ATIPP OFFICE GUIDANCE

PRIVACY IMPACT ASSESSMENTS

Purpose

This guidance will explain:

1. What is a Privacy Impact Assessment (PIA)?
2. Why and under what specific circumstances do I need to do a PIA?
3. What is the process for completing a PIA?
4. How the ATIPP Office is here to support you during the process? – and
5. How to fill out the PIA template?

1. What is a Privacy Impact Assessment (PIA)?

Privacy is recognized as a foundational value in our society - it allows us to protect ourselves from unwanted interference and attention. It helps to create boundaries to limit who has access to our personal information (PI) and what they can do with it.

For this reason, laws have been created as a mechanism to protect privacy, and in the Yukon this law is the *Access to Information and Protection of Privacy Act (ATIPP)*.

The *ATIPP Act* includes measures to give people control over their PI. The kind of control we're talking about here includes how PI is collected, used, disclosed, and safeguarded by the Yukon government (YG). As such, the *ATIPP Act* protects peoples' privacy by making rules surrounding the **collection, use**, and **disclosure** of PI.

NOTE: Collection means to gather or acquire identifiable information about an individual.

Use means to access this information within the public body (department or corporation).

Disclosure happens when access to personal information is given to anyone outside the public body.

A PIA is a documented process for evaluating the collection, use and disclosure of PI to ensure compliance with the *ATIPP Act*.

It examines the types of PI involved in a given initiative and helps assist programs to only collect what needs to be collected for a given purpose. It confirms if legal authorities exist to allow for collection, use, and disclosure of PI. It clearly documents the purposes and legal authorities for the collection, use, and disclosure of PI involved in government activities.

A PIA also maps out information flows involved in the initiative to show *how* Pi is collected, used, and disclosed by an information system or other means being used to carry out the program or activity.

As programs are legally obligated and accountable for the protection and appropriate handling of PI, a PIA also helps establish an understanding of the measures needed to accomplish this. It's up to us to make sure that we protect PI, and a PIA is a tool to help us to do so.

This process enables us to identify potential privacy risks, and enables decision makers to be empowered to be proactive in addressing and mitigating these risks.

2. Why and under what specific circumstances do I need to do a PIA?

Ministerial public bodies are required to complete PIAs as per section 11 of the ATIPP Act. The Head (or delegate) responsible for the department, corporation, or program must complete a PIA before the initiative or system is implemented or goes live.

Completing a PIA reveals a commitment to protect PI - it enables programs to prevent and address risks to privacy. The process also benefits service delivery/reduces costs by only collecting and having to manage what is required to collect for a given purpose.

Under section 11 of the ATIPP Act, a PIA is required before a Ministerial public body carries out a proposed:

- program or activity;
- specialized service;
- data-linking activity;
- information management service; and/or
- significant change to an existing process.

Specialized Services and Data Linking Activities:

If your PIA relates to a specialized service or data-linking activity, a regulation under the *ATIPP Act* may be required prior to implementation (see sections 27, 28, and 29 of the *ATIPP* Act). Please contact the ATIPP Office for advice if you think this might apply to your initiative.

If your initiative involves a specialized service or data-linking activity, you will need to submit your PIA to the Office of the Information and Privacy Commissioner (OIPC) who is given the opportunity to provide recommendations to the public body prior to implementation. You must respond to the OIPC's recommendations within 30 business days (see ATIPP Act section 11(4)).

For more information on specialized services (integrated services and personal identity services) and data-linking activities, please see Chapter 2 of the ATIPP Act Interpretation Manual.

3. What is the process for completing a PIA?

When to start?

If a PIA involves a new system development or upgrade to a system already in use, it should be started during the planning phase of this development or upgrade. If it relates to new programs or significant changes to existing processes or programs, it should also be started during the planning and development stage. When you're going through a business needs analysis or at the initiation stage of a project, this is the best time to start a PIA. If you include a PIA in the project charter, you can be sure that it is completed in time so that the review period and any needed mitigation can be accommodated before the system or initiative goes live.

If a PIA is started too late in your project, addressing risks or compliance issues will require solutions to be retrofitted into the system or process. This may increase project costs and/or also affect your implementation date so it's good to avoid this.

PIAs vary in complexity, and take one week to 3 months to complete.

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.

How to prepare to complete a PIA?

PIA development team

You may wish to put together a PIA development team if your initiative is complex and/or involves multiple parties. This team can include a group of specialists such as the program manager, program staff, IT specialists (departmental IT and corporate ICT), business analysts, project manager, privacy analysts, information management specialists, and system vendor(s). Be sure to include individuals who have:

- Knowledge of the overall project, along with an understanding of the business area, including its business processes, that the project addresses and its relevant stakeholders;
- Knowledge of privacy laws/policies and information management policies/principles; and
- Expertise in information technology and information security (if your project/program involves digital information systems).

Compile documentation

Before writing a PIA, it's helpful to gather relevant and useful documentation such as:

- Background information about your project/program (a project charter, for example);
- Business requirements documents;
- Business process maps of your project/program;
- Any intake or application forms;
- Any legislation and policies, other than the *ATIPP Act*, relevant to your project/program;
- Information about where records and information is stored, how it is accessed, and where it flows;
- Any records retention and disposition schedules pertaining to your program area;
- Agreements that apply to the initiative, such as Research Agreements, Information Sharing Agreements (ISA), Information Management Service Agreements (IMSA), and/or Service Level Agreements (SLA).

What steps are involved in completing a PIA?

- Contact the ATIPP Office (privacy@yukon.ca) to see if a PIA is needed for your initiative.
- Complete a Privacy Impact Assessment template.
- Submit PIA to the ATIPP Office for feedback.
- Submit PIA to the OIPC for comment (if your initiative involves a specialized service or data-linking activity).
- Submit copy of completed, signed PIA to the ATIPP Office.
  Note: program managers can be delegated to sign PIAs – if this delegation is in place, they don't have to go to the DM for signature
- Submit a *Privacy Impact Assessment Summary* to the ATIPP Office

What resources are available to support me?

The ATIPP Office conducted a Request for Qualifications (RFQ) procurement process so that there are qualified contractors available to do this work if you need help. There are prequalified source lists that resulted from the RFQ for both PIAs and Security and Threat Risk Assessments (STRAs). For more information about STRAs, please contact the Corporate Information Security Office (CISO).

We went through this RFQ screening process so that only contractors with skills that meet baseline criteria are included on the list. We recommend that if you contract out the work, you issue an Invitational Tender or RFP, but you can also Direct Award from the list.

After you award the contract, create a service contract and provide the current PIA template issued by the ATIPP Office to the contractor. We also have information prepared for the service contracts to help with creating those if you need help. If anyone on your team needs assistance during any part of this process, please don't hesitate to contact us at privacy@yukon.ca.

4. How the ATIPP Office is here to support you

The ATIPP Office's Senior Access and Privacy Analysts and Privacy Compliance Specialists provide advice, review, and support for PIAs.

We do this by helping determine whether a PIA is required, we assist with procurement from the prequalified list of contractors, we provide templates, forms, guidance, and advice, and review PIAs and provide comments and recommendations. Please ask questions! If you are having difficulty explaining your project or understanding any part of the PIA template, don't hesitate to contact us for assistance.

When you are ready to provide us with a draft of your PIA for review, we will give comments and recommendations back to you within 30 business days. After you consider/incorporate our recommendations, please provide us with an updated version of the PIA for final review. Be sure to consider these timelines for review in your project plan.

After the DM or delegated program manager signs the PIA, forward a signed, final copy to the ATIPP Office at privacy@yukon.ca.

> **NOTE:** 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.

5. How to fill out the PIA template

Section 1: PIA DOCUMENT CONTROL

This administrative section includes information to be recorded about who is drafting the PIA, as well as the date and version of the document. The 'Reviewed by' part is filled out when the PIA is sent to the ATIPP Office for our review. There are also areas to include any relevant policies and agreements, and this is where you will indicate if the PIA includes any appendices.

All of the highlighted text in the template can be removed if it does not apply to your situation. We have provided the examples that are highlighted to help prompt you to include the types of documents and information that you may wish to include if relevant.

Section 2: GENERAL

The intention of this section is to provide background information and context about your initiative, which includes a description of all PI involved. Describing your initiative in this way will allow you to complete the rest of the PIA template, so it's an important first step to complete.

When completing this section, it's helpful to have someone on board who understands the business processes and system(s) involved in the initiative, as well as someone who has knowledge of privacy laws and policies. If you need assistance to complete this section, please don't hesitate to contact the ATIPP Office.

Question 2.1.1 asks you to describe the initiative (program, activity, service, or system) that is subject to the PIA and the context within which it functions. Depending on the complexity of the initiative, your answer to this question may be lengthy and include a Background, Current State and Future State description.

Program managers are encouraged to use project information that is already available when answering this question (attaching a project charter or business case, for example).

Information from this section of the PIA is what is used to create a PIA summary to publish in the Access to Information Registry.

Question 2.1.2 asks you about the scope of the PIA. This is where you will indicate what is involved: specific goals, deliverables, features, functions, and deadlines.

For example: “the project scope includes the installation of Software A in XX department for use by 2 authorized staff to conduct specialized patient testing for a 3 month pilot project commencing on Jan 1, 2022 and ending on Mar 31, 2022.”

This information can often be found in a Briefing Note or Project Charter for larger projects. In some cases, identifying what is out of scope can add clarity to what precisely is in scope.

Question 2.1.3 asks you to list the parties involved in the initiative. This includes other public bodies, partners, service providers, and vendors. This will help to identify what legal authorities must in place before any sharing (disclosure) and further use of PI occurs. It also serves to pinpoint if and when Information Sharing Agreements (ISAs) and/or Information Management Service Agreements (IMSAs) will need to be created.

Question 2.1.4 asks you to list all of the types of PI involved within the scope of the initiative. Here it is best to have a comprehensive list of all types of information that you think might be PI so that the ATIPP Office can help you determine which information is considered “personal information,” as defined by the ATIPP Act.

NOTE: Section 2 is the foundation of the PIA, so you are welcome to contact the ATIPP Office for our input before proceeding with the rest of the PIA. This way, we can assist you to determine whether the PI being collected is the minimum amount necessary for the purpose, as well as offer suggested changes to business processes to ensure compliance with the ATIPP Act.

Here is a list of types of PI to help you identify everything that is involved in your initiative – please note that it does not include everything that could be considered personal information and/or personal health information:

Identification and Contact Information	
Name or alias	
Address	
Residency	
Home or cell phone	
Email address	
Gender	
Nationality	
Place of Birth	
Date of Birth	
Age	
Martial status	
Number of dependents	
Signature	

Unique Identifiers	
User name	
Password	
Unique identification number	
Social insurance number	
Case file number	
Electronic signature	
Yukon Health Insurance number	
Employee ID	
Driver’s license number	
Other (please specify)	
Employment Information	
Name of Employer	

Financial Information	
Real estate	
Tax information	
Credit history	
Income	
Expenditures/liabilities	
Bank accounts	
Credit or debit card numbers	
Expiration dates	
Magnetic stripe data	
PIN or security code	
Insurance information	
Legal status (judgements, injunctions, proceedings)	
Other (Please specify)	

Other (Please specify)	
Physical Characteristics	
Skin colour	
Eye colour	
Hair colour	
Height	
Weight	
Scars	
Fingerprint	
Iris scan	
Blood type	
Photograph	
Video image	
Other (Please specify)	

Employment history	
Employment references	
Experience/training	
Information generated during recruitment or selection process	
Employment history	
Employment references	
Opinion about another individual	
Other (Please specify)	
Education Information	
Academic history/status	
Degrees	
Professional licenses	
Certificates	
Awards	
Grades	
Other (Please specify)	

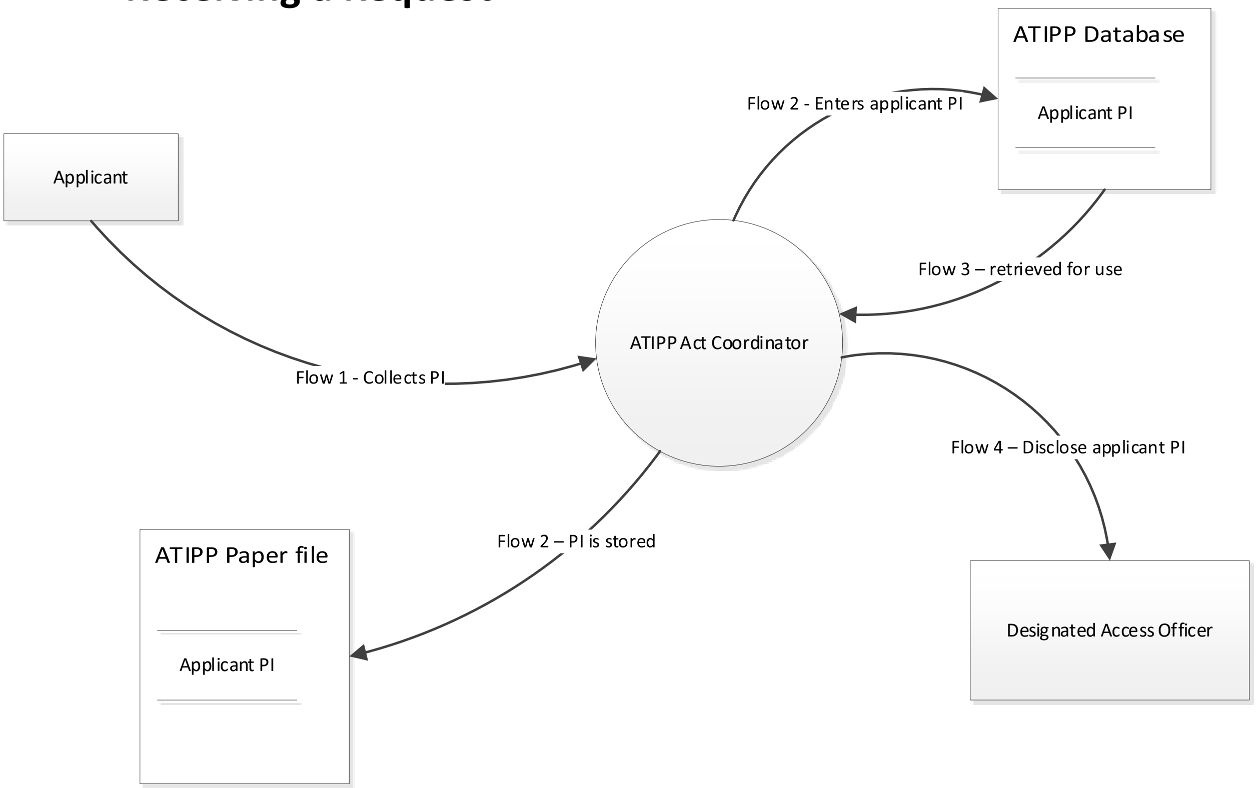
Health Information	
Health care status or diagnosis	
Test results or medical images	
Medications	
Diagnosis	
Disability	
Sensitive Information	
Religious views or affiliation	
Philosophical beliefs	
Political views	
Union membership	
Health information	
Genetic information	
Data on sexual life/preferences	
Ethnic background	
Criminal history	
Information about vulnerable person	
Other (please specify)	

Section 3: PERSONAL INFORMATION FLOW DIAGRAM AND TABLES

Personal information flow diagrams may be created using Microsoft Visio, which is a great tool; however, you can present the information in any format as long as the reader can have a beginning-to-end understanding of how the information flows. *The PI flow diagram is optional to include, but you must include a PI flow table.*

Here is an example of a personal information flow diagram:

Receiving a Request



Personal information flow tables assess whether your plan includes the legal authority to collect (sections 15 and 16 of the *ATIPP Act*), use (section 21 of the *ATIPP Act*) and disclose (section 25 of the *ATIPP Act*) PI. Completing a business process map of your initiative will help you to complete the table.

Flow tables represent information flows best when you break your initiative into its most basic part and this sometimes will result in more than one flow table. Pay special attention to the times when:

- You are collecting personal information from someone or somewhere;
- You are using the personal information; and/or
- You are disclosing or sharing the information with another individual or program area.

Make sure all uses of PI are identified in your flow table. For example, you may collect PI to determine an individual's eligibility to participate in a program, as well as to evaluate your program.

Examples of instances from where PI may be collected:

- Application or submission forms;

- Comment boxes or web postings;
- Consultations and surveys;
- Analytics; and
- Receiving information about an individual from another program area.

Examples of instances where you may plan on disclosing PI:

- Sharing information with another program area;
- Publishing information in print or online;
- Verifying information for another program area; and
- Providing information in answer to a request from areas such as law enforcement, another public body, or a municipality.

This example below shows types of PI that may be collected, used and disclosed for a clearly defined purpose. For each purpose identified, you'll document the legal authority to collect, use, and/or disclose the information. Look at your program's governing legislation to find these legal authorities, as well as the *ATIPP Act*.

Information Flow	Description (Collection, Use, Disclosure)	Types of Personal Information	Purpose	Legal Authority	Who is accountable
1	PI is collected directly from the applicant by the ATIPP Act Coordinator	Program Requests: Name, address, phone number, Access request Personal Information Requests: Name, address, phone number, date of birth (if required), Access request	PI is collected to identify the individual, identify records requested, to contact the individual about their request, mail records	Collection – ATIPP 15(a)*(c)(i) *legally authorised under ATIPP 44(1)	ATIPP Office, HPW
2	PI is used by the ATIPP Act Coordinator	Name, address, Access request	PI is input into database and a paper file is opened where hard copies are stored PI is used for the purpose of producing letters required to respond to request and maintaining paper file	Use – ATIPP 21(a)	ATIPP Office, HPW
3	PI is used by ATIPP Act Coordinator	Name, address, phone number, Access request	To communicate with applicant regarding: clarification, waivers, extensions, estimate of costs, final response, third party consultation	Use – ATIPP 21(a)	ATIPP Office, HPW

4	PI is disclosed by the ATIPP Act Coordinator to the public body's Designated Access Officer	Personal Information Requests: Name, date of birth (if required), Access request Program Requests: No PI is disclosed, only the request	Personal Information Requests: PI is disclosed to match records to applicant and respond to applicant's request The name and DOB are used by the Designated Access Officer as a control to ensure only the applicant's PI is disclosed	Disclosure – ATIPP 25(c)(i)(ii)	ATIPP Office, HPW

Section 4: COLLECTION

The intention of this section is to ensure the collection of PI is compliant with relevant legislation and is limited to that which is necessary for the purposes of the program or activity.

4.1 Collecting personal information

Question 4.1.1 asks you to describe how PI is **collected directly.**
Address the following in your response - whether it was collected directly from:

- the individual;
- an authorized representative (include sample of authorization); and/or
- a parent or guardian.

Whether it was collected through:

- an online form;
- a paper form;
- a fax to the program;
- an email to the program; and/or
- a snail mail to the program.

Question 4.1.2 asks you to describe how PI is **collected indirectly**.
This covers situations that involve collecting from a source other than the individual. For example, if your program collects PI from another public body, not from the person the information is about, your program is collecting this information 'indirectly'. You require authority to indirectly collect personal information - these authorities can be found in section 16 of the *ATIPP Act*.

Question 4.1.3 asks you to describe how PI being collected is the **minimum amount** needed to meet the purpose for collection. This is where you'll explain any purposes for collection PI that may not be entirely clear to ensure that your program only collects the minimum necessary.

If your program has conducted a review of the PI collected to ensure only the minimum necessary is being collected, include the following information in your response:

- the individual who conducted the review; and
- the date the review was completed.

4.2 Collection Notice

Question 4.2.1 asks you to provide the text that will be included in a **collection notice** that is required under section 17 of the ATIPP Act. This is where you provide your proposed or existing wording for a collection notice that will communicate to individuals why their PI is being collected, under what authority it is being collected, and who to contact if they have questions related to the collection. The ATIPP Office has published a Collection Notice Checklist to assist with this.

Here is an example of a collection notice:

Personal information is collected under [Name of Act, Section #], for the purposes of [describe purpose]. For further information, contact the [Director, Branch at (867) XXX-XXXX, toll free, within Yukon 1-800-661-0408, ext.5111].

Question 4.2.2 asks you to provide details on **where the collection notice will be posted.** This is where you document the location where individuals are able to view the notice before collection takes place. You can alternatively attach a screen shot or a copy of your form where the collection notice is/would be located as an appendix to the PIA.

4.3 Collection Risks

This is where you identify any risks related to the collection of PI, along with strategies for mitigation, the person responsible for mitigation activities, and timeline for completion. Some examples of common risks relate to unauthorized collection include:

- Over collection of PI – when PI is collected "just in case we may need it" rather than for an authorized purpose; and
- Consent is being used as an authority for direct collection of PI – this is not permissible under the *ATIPP Act* unless for a prescribed purpose (through regulation).

Section 5: SECURING PERSONAL INFORMATION

The protection of PI is largely accomplished through establishing adequate security measures. This means that the information must be protected when it is at rest (for example, on an encrypted USB or a secure server) and in transit (for example, when being disclosed to another public body or third party). Secure management of PI is addressed by section 30 of the *ATIPP Act* and specific requirements are expressed in section 9 of the *ATIPP Regulation*. The intention of this section of the PIA is to ensure that security measures needed to protect PI are in place, though documenting planned/existing measures, uncovering security risks, and devising mitigation strategies to minimize/eliminate the risks.

5.1 Security Threat and Risk Assessment (STRA)

Question 5.1.1 asks you if a STRA been completed for the initiative. If yes – you are prompted to attach the STRA as an appendix. If no – complete 5.1.2, 5.1.3 and 5.1.4.

Question 5.1.2 asks you to describe the **physical security measures** taken to protect the PI. These involve protecting hardware, software and information from physical damage or loss due to natural, human, or environmental threats.

Examples of controls related to physical security are: assigned security responsibility, media controls, physical access controls and workstation security.

- Assigned security responsibility means an employee should be assigned as responsible for security.
- Media controls are policies and procedures that govern the receipt and removal of hardware, software, disks, tapes, etc., into and out of the organization.
- Physical access controls limit access to information systems to individuals authorised to see the information. Examples include: equipment control, a facility security plan, procedures that verify user identity before allowing access to an area, a procedure for maintaining records of repairs and modifications to hardware, software, and physical facilities, antitheft devices, and a visitor sign-in procedure.
- Workstation security controls ensure workstations that allow access to PI are placed in secure or monitored areas. Controls that can be employed include; secure workstation policy and workstation placement to prohibit visitors from viewing screens.

Here are some questions to ask:

Do physical security measures for your office space include:

- locked cabinets;
- locked office doors;
- pass cards;
- motion detectors and other intrusion alarm systems; and/or
- procedures for visitors?

Do physical security measures for workstations include:

- publicly accessible service counters kept clear of PI;
- situating workstations so visitors cannot read screens; and
- password protected screen savers?

Is there a nightly closing protocol that requires employees to:

- clear all personal information from desks and place files containing personal information in locked filing cabinets;
- lock all office doors and cabinets;
- log out of all computers;
- remove all documents that contain PI from fax machines and printers; and/or
- set intrusion alarms (where installed)?

Are employees aware of how to securely dispose of information or equipment?

Question 5.1.3 asks you to describe the **technical security measures** taken to protect PI. These safeguard information systems and the networks on which data and information are maintained.

Examples of controls related to technical security include: access control, entity authentication, audit trails, encryption, firewall protection and virus checking.

- Access control addresses the need to have only individuals with a 'need to know' having access to PI. Controls over access can be user-based access, role-based, and/or context-based.
- Entity Authentication verifies that an individual is who they claim to be. Two-factor authentication is the recommended standard.
- Audit Trails show who has had access to a system and what operations were performed during a period of time.
- Encryption ensures that information in transit and at rest (being stored) is secure.
- Firewall Protection involves a system or combination of systems that supports an access control policy between two networks. Basic types of firewalls include packet filter (or network level) and proxy servers (or application level).
- Virus Checking involves having antivirus software installed and ensuring the virus catalogue is updated frequently.

Here are some questions to ask:

- Does the organization use a variety of mechanisms (firewalls, routers, intrusion detection and prevention systems, audit logs, system performance tools) to continuously monitor the operations of their systems to detect anomalies in service delivery levels?
- Are systems that are exposed to a public network “hardened”?
- Does the LAN that is connected to a public network use perimeter defence safeguards?
- If wireless devices are used, are the strongest security features of the wireless device enabled (encrypted and authentication, for example)?
- Is a wireless intrusion detection system employed?
- Are operating systems kept up-to-date with patches and fixes?
- Is there a regular schedule for updating definitions and running scans with anti-virus, anti-spyware and anti-rootkit software?

- Are vendor software websites regularly checked for alerts about new vulnerabilities and patches?
- Are all system/audit logs that relate to the handling of personal information regularly monitored?
- Are procedures in place to ensure that security events (e.g. unauthorized access, unsuccessful system access attempts, etc.) are identified, recorded, reviewed and responded to promptly?
- Are backup processes in place to protect essential business information such as production servers, critical network components, configuration backup, etc?
- Are there controls that prevent or detect unauthorized software?
- Is there a patch management process for new security vulnerabilities?

Question 5.1.4 asks you to describe the **administrative security measures** taken to protect the PI. These cover a range of organizational activities and are generally intended to control human behaviour through policies, procedures and agreements. Many of these will guide and support the implementation of physical and technical security measures.

Issues to be addressed by administrative security measures include security management functions, assigned security responsibility, workforce security, information access management, security awareness and training, security incident reporting, contingency planning, evaluation, and third party service providers.

Security management functions include risk assessments of the vulnerability of the system, sanctioned policy for employees who do not comply with policies and procedures, and security review procedures to ensure records of system activity are reviewed (review of audit logs, access reports, and security incident tracking reports).

Assigned security responsibility means an individual within the organisation needs to be assigned responsibility for overseeing the development of policies and procedures, training staff, and monitoring compliance.

Workforce security includes the policies and procedures needed to govern mechanisms to prevent employees from having unauthorised access to information. Onboarding clearance procedures and termination procedures are examples of workforce security controls.

Information access management includes the policies and procedures needed to articulate and govern access controls – they incorporate information about employees' 'need to know'.

Security and privacy awareness and training are mechanisms that inform employees of legislated and corporate requirements and expectations.

Security incident reporting includes written practices that need to be in place to address a security or privacy breach.

Contingency plans are policies and procedures that need to encompass the following: data backup planning, disaster recovery planning, and emergency mode operation planning.

Evaluation includes regularly scheduled evaluation processes that need to be encompassed within existing policies and procedures to ensure the effectiveness of security measures are tested.

Policies and procedures need to ensure formal agreements between third party service providers and clients need to be in place, and that these agreements fulfill the requirements of the governing privacy legislation. For example, Information Management Service Agreements (IMSA) may be required under section 33.

Here are some questions to ask:

- Are employees aware of or affirmed in writing they have read and understood corporate privacy policies?
- Are agreements in place for PI shared between your program and another party?
- Do all contracts that involve PI contain a privacy protection schedule?
- If information management services are part of a contracted service, has a written agreement (Information Management Service Agreement) been embedded in the contract?
- Are employees required to sign confidentiality agreements?
- Are potential employees who will have access to personal information adequately and appropriately screened?
- Is there a process to ensure immediate recovery of keys and pass cards, and for withdrawing access privileges and termination (voluntary or involuntary) occurs?
- Is there a contingency plan (including Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan)?
- Are standards in place on the use of various communications media (both physical and electronic media)?
- Is there a policy governing the use of mobile devices and removable media if being used to store PI?

Question 5.1.5 asks you if staff have completed the access and privacy training in YGLearn. This question is included to highlight the need for staff to complete training to ensure compliance with section 9 of the *ATIPP Regulation*. Privacy training for employees is one of the most effective ways to prevent privacy breaches.

Question 5.1.6 asks you if staff is aware of how to respond to suspected unauthorized collection of PI and privacy breaches. This question highlights the need to communicate existing policies and practices to staff in order to operationalize successfully.

5.2 Security Risks

This is where you identify any risks related to the security of PI, along with strategies for mitigation, the person responsible for mitigation activities, and timeline for completion. If a STRA has been completed, you can include the ***mitigation strategy*** from the STRA as an appendix instead of completing the table.

Common ways in which the security of information may be compromised are:

- Confidentiality:
  - failing to encrypt information while it is being stored or in transit;
  - failing to control access to the information; and
  - failing to train staff about their obligation to keep information confidential.
- Integrity:
  - failing to ensure information is not corrupted
- Availability:
  - failing to ensure information is made available to authorized users when needed.
- Authentication:
  - failing to confirm the identity of people to a system.

Section 6. ACCURACY, CORRECTION, RETENTION

Section 22 of the *ATIPP Act* stipulates that if an individual's PI is used by to make a decision that directly affects that individual, there must be reasonable measures in place to ensure that the PI is accurate and complete and retained for at least one year after the decision is made. The *ATIPP Act* also gives individuals the right to request correction of their PI (section 35). The intention of this section of the PIA is to ensure that your initiative is in compliance with these sections of the Act.

6.1 Using personal information

Question 6.1.1 asks if your initiative uses PI to make decisions that directly affect individuals. This is where you'll document the use of PI for such purposes to ensure that you are aware of all instances where/when this is occurring. For example, if an individual's birthdate is used to determine eligibility for a benefit or service, the individual's PI has been used to make a decision that directly affects them (that is, whether or not they receive that benefit or service). By being aware of and documenting all instances, you will be able to appropriately retain the information.

Question 6.1.2 asks you to describe the measures you will take to confirm accuracy and completeness of collected PI to ensure it is accurate, complete and up-to-date for the required purpose. This highlights how the review and documentation of such processes is key to ensuring that adequate processes are in place. Examples include: error-proofing forms, manually verifying information before decisions are made, getting PI directly from an individual, and periodically checking databases.

Question 6.1.3 asks you if an information management service is used as a part of your initiative. This is to prompt you to identify if information management services are being utilized so that a written agreement is entered into as per section 33 of the *ATIPP Act*. The ATIPP Office has a created a template called an Information Management Service Agreement (IMSA) to accommodate these situations. An IMSA is drawn up to fulfill requirements of the *ATIPP Act* and ensure that privacy and security requirements for protection of information are agreed to by a third party service provider (Information Manager) when information is managed and stored by a third party. Please contact us at privacy@yukon.ca if you have questions.

Question 6.1.4 asks you to describe how PI is not kept for longer than is necessary. This is to ensure PI is retained only as long as necessary for the fulfillment of the stated purposes and will decrease risks associated with retaining PI for longer than required.

6.2 Correcting personal information

Question 6.2.1 asks you to describe how an individual's PI can be updated or corrected to enable compliance with section 35 of the *ATIPP Act*. Individuals have a right to request a correction to their PI if they believe it is wrong or incomplete.

Here are some questions to ask:

- Is a policy or procedure in place?
- Do individuals have the ability to update their own PI?
- Will notes or a record be made on a government case file?
- Will PI provided be checked for accuracy? – and,
- What steps are taken to notify parties the PI was shared with of the corrections?

6.3 Records Retention and Disposition

Question 6.3.1 asks you to indicate which Records Retention and Disposition Schedule(s) apply to your initiative. Government records must be disposed of securely in accordance with approved records schedules. Records schedules contain retention periods (how long records can be kept) and disposition decisions (whether the records will be destroyed or transferred to Yukon Archives when the retention period has passed). You can contact your Departmental Records Officer for more information about the schedules that apply to your initiative.

Question 6.3.2 asks you to describe how retention and disposition will be enacted within the electronic system(s) that maintain the records. This is to ensure that a method to appropriately dispose of the PI is incorporated into systems that maintain the information.

6.4 Accuracy, Correction, Use and Retention Risks

This is where you identify any risks related to the accuracy, correction, use and retention of PI, along with strategies for mitigation, the person responsible for mitigation activities, and timeline for completion.

Common risks associated with accuracy, use, and retention include:

- not having retention and disposition defined and authorized through applicable records schedules;
- keeping PI for too long or not long enough;
- lacking processes for correction of PI or the ability to do so in an information system; and
- lacking processes for checking accuracy of PI collected.

Section 7: DISCLOSURE OF PERSONAL INFORMATION

The intention of this section is to ensure that PI is only used and disclosed in compliance with relevant legislation and that appropriate agreements are in place.

7.1 Routine Disclosures

Question 7.1.1 asks you if your initiative will involve routine or systematic disclosures of PI. If this is the case, you must identify from whom or to whom the PI is being routinely disclosed and for what purpose. If this is the case, you will need to attach your Information Sharing Agreement (ISA). If you have not completed an ISA, please contact the ATIPP Office for assistance.

Here are some questions to ask:

- For what purpose will the PI be used or disclosed?
- What organization will the information be disclosed to?
- Has consideration has been given to de-identify the information?
- Will data-linking occur?
- Will unique identifiers will be used or assigned?
- Will an agreement be entered into? If yes - attach the ISA(s) that relate the disclosure(s) as an appendix.

Question 7.1.2 asks you if your initiative discloses PI for a research or statistical purpose. Please see ATIPP section 26 for more information about requirements in this circumstance. If information is being disclosed for this purpose, you will need to attach your Research Agreement. If you have not completed a Research Agreement, please contact the ATIPP Office at privacy@yukon.ca for assistance.

7.2 Disclosure Risks

This is where you identify any risks related to the disclosure of PI, along with strategies for mitigation, the person responsible for mitigation activities, and timeline for completion.

Common risks associated with disclosing (sharing) information include:

- failing to consider alternative approaches to sharing PI (de-identifying it or sharing aggregated data, for example);
- failing to make reasonable efforts to ensure the accuracy of the PI being shared;
- failing to clearly define the scope of an ISA such that only the minimum amount of PI required for the stated purpose is shared;
- unclear or inadequate purpose for secondary use(s) of the PI;
- failing to determine whether or not an individual's consent is required before disclosing the PI; and
- failing to ensure that the PI being shared is being protected by reasonable measures in order to preserve its confidentiality.