant in the circumstances and is reasonably available to the designated privacy officer.

Subsection 7 provides the requirements for notification when a breach involving risk of significant harm occurs. Public bodies are required to notify the Head or designate of the public body, the OIPC, along with all affected individuals. If the public body is a **"MINISTERIAL BODY"**, they are also required to provide a copy of the breach report to the Access and Privacy Officer (ATIPP Office).

32(7) If a designated privacy officer determines that there is a risk of significant harm to affected individuals due to a privacy breach, the designated privacy officer must, without delay after making the determination

32(7)(a) notify the head of the public body of the privacy breach and the risk of significant harm to the affected individuals;

32(7)(b) provide to each affected individual, in accordance with the regulations and each applicable protocol, a notice of the privacy breach and the risk of significant harm to them;

32(7)(c) provide to the commissioner

32(7)(c)(i) a report made in accordance with subsection (8), and

32(7)(c)(ii) a copy of the notice referred to in paragraph (b); and

32(7)(d) in the case of a privacy breach relating to a ministerial body, provide a copy of the report referred to in subparagraph (c)(i) to the access and privacy officer.

Subsection 8 provides the public body's privacy breach reporting requirements.

32(8) A report made by a designated privacy officer under subparagraph (7)(c)(i) must include

32(8)(a) the designated privacy officer's reasons for determining that a risk of significant harm to the affected individuals exists;

32(8)(b) the designated privacy officer's assessment of the cause of the privacy breach; and

32(8)(c) a description of each measure that the public body has implemented or is implementing to reduce the risk of significant harm to the affected individuals.

Subsection 9 is the Information and Privacy Commissioner's responsibilities for responding to a report of a significant privacy breach.

> **32(9)** On receiving a report made under subparagraph (7)(c)(i), the commissioner may recommend, in writing, to the head of the public body to which the report relates that the public body implement measures, as specified by the commissioner in the recommendation, that are likely to
>
> **32(9)(a)** reduce the risk of significant harm to the affected individuals; and
>
> **32(9)(b)** prevent the occurrence of, or mitigate the effect of, a privacy breach in similar circumstances.

Subsection 10 outlines the public body's discretionary response to the Information and Privacy Commissioner's report in 32(9). There is no requirement to respond, however it would be advised as a best practice to respond to any report to reduce risk, mitigate or prevent a similar breach.

> **32(10)** Not later than 30 days after the day on which the head of a public body receives a recommendation under subsection (9), the head must, in respect of each measure specified in the recommendation
>
> **32(10)(a)** decide whether to require the public body to implement the measure; and
>
> **32(10)(b)** provide a notice of their decision to the commissioner.
>
> **32(11)** If the head of a public body does not, within the applicable period, provide the notice referred to in paragraph (10)(b) in respect of a specific measure, the head is considered to have decided not to require the public body to implement the measure.

For more on assessing a breach and writing a breach report, please see the Designated Privacy Officer Toolkit.

SECTION 33 Information Management Service

This provision authorizes a public body or service provider to manage personal information for which another public body is responsible. This provides flexibility in maintaining data external to the public body and clarifies who is accountable for the information.

"INFORMATION MANAGEMENT SERVICE" means a service described in an agreement made under subsection 33(3).

"INFORMATION" means information contained in a record.

For example, a public body may authorize the Information Communications and Technology program in the Department of Highways and Public Works (ICT-HPW) as their information manager.

The Information Communications and Technology Program of the Department of Highways and Public Works (HPW-ICT) is *mandated* to provide leadership, advice and **centralized network, software and telecommunications services to the Government of Yukon** in support of their evolving use of computer and communications technologies.

NOTE: HPW-ICT is a **PROGRAM** of the ministerial public body – the Department of Highways and Public Works - mandated as a **CORPORATE RESOURCE** to Government of Yukon.

HPW-ICT should not be confused with the Information Technology and Client Solutions Unit of Highways and Public Works (HPW-ITCS), which is an **ACTIVITY** of the public body that provides internal IM/IT resources to the department.

This provision also establishes that a written agreement needs to be signed by the public body and information manager and lists certain criteria that must be included in the agreement. The ATIPP Office has produced a template to use for these agreements that includes all essential elements.

It also identifies that the public body that provides the data to the information manager is still 'holding' this information and remains accountable for the information manager's management of this information.

"HOLD", in respect to information, means to have custody or control of the information.

> **33(1)** Subject to subsections (2) and (3), a public body may provide another public body or person (referred to in this section as the "information manager") access to personal information held by the public body for the purpose of the provision of an information management service to the public body.
>
> **33(2)** An information management service may include a service of only the following types:
>
> **33(2)(a)** the management of personal information held by a public body;
>
> **33(2)(b)** the provision of an information technology service to a public body;
>
> **33(2)(c)** a service of a similar type prescribed as a type of service that may be provided as part of an information management service.
>
> **33(3)** Before a public body provides an information manager access to personal information held by the public body, the public body and the information manager must

enter into a written agreement that includes a description of each service to be provided as part of the information management service.

33(4) After entering into the agreement referred to in subsection (3), the information manager may use the personal information provided to it under the agreement only for a service described in the agreement.

Subsection 5 provides greater certainty that the information manager does not hold (have custody and control) of information subject to an information management agreement with another public body

33(5) Personal information to which an information manager has been provided access by a public body under this section

33(5)(a) is not considered to be held by the information manager; and

33(5)(b) is considered to be held by the public body.

DIVISION 8 ACCESSING AND CORRECTING PERSONAL INFORMATION

SECTION 34 Individual's right to request access to their personal information

This section provides a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant. The applicant also has the right to request correction of it.

There are no restrictions as to who may make a request. The applicant can be any person who is residing inside or outside of Yukon, including individuals, corporations, and organizations. The Act does not specify a minimum age, which means that minors may also make requests.

> **34** An individual may request access to their personal information held by a public body by submitting an access request in respect of the personal information.

Some individuals who live in remote areas may be disadvantaged in comparison with other members of the public in their ability to make an ATIPP request. Public bodies should take such situations into account and assist applicants in ways that will enable them to exercise their access rights without excessive cost or delay.

SECTION 35 Personal information correction request

Under this section of the Act, an individual who believes that his or her personal information, in the custody or under the control of a public body, contains an error or omission may request the public body to correct their personal information.

Information is personal information if it meets the definition of **"PERSONAL INFORMATION"** in **section 1** of the Act, regardless of whether the public body created or gathered the information directly or obtained it from someone else.

"HOLD" in respect of information, means to have custody or control of the information.

CONTROL is when a public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

In order to request a correction of personal information, an individual does not have to make a request for access to his or her personal information. For example, a public body may refer to information contained in a record and the individual may challenge the accuracy of that record without having seen it.

A request for correction may be generated as a result of an adverse administrative decision (e.g. a denial of a claim or benefit). The ATIPP Act does not require the public body that made the decision to revisit that decision as a result of the request.

The Act gives individuals the right to request a correction of personal information, not a right to have a correction made. The public body may either correct the information, by changing it or adding new information, or may refuse to correct the information, subject to other provisions discussed below.

When considering requests for correction of personal information, it is important to distinguish between the two types of information addressed under this section:

- FACTUAL INFORMATION about the applicant, such as age, date of birth, income information or qualifications**;** and

- OPINIONS about the applicant, such as subjective assessments or evaluations of an individual's condition, abilities or performance.

The individual must provide proof in support of the request for correction of factual information. The proof should be of the same nature and at least the same quality as the personal information required when the original collection took place. Examples of documents that might be required to prove facts include a birth or baptismal certificate to prove age, or a notice of assessment from the Canada Revenue Agency to prove income.

Factual information does not need to be corrected if the facts are in dispute and it is not possible to make a factual determination about the issue through the inquiry process.

A public body must not correct an opinion including a professional or expert opinion. The significance of an opinion may be that it reflects another person's view at the time it was offered, and it may be important to have a record of that view at a later date. The Act allows an individual to have his or her views about that opinion added to the record for other readers to consider.

How a request is made

In many cases, an individual will ask for personal information to be corrected and supply proof of correction submitting a formal request. Public bodies can and often will make corrections without a request under the Act if this is practical and expedites public business.

Where, in the opinion of the individual, an error or omission exists, a request for correction can be made to the public body in the form of a letter or on a Request to Correct Personal Information Form.

Requests for correction are subject to the same rules as requests for access under the *Act*. This includes time limits. It also includes a duty on the part of the public body to seek clarification of a correction request, if necessary. The Information and Privacy Commissioner has the power to review the actions of a public body with respect to requests for correction of personal information.

> **35(1)** An individual who believes that there is an error or omission in respect of any of their personal information held by a public body may, in accordance with the regulations, if any, request that the head of the public body correct the error or omission.

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.

Please see the *ATIPP Act Regulations* for more information.

Subsection 2 provides the time limit and process for evaluating the request and the head's discretion to make or refuse the request.

> **35(2)** Not later than 30 business days after the day on which the head of a public body receives a request made under subsection (1), the head must
>
> **35(2)(a)** make the requested correction to each record held by the public body that contains information to which the request relates, and provide a notice to the individual who made the request that specifies each correction that was made; or

To apply **Subsection (2)(a)** and correct an error, a public body must correct <u>all records</u> containing the personal information. This includes records in all information storage mediums whether paper or electronic, including systems. The record should be annotated with the date of the correction. A linking mechanism, as described below, may have to be employed when personal information is stored on a medium such as microform, which may be more difficult to update.

To ANNOTATE personal information means to add the requested correction to the original record. An annotation should be signed and dated. When designing electronic forms and databases, provision should be made for allowing annotation.

To LINK a record means to attach, join or connect the record to the requested correction. This may consist of a letter or statement from the applicant, or a copy of the Request to Correction Personal Information Form.

35(2)(b) refuse to make the correction and take the following actions:

35(2)(b)(i) note the following on each record to which the request relates:

35(2)(b)(i)(A) that the request was made,

35(2)(b)(i)(B) the date on which the request was made,

35(2)(b)(ii) provide a notice to the individual who made the request that states

35(2)(b)(ii)(A) that the request is refused,

35(2)(b)(ii)(B) the head's reasons for refusal,

35(2)(b)(ii)(C) that the making of the request has been noted on the relevant records, and

35(2)(b)(i)(D) that the individual has a right to make a complaint under section 36 in respect of the refusal.

When a correction is refused or cannot be made, the public body must annotate or link the personal information with that part of the requested correction which is relevant and material to the record in question as outlined in subsection (2)(b).

RELEVANT AND MATERIAL means that there is a direct connection between the correction requested and the use that has been or may be made of the personal information and that the correction is substantive. The correction should be both pertinent to the subject matter and significant in its content.

A public body may refuse or be unable to make a correction that an applicant requests. This may be because the information is not personal information, the applicant has not submitted adequate proof in support of the requested correction, or the information consists of an opinion rather than fact.

In the case of factual information, when the public body is not satisfied with the proof presented, the public body does not change the information but rather annotates it or links the presented information to the original information.

In the case of an opinion, a public body may describe the information in dispute and place this description, along with a statement that the applicant does not agree with the opinion or

interpretation, on the record. If practicable, the applicant's request for correction may be attached.

A public body is required to note only that part of the requested correction which is relevant to the record being annotated or to which the link is being made. Public bodies must not place the applicant's entire request on the record if it contains material that is not relevant to the use made of the record.

Annotating a request for correction

The ATIPP Office provides a template form for annotating personal information. A public body may use this form to set out an annotation relating to a correction that was requested but not made. This form clearly indicates to users that the information has been linked to a correction request and not corrected. It is filed with or linked to the information for which a correction was requested.

A copy of this form must be sent to the individual requesting a correction at the time the individual is informed that the correction is not being made with the accompanying notification. Any further information supplied by the individual after receiving this notice must be filed with the form.

If the Annotation to Personal Information Form or the Request to Correct Personal Information Form cannot be physically attached to the record, a flag may be placed in the file or system containing the personal information in dispute. This will refer a user to a separate file, containing the actual disputed personal information, and indicating that a request for correction or addition of information was made but not granted.

When a public body makes an annotation or linkage regarding a request for correction that has been refused or regarding a request for correction that has been agreed upon, it must ensure that the new information is stored with the original information and will be retrieved whenever the information in question is used for an administrative purpose directly affecting the individual involved. Annotations must be made available to all users of the file or the information, including the individual, should he or she request access to his or her personal information.

Subsection 3 requires the head of the public body to ensure any personal information they hold that has been corrected, is also corrected by other public bodies or organizations to which the information was disclosed.

In order to fulfil this requirement, it's important for public bodies to have current Information Sharing Agreements and records of disclosures. Notification is required if the personal information has been shared in the year prior to the request for correction.

> **35(3)** Without delay after making a correction in accordance with paragraph (2)(a), the head of a public body must provide notice of the correction to each other public body or person to whom the head disclosed, within the 12-month period before the correction was made, the personal information to which the correction relates.

Subsection 4 ensures through the notification process that other public bodies or organizations have accurate and complete information for their own decision-making processes.

> **35(4)** Without delay after receiving a notice under subsection (3), the head of each other public body must make the correction specified in the notice in respect of all records that are held by the public body and that contain the personal information to which the correction in the notice relates.

> **35(5)** If the head of a public body does not take any action under subsection (2) in respect of a request made under subsection (1), the head is considered to have refused the request.

> **35(6)** The head of a public body must not charge a fee for a request made under subsection (1), or a notice or correction relating to such a request.

PART 2

DIVISION 9 – PRIVACY COMPLAINTS

SECTION 36 Personal information correction complaint

This provision establishes an individual's right to make a complaint to the Information and Privacy Commissioner about a head's decision in respect of a personal information correction request.

A request for correction may be generated as a result of an error or omission leading to an adverse administrative decision (e.g. a denial of a claim or benefit). The *ATIPP Act* does not require the public body that made the decision to revisit that decision as a result of the correction request. The Act gives individuals the right to request a correction of personal information, not a right to have a correction made.

The public body may either correct the information, by changing it or adding new information, or may refuse to correct the information, subject to other provisions discussed below.

> **36** An individual may, in relation to their personal information, make a complaint to the commissioner in respect of the following by filing the complaint in accordance with section 90:

Section 90 of the ATIPP Act outlines the individual's right to file a complaint to the Information Privacy Commissioner. Individuals have 30 business days after receiving notification to file their complaint.

> **36(a)** an action taken by the head of a public body under subsection 35(2);
>
> **36(b)** the failure of the head of a public body to take an action as required under subsection 35(2).

The Commissioner has 10 business days to decide whether a complaint under this provision of the Act is warranted under **section 91**.

Section 37 Privacy complaint

This provision provides individuals with the right to submit a complaint to the Information and Privacy Commissioner, if they reasonably believe that a public body has engaged in the unauthorized collection, use or disclosure of their personal information. This section enables the commissioner to monitor public bodies' compliance with this Act and ensure that public bodies' decision-making is conducted in accordance with the purposes of this Act and that their administration is in accordance with the purposes of this Act.

> **37** An individual may, if they reasonably believe that a public body has collected, used or disclosed their personal information in contravention of this Part, make a complaint to the commissioner by filing the complaint in accordance with section 90.

For more on complaints, see **section 90** of the Act in Chapter 5.