TOOLKIT FOR DESIGNATED PRIVACY OFFICERS

PURPOSE

This toolkit was created for Designated Privacy Officers (DPOs) of public bodies. A DPO is a designated officer for a public body that has assigned functions and responsibilities under the *Access to Information and Protection of Privacy (ATIPP) Act and Regulations*.

This resource will outline DPO responsibilities and offer guidance to accomplish the tasks assigned to the role.

Specifically, this toolkit will describe what is required to respond to and assess unauthorized collection of personal information (PI), as well the process for assessing and reporting on privacy breaches.

This toolkit provides detailed guidance to help you manage breaches and complete the Designated Privacy Officer Breach Reporting Form. It will cover:

- Timelines when managing breaches;
- Determining risk of significant harm to affected individuals; and
- Notifications, including who should be notified, when and how this should occur.

Who designates Privacy Officers?

Heads of public bodies (or their delegates) have the task of designating DPOs.

The *ATIPP* Act requires the Head of a public body to designate **one** DPO for a public body. The ATIPP Office has created forms for this purpose: a form to designate the DPO is provided to Heads in the Toolkits for Heads of Public Bodies. The Designation form for Privacy Officers is also available in the Access to Information Registry.

Ministers are the Heads of Ministerial public bodies.

The Access to Information and Protection of Privacy (ATIPP) Regulation prescribes statutory bodies and entities as public bodies and include information about who is the Head for the statutory body/entity.

If you belong to a statutory body/entity listed in Schedule 1, Part 1 of the *ATIPP Regulations*, this means that your statutory body is prescribed as a program or activity of a Ministerial public body. In these situations, the DPO for the Ministerial public body

also serves as the DPO for the statutory body that is a program or activity of the Ministerial public body.

If you are a part of a statutory body/entity listed in Schedule 1, Part 2 or 3 of the *ATIPP Regulation*, this means that your statutory body/entity is a 'stand alone' public body and the prescribed Head for your organization needs to designate a DPO.

What is personal information?

When assessing whether an unauthorized collection of personal information (PI) or a privacy breach has occurred, it is important to identify any personal information involved. This section describes what is meant by personal information to ensure that any personal information involved is identified and included in your assessment.

The *ATIPP Act* provides a simple but broad definition of PI: "recorded information about an identifiable individual." Appendix A of the Designated Privacy Officer Breach Reporting Form contains a list of categories and examples of personal information and personal health information.

The following is a non-exhaustive list of examples considered to be personal information of an individual:

- Name, home, mailing or email address or phone number;
- Age, sex, gender identity or expression, or sexual orientation;
- Fingerprints, blood type or any other biometric information;
- Ethnicity or nationality;
- Current and past physical or mental health, including personal health information;
- Marital, family, education or employment status or history;
- Political or religious beliefs, associations or activities;
- Identifying number, symbol, or other particular assigned to an individual;
- Information of a financial or law enforcement nature (associated with an individual);
- Anyone else's opinions about the individual; and
- The individual's personal views or opinions, except if they are about someone else.

It is important to note that personal information (PI) includes information that can be combined with other information to identify a specific individual through association or inference. For example, if one links information such as ethnic origin to health information and only one person in a small town has this ethnic origin, revealing the ethnic origin has the potential to reveal sensitive health information about that individual.

Overview of DPO Responsibilities and Functions

DPOs have responsibilities related to:

- Assessing and responding to unauthorized collection of PI;
- Assessing suspected privacy breaches;
- Determining risk of significant harm to affected individuals if a breach has occurred;
- Notifying Heads and affected individuals if risk of significant harm is present;
- Notifying the Office of the Information and Privacy Commissioner (OIPC) when risk of significant harm is present, and also at least one day in advance if public notice of the breach is to be given;
- Completing breach reports, which include measures for containment and recommendations for mitigation;
- Providing breach reports to the OIPC if the breach involves risk of significant harm to individuals; and
- Providing the breach reports to the Access and Privacy Officer (APO) if the public body involved is a Ministerial public body and involves risk of significant harm to individuals.

Responsibilities fit into 2 main functions:

1. Assessing unauthorized collection of PI, and
2. Assessing and reporting on privacy breaches.

1. Unauthorized Collection

A public body may only collect the PI of an individual for the purposes outlined in section 15 of the *ATIPP Act*. Whenever a public body collects PI directly from individuals, it is required under section 17 of the Act to have a collection notice.

Unauthorized collection of personal information can occur when the PI collected is beyond the amount that is reasonably necessary to carry out the purpose for which the PI is collected and if the collection is not authorized under section 15 or 16 of the *ATIPP Act*.

The two steps below are triggered when an employee suspects an unauthorized collection of PI.

Step 1: Employee is to report unauthorized collection to DPO
Timeline: Immediately on learning of the unauthorized collection.

Public body employees who believe that an unauthorized collection of PI has occurred or is occurring must immediately report the suspected unauthorized collection to the Designated Privacy Officer (DPO).

Employees complete the Unauthorized Collection Reporting Form and provide this form to the DPO.

Step 2: Designated Privacy Officer to respond and assess
Recommended Timeline: Within 5 working days after unauthorized collection is discovered.

The DPO must take action when receiving a report of unauthorized collection of PI. This response involves:

- An assessment of the report – to accomplish this, the DPO can request more information about the unauthorized collection from the head and/or employee(s);
- Action to discontinue or prevent unauthorized collection if unauthorized collection has occurred/is occurring – this can involve the DPO directing any employee of the public body to take the required action;
- Action to dispose of the PI collected through unauthorized collection – the *ATIPP Regulations* specify that disposal must involve destroying it in accordance with policy/procedure such that it cannot be reasonably reconstructed or retrieved.

- In cases where the PI collected without authority is used to make a decision that directly affects an individual, the public body must ensure that PI is accurate and complete before making the decision, and retain the PI for at least one year after the decision is made.

2. Assessing and Reporting on Privacy Breaches

What is a Privacy Breach?

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

The most common privacy breaches occur when information of clients or employees is stolen, lost or mistakenly disclosed. Some examples of privacy breaches are:

- Faxes that go to the wrong number;
- The storage of the personal information on and subsequent loss of a flash drive/USB stick or hard drive that was not encrypted;
- A system that handles PI being hacked into;
- Snooping or browsing through information systems; and
- Sharing personal details about someone with others without authority under the ATIPP Act.

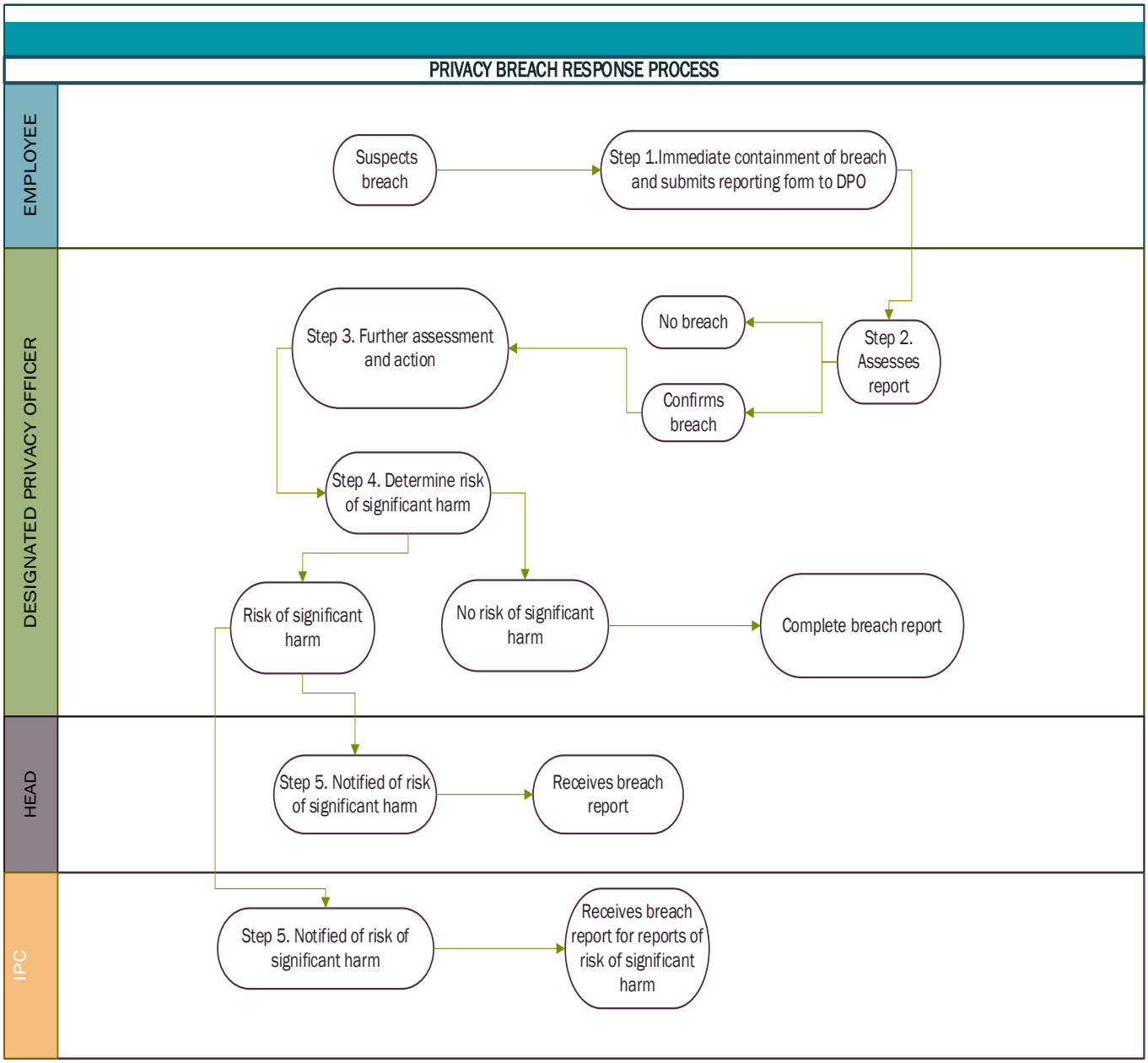
The *ATIPP Act* and *Regulations* define 'protection' of PI to include what is needed to protect the confidentiality, integrity, and availability of PI, as well as protecting it from a privacy breach.

Secure management of PI includes the requirement for public bodies to create and maintain the appropriate administrative, technical and physical security measures that protect PI against risks to unauthorized use and disclosure. These measures are formulated based on the types and sensitivity of PI at risk, benefits and costs of security measures, and risk of significant harm to individuals.

In the event of a privacy breach, DPOs have clear responsibilities that relate to the management of breaches. The steps below are triggered when an employee suspects a privacy breach has occurred or is occurring

Privacy Breaches – What to Do?

Steps involved in the privacy breach response process:



*** AFFECTED INDIVIDUALS MUST BE NOTIFIED WHEN THERE IS A RISK OF SIGNIFICANT HARM ***

* The Access and Privacy Officer must receive a copy of the breach report when risk of significant harm to individuals is present and the breach involves a Ministerial public body.

Breach Reporting

Step 1: Employee contains the breach to the degree possible

***Timeline:* Immediately**

Public body employees who suspect or observe a privacy breach must immediately take steps and get help if needed from their Designated Privacy Officer (DPO) to contain the breach.

Containment actions can include:

- Stopping the unauthorized practice;
- Recovering the information and have recipient confirm – in writing:
    - That no copies of the information were made,
    - That the information was not and will not be communicated, and
    - That all copies have been securely destroyed; and
- Revoking or changing computer access codes.

If the breach is a result of unauthorized access to an IT asset such as a computer, server or network, the device, system, or repository in question should be dealt with - contact the public body's IT support and/or Information and Communications Technology (ICT) in Highways and Public Works (HPW), whoever is applicable in the circumstances.

The employee completes the Privacy Breach Reporting Form for Employees and submits it to their DPO without delay. This enables the DPO to evaluate the situation and implement mitigations to reduce the number of individuals affected and/or involved. Reporting a suspicion or any perceived security vulnerabilities is an important breach prevention tool as it can enable a breach to be prevented before it occurs.

Note: Members of the public who suspect a breach of their PI has occurred may submit a Privacy Breach Complaint form or contact the ATIPP Office. The DPO of the department in question will respond to the complaint as outlined in the Privacy Complaint Policy.

Step 2: DPO assesses report to determine if breach has occurred

***Recommended timeline:* Same day as the breach is reported**

When DPOs receive a breach reporting form, they should be able to make a reasonable determination about whether or not a breach has occurred during the initial stage of the breach response.

Things to do to determine if a breach has occurred:

- Discuss the suspected breach with the employee, to gather facts and additional information if needed;
- Determine whether the suspected breach involves one or multiple public bodies; and
- Evaluate the suspected breach by reviewing the occurrence with the public body's governing legislation, as well as any existing agreements, policies, protocols and privacy compliance documents.

Note: Examples of privacy compliance documents and other administrative safeguards include Collection notices, Personal Information (PI) Maps, Privacy Impact Assessments (PIA), Information Management Service Agreements (IMSA), Service Level Agreements (SLA), Information Sharing Agreements (ISA) and Research Agreements.

Public body employees may report a suspected breach that when assessed, is determined to not be a breach. In this case, it is important to provide a clear rationale so that the individual understands why the suspected breach was not determined to be a breach. For example, something suspected as snooping could have been part of a system audit process/periodic review of user access. Be sure to document when a suspected breach occurs and does require a resulting breach report.

Step 3: Further assessment and action

Recommended timeline: *Immediately*

Once a breach has been confirmed to have occurred, immediate action may be required. If the breach is believed to have been a result of criminal activity, the RCMP should be notified immediately. If the notification includes the disclosure of PI to the RCMP, there must be the authority to disclose to RCMP. Any disclosures involving PI related to the process described in this section must have authority.

Appropriate containment measures, if not already enacted, must be deployed. This information – containment actions – is documented in Section 2 of the *Designated Privacy Officer Breach Reporting Form.*

Only individuals that can reasonably be determined to have a legitimate need-to-know should be informed of the breach. In this way, information is restricted to authorized employees that require it to carry out their work. Individuals are not entitled to know about breaches merely because of their status or rank. With breaches, the more people that are made aware, the wider the breach may become.

The affected program's director should be notified of the breach. In collaboration with the director, the DPO determines what member(s) of senior management, if any, should be notified. When a risk of significant harm is present, the Head must be notified.

At any time during the breach assessment process, public body employees and Designated Privacy Officers DPOs may contact the ATIPP Office for assistance with the breach.

If the breach involves other public bodies, other DPOs should be notified as required.

Note: An incident response team may be formed to examine the facts and assist with determining the cause and extent of the breach. This team can include representatives from the legal service branch, IT area and/or an individual from the affected program area. Incident response may require a communications plan for issuing a public statement if a risk of significant harm is evident.

Step 4: Determine Risk of Significant Harm
Recommended Timeline: 5 *working days*

Without delay after confirming that a breach has occurred, the DPO must determine whether the privacy breach introduces a risk of significant harm to affected individual(s).

To determine whether there is a risk of significant harm, the DPO must first determine any significant harm that is associated with the breach. A factor in this determination is the sensitivity of the information involved in the breach.

Significant harm includes bodily harm, 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.

Next, the DPO must determine if there is a risk, meaning "possibility" that the individual may suffer or be exposed to the significant harm. The custodian should consider the factors outlined in paragraphs 32(6)(a) through (h) of the *ATIPP Act* to make this determination.

Risk of significant harm can be determined by analysing these factors:

- The sensitivity of the personal information (PI) involved;
- The possibility that the PI is, has been, or will be used or disclosed in an unauthorized manner;
- How much time passed from the occurrence of the privacy breach and its discovery;
- The number of affected individuals;
- The type of relationship, if any, between affected individuals and any person who may have seen the PI (this is a factor of particular importance in a small jurisdiction such as the Yukon);
- The measures, if any, that the public body has implemented or is implementing to reduce the risk of significant harm to affected individuals;
- If the PI has been lost, stolen or disposed of, whether or not any of it has been recovered;
- The possibility that the information could be used for identity theft or fraud;

- How many people had access to the PI;
- Immediate containment and mitigation measures able to taken; and
- Any other available information that is relevant in the circumstances.

Note: Use Part 2 of the ATIPP Act (Protection of Privacy) as a resource. The factors used to determine risk of significant harm are outlined in Section 32 (6) a-h in the ATIPP Act.

Remember: breaches are impacted by **context**. Breaches involving a combination of personally identifiable information typically involve more risk than those involving only a single piece of (non-sensitive) PI. Combinations that involve highly sensitive information (name + *SIN number*) are most always assessed as causing a risk significant harm. The combination of unauthorized disclosure of PI including name of individual, date of birth and address can cause a high risk for identity theft or fraud.

If risk of significant harm is identified for one or more individuals, continue on to **Step 5 – Notification.** This information – risk of significant harm analysis – is documented in Section 3 of the *Designated Privacy Officer Breach Reporting Form*. For an example of a breach scenario that includes a risk of significant harm to affected individuals, jump to the end of this document.

If the outcome of the analysis reveals no risk of significant harm to affected individual(s), continue to **Step 6 - Complete DPO Breach Reporting Form** section.

Step 5: Notification

***Recommended Timeline:* Within 2 – 3 weeks**

Risk of significant harm triggers immediate notification to applicable Head(s), affected individual(s) and to the Office of the Information and Privacy Commissioner (OIPC).

If there is a risk of significant harm, all affected individuals MUST be notified and this is required under section 32(7)(b) of the ATIPP Act.

This means that notifications should be instigated prior to fully completing the breach report. After notifications are accomplished, circle back to completing the form.

Direct notification to affected individuals is required unless one of the circumstances in Section 10 of the *ATIPP Regulations* is present. Section 10 of the *ATIPP Regulations* prescribes the circumstances under which public notices may be provided rather than notifying individuals directly.

These circumstances include when the public body does not have accurate contact information for affected individuals or when the DPO has determined that providing the notice directly to the affected individuals would unreasonably interfere with the public body's operations.

If public notice is to be given due to the public body not having accurate contact information or determining that direct notice would interfere with the public body's operations, the OIPC must be notified at least one (1) day in advance, and the *ATIPP Regulations* indicate what must be included in the public notice and the notice to the OIPC.

Section 10 of the *ATIPP Regulations* also prescribe what information must be included in a public notice, and that a written copy of the notice must be retained by the public body for a period of at least one year after the notice was provided to the public.

Note: Both direct and public notices to individuals affected by risk of significant harm must contain certain information as prescribed by the ATIPP Regulations. See Section 10 (7) of the *ATIPP Regulations*.

When notifying affected individuals, all public bodies are required to use the Privacy Breach Notification Template provided by the ATIPP Office.

Step 5: Complete Designated Privacy Officer Breach Reporting Form

***Recommended Timeline:* Within 4 – 6 weeks**

Suspected breaches and actions taken to respond to breaches are documented in a breach report. Describe the incident without identifying the affected individual(s).

It is important to communicate to employees that they should not discuss a suspected breach, or share information with others. Although this may be done with good intentions for mitigation purposes, it could work against the public body by expanding the breach to a wider group.

Some older systems do not have easily obtainable audit reporting and may require third party assistance (ICT, system developers) to produce audit reports.

If it's necessary to collect information to complete the report, any documents transmitted electronically that include personal information should use Secure File Transfer (SFT). Remember to redact any personal information (PI) of the affected individuals that is contained in these documents if they are attached as appendices to the report.

How to fill out the form?

To complete the breach report, the "who, what, when, where and why" surrounding the circumstances should be asked and answered. Here are some examples of questions to help describe the circumstances:

- Did the breach involve paper or electronic records?
- Was the breach due to improper access controls related to a lack of controlling tight permissions for a system? For example, is the breach due to a previous employee (or contractor) having access to a system they no longer should be using?
- Are permissions restricted only to employees who have a legitimate work purpose?
- Is PI accessed off-hours, or is there a record of suspicious log-in activity that may suggest an employee's log-in information has been breached?
- Is there a pattern of PI being accessed or downloaded that is suspicious?
- Has PI been shared (disclosed) outside of the program, activity or service area?
- Has a contractor collected PI and used it outside the approved stated purpose in the contract?
- Is a supplier using a system that lacks approved security standards for storing PI?
- Is the breach due to a lack of internal policies, guidance or training on setting permissions, or restricting access to specific groups or users?
- Was the information used or disclosed outside of or beyond the initial breach?
- Was the breach a consequence of not having adequate systems for managing records?
- Was the breach connected to lack of compliance in relation to a Research Agreement, Information Sharing Agreement, or Information Management Agreement?

Note: Recommended best practice is to establish a consistent **naming convention** for reports. Here is the ATIPP Office's naming convention:
Document Acronym - Public Body Acronym - Current year – Sequential number
Example: PB-HPW-2021-01
(PB = Privacy Breach, HPW = Department of Highways and Public Works)

Be clear about whether the cause was due to failed physical, technical or administrative safeguards. For example, if the breach resulted from weak administrative security measures and mitigation strategies only focus on physical safeguards, future breaches related to administrative process could occur again.

Please consult Guidance on Safeguarding Information Assets in the Access to Information Registry for more information about security safeguards.

In some cases, a security audit may be necessary. After a privacy breach occurs, be sure to make any needed changes to be diligent to prevent future breaches. Depending on the type of breach, some necessary activities include:

- Create or update policies, user agreements, contracts, Information Management Service Agreements, and other administrative security measures;
- Review and implement necessary changes to technical and physical security measures and ensure necessary standards for compliance are in place;
- Update the Breach Reporting Form as needed to reflect mitigation recommendations lessons learned from the breach;
- Develop or improve, as necessary, adequate long-term safeguards against further breaches;
- Audit at the end of the mitigation process to ensure that any prevention strategies have been fully implemented;
- Associate timelines with prevention strategy; and
- Ensure all employees have taken privacy training.

Note: Always remember - when you are able to understand the cause of the breach, it's possible to make needed improvements.

For breaches that involve a risk of significant harm to individual(s), a copy of the completed report must be provided to the Office of the Information and Privacy Commissioner and Access and Privacy Officer. The submission to the Access and Privacy Officer is only required if the breach involves a Ministerial public body.

Privacy Breach Example

Here is an example of a privacy breach that helps to illustrate the process:

Highways and Public Works = HPW
Corporate Information Management = CIM
Employee #1 in HPW = E1
Employee #2 in HPW = E2

E1 lost a USB that contains the employment information of ten (10) individuals. The employee information includes the following PI: name, date-of-birth, residential address, personal phone number, employee number, employment history and performance evaluations.

This reveals a privacy breach has happened because a loss of PI has occurred. The situation also involves a violation of security measures (see: Secure management of personal information ATIPP Regulations section 9).

Containment measures:

When E1 realised the USB was missing, they took the following steps:

1. Tried to locate the lost USB - retraced their steps, searched their office and vehicle;
2. Contacted the government office where they had been with the USB and discovered that E2 (a colleague in the same department) confirmed they were in possession of the USB;
3. E1 retrieved the USB from E2 - unfortunately, E2 confirmed they had accessed the contents of the USB;

This reveals unauthorized use (see: Use only if authorized ATIPP Act section 21) and also involves a violation of security measures (see: Secure management of personal information ATIPP Regulations section 9).

4. E1 asked E2 to confirm they knew the individuals whose information they accessed and E2 knew the individuals;
5. E1 asked E2 to confirm, in writing, that no copies of the USB were made and the information they viewed will not be communicated; and
6. E1 completes Privacy Breach Reporting Form for Employees without delay and provides it to the DPO.

Risk of Significant Harm Analysis

This scenario reveals a **Risk of Significant Harm** because E2 knows the individual and now knows all the information contained on the USB about them, including their performance evaluations. E2 can confirm that no copies of the USB were made and that the information they viewed will not be communicated, but it does not erase what they learned about the individuals. The individuals whose performance evaluations were revealed to this individual have a right to know that this has occurred as they may be embarrassed or humiliated. To address the risk of significant harm, E2 needs to also know that the employees affected will be notified of the privacy breach. When the breach report is completed, it must be submitted to the Office of the Information and Privacy Commissioner and the Access and Privacy Officer.