Access to Information and Protection of Privacy Training: Level 1

Employee Training Transcript

December 2020

MODULE 1: INTRODUCTION

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

Purposes of the A*TIPP* Act

1 To protect the privacy of individuals by controlling and limiting public bodies collection, use, and disclosure of personal information

2 For the prevention of privacy breaches by requiring public bodies to implement security measures to protect the personal information they hold.

3 To ensure individuals can access their personal information and a right to request a correction of it.

4 To require public bodies to make types or classes of information openly accessible without an access request.

5 To allow the public a right to access information held by public bodies (subject to specific exceptions) to ensure government transparency and to facilitate meaningful participation in the democratic process.

6 To provide the Information and Privacy Commissioner with powers and duties that enable the monitoring of public bodies' compliance with the Act and ensure decision-making and administration is conducted in accordance with the purposes of the Act.

[Slide 3]

The Act has 2 major parts:

Protection of Privacy

Access to Information

[Slide 4]

The Act provides the Information and Privacy Commissioner with powers and duties that enable monitoring of public bodies compliance with the Act. This is outside of government oversight.

[Slide 5]

To understand how the Act works and how it applies to you, we'll cover 9 topics in this course.

Module 1: Introduction

Module 2: Roles under the *Act*

Module 3: Privacy Impact Assessments

Module 4: Collecting personal information

Module 5: Using personal information

Module 6: Disclosing personal information

Module 7: Access requests

Module 8: Privacy Breaches

Module 9: Offences and penalties

[Slide 6]

What is ATIPP?

[Slide 7]

The *Access to Information and Protection of Privacy Act*, commonly referred to as the *ATIPP Act*, is a Yukon law that governs the right to access and the protection of information held by public bodies.

The *ATIPP Act* first came into force in 1996. In 2016, government completed a comprehensive review of the *Act*, and in 2018, the law was re-written.

[Slide 8]

There are two parts to the *Act*.

ACCESS

- Governs access to records held by a public body
- Guarantees access to records in the custody and control of public bodies, with specific exceptions to access
- Provides access to an individual's own personal information and the right to request corrections to this information

PRIVACY

- Governs the protection of privacy of personal information held by a public body
- Protects unauthorized collection, use and disclosure of personal information

In addition, the *Act* establishes a compliance authority and an independent review of decisions made by public bodies.

[Slide 9]

The 2020 update of the *Act* enhances these aspects by:

Increasing information available to the public to ensure transparency and accountability of the government

Requiring ministerial bodies to proactively publish certain types and classes of information (providing free info to the public)

Using a client-focused approach to management of personal information that enhances program and service delivery while protecting individual's rights to privacy

Requiring protection of personal information that aligns with public expectations in a modern context

[Slide 10]

What records are subject to the *ATIPP Act*?

[Slide 11]

The *Act* applies to all records regardless of the medium used to store or record the information.

[Slide 12]

A record is a storage medium in which information is contained and stored by does not include any software or mechanism used to store or produce the information.

A storage medium includes written, graphic, electronic, digital, photographic or audio media.

[Slide 13]

A record is held by a public body if the public body has physical possession of that record.

[Slide 14]

A public body holds the record when the record is in the custody or control of the head or an employee of the public body.

Employees of the public body include individuals who provide a service to the public body, which include individuals who provide a service to the public body, which includes contractors and volunteers.

[Slide 15]

ATIPP does apply to: All records held by a public body

ATIPP does not apply to:

- Records that are exempt from the Act: court records, specific records of judges and persons exercising similar powers, including their personal notes and draft decisions
- Certain types of materials specifically excluded from the Act, e.g. teaching materials, personal and constituency records of elected officials

[Slide 16]

Who does the *ATIPP Act* apply to?

[Slide 17]

The *ATIPP Act* applies to all public bodies as described in the Act.

If you are an employee of one of the three types of public bodies listed under the Act, ATIPP applies to all the records you create in the course of your employment.

[Slide 18]

Ministerial public bodies

Public bodies that have a Minister as the head.
Examples of ministerial public bodies are: the Department of Environment, the Public Service Commission and Yukon Liquor Corporation.

Statutory and Non-Statutory public bodies

Statutory or Non-Statutory public bodies and their heads are defined through *ATIPP Act Regulations*.

If you are a member of a board or committee, you may be designated as a program or activity of a ministerial public body. Check the *ATIPP Act Regulations* to see which type of public body you operate under.

[Slide 19]

Who is excluded from ATIPP?

The following groups are not considered to be public bodies under ATIPP

Court

Judge

Municipalities

Office of an officer of the Legislative Assembly

First Nation governments

Office of a member of the Legislative Assembly (MLA)

[Slide 20]

For employees of any public body under the Act, any record you create as an employee in the course of your work is subject to ATIPP.

[Slide 21]

What are some examples of records an employee might create?

Reports, contracts, handwritten notes

Text messages

Emails, online messaging

[Slide 22]

If you receive a request for records from your Designated Access Officer (DAO) to respond to an access request, you are required under the *ATIPP Act* to respond and provide all relevant records.

Purposefully withholding or deleting information is an offence under the law.

You will learn more about Designated Access Officers and other roles important to the Act in a later module.

[Slide 23]

What happens when ATIPP conflicts with another law?

[Slide 24]

When two laws (acts) conflict, one law has supreme authority or power over the other.

This is known as paramountcy and can impact how you respond to an information access request.

[Slide 25]

In general, application of the *ATIPP Act* is paramount over all other Yukon laws unless another act has a provision or section that specifically excludes application of the *ATIPP Act*.

Where these exemptions exist, provisions in the other act must be considered to determine the applicable statute (law).

[Slide 26]

Example

The *Land Titles Act*, provision 210 states the *ATIPP Act* does not apply to records kept by the registrar under Part 2, Division 3 of the *Act*.

This allows the Registrar of Land Titles to make specific personal information publicly available in order to fulfill their duties and powers under the *Act*. For example, the names of individuals and details of their owned property are not considered personal information protected under ATIPP.

[Slide 27]

Congratulations! You have finished reviewing the material in Module 1.

MODULE 2: ROLES UNDER THE *ACT*

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

Now that we understand the foundations of the *Access to Information and Protection of Privacy Act*, let's explore the various key roles involved in upholding ATIPP.

[Slide 3]

What are the key roles under ATIPP?

[Slide 4]

Access and Privacy Office (APO)

How they are appointed

Public body employee appointed by the Minister of Highways and Public Works

Role Responsibilities

- Operates the ATIPP Office and is the point of contact for access requests and responses on behalf of public bodies
- Responsible for accepting and refusing access requests, estimating costs, waivers, extensions, compliance inspection audits on public bodies, establishing an Access to Information Registry and publishing information related to Privacy Impact Assessments (PIAs) and protocols to unsure public bodies are following rules on standardization and compliance under the *Act*.

[Slide 5]

ATIPP Office

How they are appointed

Employees in the ATIPP Office may have delegated authority from the Access and Privacy Officer (APO)

Role Responsibilities

- Develop guidelines, best practices and provide assistance to public bodies in the administration of the legislation, as subject matter experts.
- Services include providing publicly available resources (manuals, toolkits, templates, information notes, training, etc.)

- Receives direction from the Access and Privacy Officer (APO) and may have duties or functions of the *ATIPP Act* delegated by the APO
- Provides centralized ATIPP Shared Services as Designated Access Officers for select ministerial public bodies

[Slide 6]

Head

How they are appointed

Heads of ministerial public bodies are ministers and may delegate their responsibilities to other employees, typically the DM.

Statutory & Non-Statutory public body heads are defined in the *ATIPP Act*. Heads of these public bodies are prescribed in the *ATIPP Act Regulations*

Role Responsibilities

- Responsible for decisions made under the *ATIPP Act* that relate to the public body
- Heads of ministerial bodies are defined as a MINISTER of a department, corporation or directorate in Government of Yukon.
- Ministers normally delegate ATIPP duties and functions to their Deputy Ministers, who become the Head through delegation
- The Designated Access Officer(s) (DAO) and Designated Privacy Officer (DPO) report directly to the head
- The head receives recommendations from the Access and Privacy Office (APO) and Information Privacy Commissioner (IPC)

[Slide 8]

Designated Privacy Officer (DPO)

How they are appointed

Designated by the head of the public body

Role Responsibilities

- One employee of a public body that is responsible for the public body's privacy compliance under part 2 of the *Act* (Protection of Privacy) in relation to unauthorized activities and privacy breaches
- The head of a public body may designate one employee as both officer positions - A Designated Access and Privacy officer (DAPO), to fulfill the functions and responsibilities of both positions under the *Act*

[Slide 9]

Information and Privacy Commissioner (IPC)

How they are appointed

Appointed by the Legislature

Role Responsibilities

- Appointed as an Officer of the Legislature to perform powers and duties under the *ATIPP Act*
- Operates the Office of the Information and Privacy Commissioner
- Receives complaints from the public regarding their rights under the *ATIPP Act* (e.g. personal information correction requests, privacy complaints, refusals to access to information)
- Conducts privacy compliance audits of public bodies
- Provides recommendations on privacy impact assessments

[Slide 10]

Congratulations! You have finished reviewing the material in Module 2.

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

One tool used to support compliance under the *Access to Information and Protection of Privacy Act* is a privacy impact assessment (PIA). Let's take a look at how a PIA is used.

[Slide 3]

What is a privacy impact assessment and when is it required?

[Slide 4]

A PIA is an assessment conducted by a Ministerial public body. It is used to assess privacy and security risks and to ensure adherence to the *ATIPP Act*.

PIAs are required to be conducted before the body carries out or provides a proposed or significant change to:

- Program or activity
- Specialized service
- Data-linking activity
- Information management service

What is a program, activity or service?

The *Access to Information and Protection of Privacy Act* provides a definition of a program or activity of a public body. For greater certainty, *ATIPP Act Protocols* provides clear rules on programs, activities and services to assist public bodies with complying with the *Act*.

A program or activity of a public body is:

Created through legislation, and

Receives public funding to operate

A service is provided to the public under a public body's program or activity. A service may also be provided internally to other public bodies.

Example: The Department of Community Services (public body), Community Development Division (program) Sport and Recreation Branch (activity) provides high performance athletic funding to local athletes (service) to support their attendance at competitive sporting events.

[Slide 5]

A PIA is a comprehensive document designed to ensure the public body evaluates the project or initiative for technical compliance with the *ATIPP Act* and privacy implications for individuals.

PIAs are not required for statutory and non-statutory public bodies, but are recommended as a best practice.

To assist ministerial public body employees understanding of PIAs, a Privacy and Security Assessment must be submitted to the ATIPP Office. This assessment will help determine if your project or initiative requires a PIA.

For assistance with this process, please contact the ATIPP Office.

[Slide 6]

1 A PIA is started at the business needs analysis or initiation phase of the project

2 The project manager tasked with the project or initiative for the program, activity or service change may work with a PIA development team to develop the PIA per *ATIPP Act* requirements.

Who is involved in a PIA development team?

A PIA development team is a collaborative team of specialists, which may include the project manager, program staff, IT specialists (department IP and corporate ICT), business analysts, information management specialists, and the system vendor (contractor)

3 As part of the PIA, the following documents may be included:

- Personal Information Map

What is a Personal Information Map?
A Personal Information Map is a tool used to inventory all personal information holdings of departments and its programs, and identifies the authorities for collection, use and disclosure.

- Security Threat Risk Assessment (STRA)

What is a Security Threat Risk Assessment?

A Security Threat Risk Assessment is used to assess digital security risks and adherence to security standards, such as ensuring information is stored in Canada.

4 All PIAs must be submitted to the ATIPP Office for review and recommendations.

PIAs for a specialized service or data-linking activity must be submitted both to the ATIPP Office and IPC for review and recommendations.

Although not required, it is best practice to submit all PIAs to the IPC.

5 The ATIPP Office and Information and Privacy Commissioner (if applicable) will provide the head of the public body with recommendations based on the submitted PIA.

The public body must respond to any recommendations.

6 The PIA is completed before changes to the program, activity, or service are implemented (before testing can commence, the system is turned on, prior to collecting any personal information)

[Slide 7]

Congratulations! You have finished reviewing the material in Module 3.

MODULE 4: COLLECTING PERSONAL INFORMATION

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

The *Access to Information and Protection of Privacy Act* dictates that public bodies cannot collect personal information unless it meets one of the criteria for collection outlined in the Act.

In this module, we will find out what constitutes personal information, when it can be collected, and how

[Slide 3]

What is personal information?

[Slide 4]

Personal information (PI) is recorded information about an identifiable individual.

The *ATIPP Act* provides a non-exhaustive definition of personal information.

Examples of personal information include, but are not limited to:

Financial, employment, education, and health information; Identification and contact information, and unique identifiers like a social insurance number or IP address.

[Slide 5]

If your department or program is not a custodian of *the Health Information Privacy Management Act (HIPMA)* or the activity is exempt from *HIPMA*, all information is personal information (PI) and governed by the *ATIPP Act*.

[Slide 6]

What is NOT personal information?

Business contact information of an individual, including a current or previous employee or service provider of a public body (contractor), is not considered personal information.

Business contact information is information that makes it possible to contact the individual at their place of business and includes their name, position, title, business phone number and e-mail address.

[Slide 7]

When are public bodies authorized to collect personal information?

[Slide 8]

Personal information can be collected if:

Collection is authorized or required under a Yukon or Federal Law

Collection directly relates to and is necessary for the purposes of 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, or providing or evaluation a specialized service in respect of which the public body is the personal identity manager or partner

[Slide 9]

Collection is for a law enforcement purpose (e.g. investigation that may lead to fines or jail)

Planning a proposed program or activity, specialized service or data-linking activity which the public body is the personal identity manager or a partner

Collection is for a prescribed purpose as outlined in *ATIPP Act Regulations*

[Slide 10]

Public bodies are bound by the *ATIPP Act* if they are collecting PI directly, or contracting a service provider to collect on their behalf.

Contracts and agreements must include terminology on how service providers will meet their ATIPP responsibilities as a service provider.

Public bodies can only collect the minimum amount of PI necessary to meet the purpose.

Information cannot be collected “just in case”, or because it may be “useful to have”.

Public bodies must ensure they are collecting the minimum PI necessary, and ensure it is accurate and complete prior to using it.

At times public bodies may receive PI they have not requested, such as unsolicited resumes or another department’s mail.

This is not considered a collection, however public bodies must handle or dispose of this information in accordance with the *ATIPP Act Regulations*.

[Slide 11]

What is required for collecting personal information?

[Slide 12]

Notice of direct collection

Public bodies are required to provide a collection notice in accordance with provisions in the ATIPP Act before collecting personal information (PI).

A notification can be in many forms, e.g. printed directly on a form, provided as a separate brochure accompanying the form, shown in a pop-up window linked to an online form, or a printed notice on the wall or counter

If you are unsure whether you require a collection notice, please contact the ATIPP Office for assistance.

[Slide 13]

Report unauthorized collection of PI

If you suspect any unauthorized collection of personal information is occurring, complete an Privacy Breach Reporting Form for Employees and submit it to the Designated Privacy Officer (DPO) of your public body.

All public body employees are required to report unauthorized collection under ATIPP.

[Slide 14]

Congratulations! You have finished reviewing the material in Module 4.

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

Now that we have a better understanding of how personal information can be collected, let's look at how it should be used and managed.

[Slide 3]

What is authorized use of personal information?

[Slide 4]

Public bodies can use personal information only for the purpose under which it was collected or for a consistent purpose. Use of information is limited to the extent necessary to carry out the purpose, in a reasonable manner.

The purpose may be to administer a program or activity; to provide a service; or to determine eligibility for a benefit.

[Slide 5]

A public body is authorized to use personal information if one or more of the following conditions are met:

- Use of PI aligns with the purpose it was originally collected for, for example to provide a benefit, or issue a license
- The PI is received from another public body/partner agency in accordance with the ATIPP Act provisions on authorized disclosure
- Use of PI prevents harm to or protects the health of an individual or the public
- Consent for use has been obtained by the individual

[Slide 6]

The "need to know" principle indicates that employees should only have access to personal information they need to know. This limits both the amount and type of PI that can be collected and used.

Employees should only be accessing personal information it when it is required to perform their job duties. Accessing information for any other reason (boredom or curiosity for example) is not an authorized use and is a privacy breach.

Another example of authorized use is when the Department of Finance uses personal information collected from an individual who applied for a benefit with another ministerial public body, for the purposes of remitting a payment to the individual.

[Slide 7]

What about the accuracy and retention of PI?

[Slide 8]

Public bodies are required to make every reasonable effort to ensure that personal information collected is accurate and complete.

How can PI be kept accurate?

Generally if a public body collects information directly, it is likely accurate as the individual typically signs a statement indicating the information is correct.

However, public bodies should have processes in place to verify accuracy of information, especially if that information affects the individual - e.g. their ability to obtain a license, grant, or benefit.

[Slide 9]

How long should PI be kept for?

If PI is collected to make a decision that impacts an individual, that information must be kept for a minimum of one year. This allows the individual to access, review, and correct that information.

Examples include when PI is collected to determine eligibility for income assistance, student loans, hiring decisions, etc.

Ministerial public bodies are required to use a records schedule to determine the retention period for PI. The *ATIPP Act* cannot be used to authorize the destruction of information in the absence of an approved record schedule.

[Slide 10]

A records schedule is a legal instrument that allows for the life-cycling of records and must be approved by the Yukon's Territorial Archivist, in accordance with the *Archives Act*. It determines:

- Period of Retention: How long records must be kept by the ministerial public body onsite and off-site
- Disposition: Whether the record can be destroyed or transferred to the Yukon Archives

[Slide 11]

Without an approved records schedule, information held by ministerial public bodies cannot be legally destroyed.

[Slide 12]

Knowingly destroying a record to prevent access to information is an offence under the *ATIPP Act*.

Additional information:

For information on records schedules, contact your Department Records Officer (DRO).

For information on whether your records are subject to the *Archives Act*, contact Yukon Archives

[Slide 13]

Report unauthorized use of PI

If you suspect any unauthorized use of personal information, complete a Privacy Breach Reporting Form for Employees and contact your Designated Privacy Officer (DPO).

All public body employees are required to report unauthorized use under ATIPP.

[Slide 14]

Congratulations! You have finished reviewing the material in Module 5.

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

In addition to collecting and using personal information, public bodies also have responsibilities around when and how they can disclose personal information.

[Slide 3]

What is disclosure?

[Slide 4]

Disclose means to release, reveal, expose, show, provide copies of, tell the contents of, or intentionally or unintentionally give personal information by any means to someone.

Personal information can only be disclosed under specific circumstances as defined by the *ATIPP Act*.

[Slide 5]

What are requirements around disclosure?

Administrative controls and practices need to be in place to ensure PI is only disclosed to authorized individuals.

When new programs are developed or existing program evaluated, disclosure practices should be reviewed to ensure they are authorized under the *Act*.

Requests for disclosure of PI need to be reviewed to understand the reasons behind the request. The disclosure should help the requester while remaining cost-efficient for the public body. The type and sensitivity of information should be weighed prior to sharing. Can the disclosure be made without providing non-identifiable information?

Records of disclosure should be kept to ensure compliance with requests made. If two or more parties are involved in the disclosure, a formal information sharing agreement is required to document the terms of the disclosure.

Requests for disclosures for research or statistical purposes must be evaluated - is it authorized under the *Act*? Before information can be disclosed, public bodies are required to enter into a written research agreement.

[Slide 6]

Report unauthorized disclosure of PI

If you suspect any unauthorized disclosure of personal information, complete a Privacy Breach Reporting Form for Employees and contact your Designated Privacy Officer (DPO). All public body employees are required to report unauthorized disclosure under ATIPP.

[Slide 7]

Congratulations! You have finished reviewing the material in Module 6.

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

Individuals have the right to access records held by a public body. There are no restrictions as to who can make a request. A requester can be anyone residing in or outside of Yukon, including individuals, corporations, and organizations.

[Slide 3]

What happens when a request for information was made?

[Slide 4]

Informal vs. Formal Requests for Information

A formal information request occurs when an individual submits a request in accordance with the *ATIPP Act*. This allows an individual with rights under the Act including the right to complain to the Information and Privacy Commissioner (IPC).

An informal request is when an individual requests information directly from a program or activity of a public body, without submitting an access request. In many cases, it is reasonable to provide an individual with their own personal information or program information without an ATIPP request.

[Slide 5]

An example of an informal request would be an individual requesting a copy of an application they submitted for a benefit, or information that the public body has already made public.

If you receive an informal request and are unsure if the information should be released, contact your Designated Access Officer or Designated Privacy Officer for assistance to avoid a privacy breach.

Now let's look at the steps involved for an access request.

[Slide 6]

A request is made to the ATIPP Office

- Formal requests are submitted to the ATIPP Office in order for the access part of the Act to apply
- All access requests are treated as confidential unless disclosing the identity of the requestor is required to respond or if consent has been given

- The Access and Privacy Officer (APO) must make reasonable efforts to help a requester in submitting their request

[Slide 7]

A request is made to the ATIPP Office

- ATIPP Office employees cannot tell a requestor exactly what they can ask for, review a request for wording or grammar, or inquire about the reason for the request
- Request can be for personal information ("I would like all information with my name from January to March 2019 from the Department of Economic Development") or for program information ("Emails sent to and from the Deputy Minister of the Department of Tourism and Culture on March 12 to 13, 2019)

[Slide 8]

The ATIPP Office forwards the access request to the relevant public body

- Access requests are sent to the Designated Access Officer (DAO) for the public body that must respond to the request.
- The public body must provide an Access Information Summary within 10 days of the request. This summary provides the basis for the ATIPP Office to calculate costs that may be associated with the request.

[Slide 9]

Records are collected

- Public bodies must search for all responsive records they hold, including electronic and paper records whether they are in the office, off site, or at another location.
- All employees who receive a request for records must respond on or before the date provided by their Designated Access Officer (DAO). A lack of response is reported to the head of the public body.
- As an employee, you must respond to a request whether you hold relevant records or not. If you do not hold records related to the request, tell your DAO as soon as possible.

[Slide 10]

Records are collected

Duty to Respond

- All employees of public bodies are required under the Act to provide information as requested to their Designated Access Officer (DAO).
- If you do not respond, the DAO is required to report the lack of response to the Head.

- For ministerial public body employees, this provision means if you ignore or refuse direction from your DAO, your lack of response will be reported to your Deputy Minister

[Slide 11]

Records are collected

TIP: Reach out to your Designated Access Officer (DAO)!

The DAO is there to assist with responding to requests. You can contact your DAO if:

- The access request is confusing or unclear.
- You do not have any relevant records but are aware there is another public body that may be able to respond to the request.
- You believe responding to the request will negatively impact the program - e.g. affect negotiations with a contractor or potential litigation.
- The access request will result in a large amount of records (500+ pages).

[Slide 12]

Access is granted

- Access requests can be granted in full, part, or refused
- Some requests may require a payment from the applicant before information is released
- If requests include information from a third party, the public body may need to consult with the third party before information can be released. A third party could be an individual or a business.

[Slide 13]

Congratulations! You have finished reviewing the material in Module 7.

MODULE 8: PRIVACY BREACHES

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

The *Access to Information and Protection of Privacy Act* defines a privacy breach of personal information as the theft or loss of, or unauthorized use, disclosure or disposal of personal information.

Privacy breaches can be intentional or unintentional. They may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

What happens when there is a privacy breach?

[Slide 3]

What is a privacy breach?

[Slide 4]

The *ATIPP Act* defines a privacy breach as the theft or loss of, or unauthorized use, disclosure or disposal of personal information.

[Slide 5]

Common examples of privacy breaches are:

- Personal information being mailed or faxed to the wrong recipient
- Loss or theft of equipment containing personal information such as USB sticks, external hard drives, or laptops
- An employee accessing personal information without a legitimate work purpose (snooping)
- Disposal of equipment or paper without secure destruction, or in violation of an Act
- Absent or inadequate provisions in a contract or agreement to protect personal information
- Phishing or deceptive tactics used to trick people into disclosing personal information directly, or through a fake website
- A cyber-attack on a system that contains personal information

[Slide 6]

Examples of privacy breaches

Disposal of equipment or paper records without secure destruction of the personal information

Cyber attack on a system

The absence of provisions or inadequate provisions to protect privacy in contracts or in information-sharing agreements involving personal information

Loss or theft of equipment containing personal information, such as external hard drives, laptops or memory sticks

Phishing or the use of deceptive tactics to trick an individual into providing their personal information

Personal information being mailed, faxed or emailed to the wrong address, email address or fax number

[Slide 7]

How can personal information be protected?

There are many ways to reduce or eliminate unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction of information.

Generally, this involves limiting the amount of PI collected, and the number of individuals who may access it. Security measures should be equal to how sensitive the information is.

Employees should take all reasonable steps in their daily activities to reduce or limit exposing themselves to a potential breach. These steps can be broken into 3 categories: physical security, administrative security and technological security.

[Slide 8]

What happens if there is a suspected privacy breach?

1. Use any containment measures needed to limit the breach (e.g. stop the unauthorized practice, recover the records, or shut down the system that was breached)

2. Notify your Designated Privacy Officer (DPO) of the suspected breach. It is important to do this as soon as possible

3. The DPO will assess the situation to determine whether a breach occurred

4. If the DPO determines a breach has occurred, they will initiate an investigation to determine the facts of the breach and determine the risk of harm.

[Slide 9]

5. Provide all information requested by the DPO as soon as possible. Do not destroy or remove evidence as employees are required under the *ATIPP Act* to provide information to their DPO when requested

6. If a significant risk of harm has occurred, the head of the public body must be notified, as well as the affected individual(s) and the Information Privacy Commissioner (IPC). If the public body involved in the breach is a ministerial body, the Access and Privacy Officer (APO) must also be notified.

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

In assessing significant harm, the DPO will consider the sensitivity of the personal information involved and the likelihood that it has, is, or will be misused.

7. A privacy breach report is created, identifying risks to the public body and opportunities to correct the collection, use, and disclosure practices of personal information to reduce risk.

A privacy breach report details what factors were involved in the breach and recommendations for changes that can prevent similar breaches in the future. This may include changes to physical, administrative or technical security measures; creation of policies; provision of privacy training, etc.

[Slide 10]

REMEMBER: As an employee, you are required by the *ATIPP Act* to report any suspicions to your Designated Privacy Officer (DPO).

Reporting what you believe is unauthorized collection, use, or disclosure of personal information allows your DPO to evaluate the situation, prevent a breach before it occurs, or implement mitigations to reduce the number of individuals affected.

Reporting a suspicion is an important breach prevention tool. For example, snooping may not have occurred if the public body was conducting regular system audits and periodically reviewing user access to the system.

[Slide 11]

Congratulations! You have finished reviewing the material in Module 8.

MODULE 9: OFFENCES AND PENALTIES

[Slide 1]

Introduction to the *Access to Information and Protection of Privacy Act*

Training Level 1

[Slide 2]

An offence under the A*TIPP Act* occurs when an individual commits an offence as outlined in section 121.

In the case of offences under the *Access to Information and Protection of Privacy Act*, a person who commits the offence may be liable to:

- A fine of up to $25,000
- Up to 6 months in jail.

[Slide 3]

It's important to understand what constitutes an offence - which is the topic of this last module.

[Slide 4]

What constitutes an offence?

[Slide 5]

The *Access to Information and Protection of Privacy Act* details actions that are considered offences under the *Act*.

- Violating any provision related to prohibited collection, use, or disclosure of personal information
- Knowingly obstructing or making false statements to the Information and Privacy Commissioner, delegate, or other person exercising their duty under the *Act*
- Refusing to comply with a summons to appear or to produce records requested by the Information Privacy Commissioner (IPC)
- Breaching a term or condition in a research agreement with a public body

[Slide 6]

It is also an offence to alter, falsify, conceal, or dispose of information or a record (or to direct another person to do so) with the intent to hinder, impede or obstruct an applicant's right of access to information or to prevent a complete response to an access request from being provided under the *Act*.

[Slide 7]

If you receive an access request and find additional related records after you have already responded to your Designated Access Officer (DAO), this is NOT an offence. However, you must contact your Designated Access Officer immediately to inform them of the additional records that can be provided. Having a dedicated records program can help to mitigate this risk.

[Slide 8]

Congratulations! You have finished reviewing the material in Module 9.