PRIVACY IMPACT ASSESSMENT

A Guidance Document

ACKNOWLEDGEMENTS

This resource was created by using resources developed by Office of the Information and Privacy Commissioners from across Canada, In particular, we relied heavily on resources developed by Ontario's Office of the Information and Privacy Commissioner as well as Alberta's Office of the Information and Privacy Commissioner.

Privacy Impact Assessment

A GUIDANCE DOCUMENT

INTRODUCTION

What is a Privacy Impact Assessment (PIA)?

A PIA is a process that assists organizations in assessing whether a project, program, or process complies with the applicable access and privacy legislation. In Saskatchewan, government institutions are subject to *The Freedom of Information and Protection of Privacy Act* (FOIP), local authorities are subject to *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), and trustees are subject to *The Health Information Protection Act* (HIPA). FOIP, LA FOIP, and HIPA (herein referred to as "the legislation") set out rules as to how personal information/personal health information (PI/PHI) are to be collected, used, and/or disclosed. When a project, program, process is being designed, a PIA should be used to identify areas where there may be a privacy impact or risk.

For the sake of simplicity, whenever this document refers to a "project", that term could mean project, program, or process.

What is a privacy impact?

A "privacy impact" is when there are inadequate safeguards to protect PI/PHI, or the legislation does not authorize collection, use, and/or disclosure of PI/PHI.

How to use this guide

The goal is to guide government institutions, local authorities, and trustees in identifying privacy impacts and solutions to ensure safeguards are in place to protect PI/PHI to the greatest extent possible as well as to ensure compliance with the applicable privacy legislation. This document is meant to be a guide and not a definitive method of conducting a PIA.

What can I expect in the PIA process?

Although an organization's Privacy Officer often takes the lead on conducting PIAs, employees and representatives from participating program area, branch, division, business unit, other institutions and third parties can expect to be involved in the PIA process. The PIA process can only be effective if it comprehensively reviews the project.

The PIA process is not a short exercise and it can require a lot of time and effort depending on the complexity of the project. Further, the PIA process is not a stand-alone, one-time exercise. As projects are designed, developed, implemented, and carried out, privacy impacts may arise and will need to be addressed.

What do I do if I identify a privacy impact?

When a privacy impact is identified, that is an opportunity for organizations to make adjustments to the project to ensure PI/PHI is protected to the greatest extent possible and to be in compliance with the legislation.

For example, if the PIA reveals there is no legal authority for the collection, use, or disclosure of certain PI/PHI, then the organization should determine if such PI/PHI is required for the project. If not, then the exclusion of such PI/PHI in the project will assist the organization in eliminating a privacy impact but still carrying forward with the project.

Another example is if the PIA reveals that a contract is not in place between your organization and a third party service provider that adequately addresses how the third party is to manage PI/PHI. That is an opportunity for your organization to address this shortcoming.

STEP 1 |PRELIMINARY ANALYSIS

An organization should conduct a PIA when PI/PHI will be a part of a new project. If there are multiple organizations exchanging of PI/PHI within the project, each organization should conduct a PIA.

An organization should also conduct a PIA when PI/PHI will be a part of a new process being introduced into an already-existing project or program.

Therefore, before getting started on conducting a PIA, an organization should determine if PI/PHI is a part of the new project. This determination should be made at the early stages of the designing or development of a project.

If the new project does not involve PI/PHI, then a PIA is not required.

1.PROJECT DESCRIPTION

Provide a description of the project.

Project Title:	
Purpose/Objectives:	
Project lead (Name, contact information, and organization)	
List all organizations involved in the project.	
Additional information:	

2. INFORMATION INVOLVED

Identify the PI/PHI that will be involved in the project. Refer to the legislation for the definitions of PI/PHI.

If you check **"no"** to the first question (as in, there is no PI/PHI involved), then proceed to the third table below. If you check **"unknown"**, further consultations need to be made with the Project Lead or other key players involved in the project to determine if PI/PHI is involved.

	YES	No	Unknown
Does the project involved information about individuals in their personal capacity?			
If yes, list the group of individuals whose PI/PHI will be involved in the project (e.g. students, patients, senior citizens, etc.)			
If yes, list the types of PI/PHI that will be involved in the project.			

3. PRIVACY LEGISLATION

Identify application privacy legislation (check all that apply).

	YES	No	Unknown
***The Freedom of Information and Protection of Privacy Act* (FOIP)**			
***The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP)**			
***The Health Information Protection Act* (HIPA)**			

4.CONCLUSION

Document whether a PIA will need to be completed and the reasons for the decision. If PI/PHI is involved, then a PIA should be conducted. If PI/PHI is not involved, then a PIA does not have to be done.

	YES	No	Unknown
Does a PIA need to be completed?			
If you have checked "Yes" or "No", then document reasons for the decision			
If you have checked "Unknown", then document actions that need to be taken to make a determination if a PIA needs to be completed. Eventually, your organization needs to decide whether it needs a PIA or not.			

STEP 2 |DEFINE THE PROJECT

PIAs should be started at the early stages of the designing or development of a project. Having a good understanding of the purpose, objectives, and structure of the project will assist organizations in identifying the privacy impacts.

1.PROJECT DESCRIPTION

Provide a description of the project. This could be the same/similar to the Project Description documented in Step 1.

Project Title:	
Purpose/Objectives:	
Project Lead (Name, contact information, and organization)	
List all organizations involved in the project:	

2. PROJECT AUTHORITY

The applicable privacy legislation should have been identified in Step 1. Now, identify the regulatory and legal framework for the project. This includes the applicable legislation and regulations (other than the privacy legislation that has already been identified in step 1), bylaws, memoranda of understandings (MOU), agreements, contracts and other relevant instruments. Attach copies of relevant legislation, regulations, bylaws, MOUs, agreements, contracts and other relevant instruments to your PIA.

Name of legislation, regulation, MOU, contract or other relevant instruments	**Description**

3. PROJECT STRUCTURE

A PIA is focused on PI/PHI and the flow of the PI/PHI (collection, use, and/or disclosure) as part of a project. Identifying the organizations and program areas that will be handling PI/PHI will assist in identifying where privacy impacts may occur. If there is sharing of PI/PHI between organizations, developing an Information Sharing Agreement is a good idea. Check out the IPC's resource *Best Practices for Information Sharing Agreements* at www.oipc.sk.ca under the "Resources" tab for more information.

While it is not necessary, creating a visualization of the project may be helpful in explaining the project structure (see pages 11 and 12), as well as in completing the privacy analysis in Step 3.

3.1 List all organizations involved in developing or implementing the project

Organizations (government institutions, local authorities, health trustees, third parties)	Project Role	PI/PHI the organization will have in its possession or control

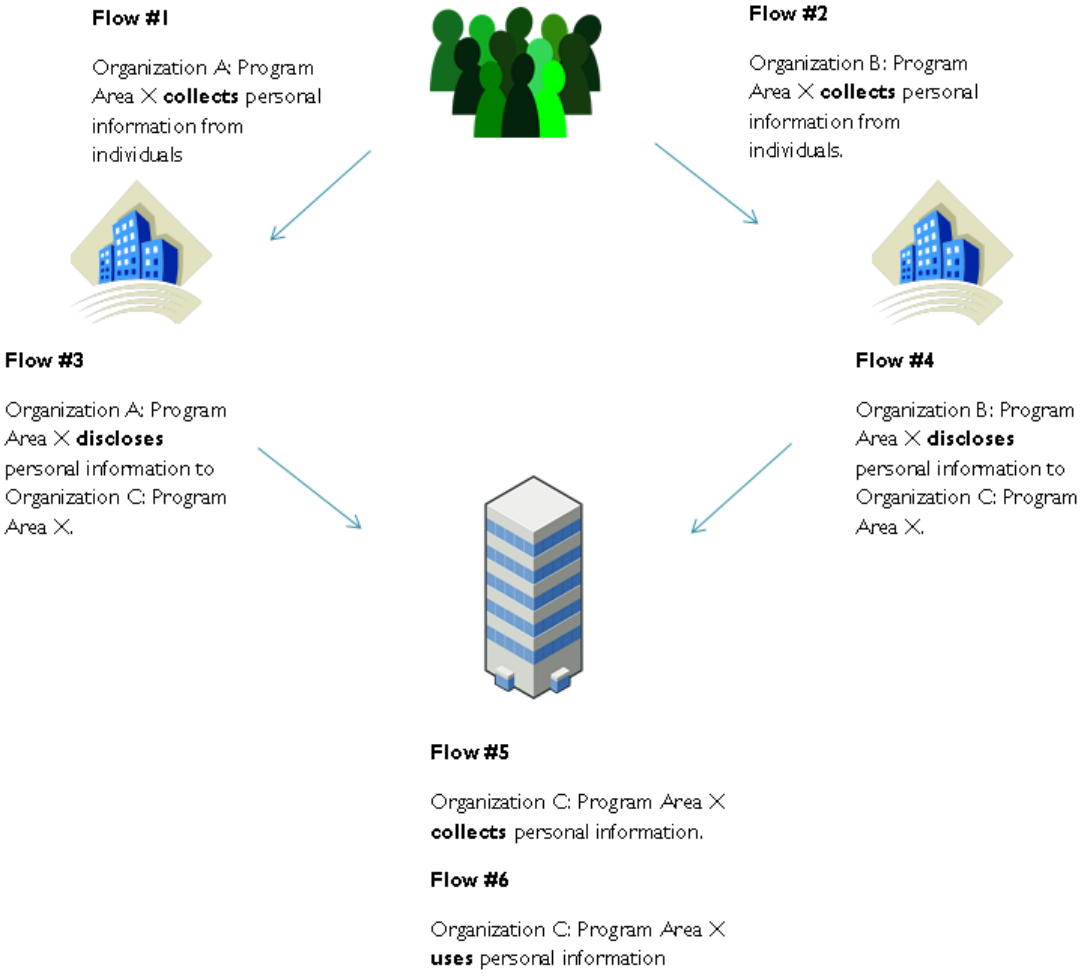
3.2 List contractors or service providers that will manage PI/PHI on behalf of your organization.

Contractors or service provider	Relationship to your organization	Project Role	PI/PHI the contractor or service provider will be managing	Instrument used to bound contractor or service provider to relevant privacy and security requirements (contract, memoranda of understanding, agreements, other)

3.3 Identify any location outside of the province where PI/PHI may be stored and the third parties involved.

PI/PHI stored outside the province	Location	Third party storing the PI/PHI outside of the province	Instrument used to bind third party to relevant privacy and security requirements

Example of a visualization of a project involving multiple organizations



Example of a visualization of a project that only involves one organization

Flow #1

Organization A: Program Area X **collects** personal information from individuals so the individuals can receive a service or benefit.

Flow #2

Organization A: Program Area X **uses** the personal information to provide a service or benefit

4.PROJECT CHARACTERISTICS

A PIA is focused on characteristics of a project that may present a privacy impact. The following questions are meant to help identify areas where there may be a privacy impact. The questions below are not a comprehensive list. Therefore, please use the space at the end of the table if there is any activity that you think may have a privacy impact.

Since PIAs should be started at the early stages of the design or development of a project, there may be a lot of "unknowns". If you check the "Unknown" box, use the "Additional Information/Action items" column to document what will be done to define the project characteristic.

	Yes	No	Unknown	Additional Information/Action items
Will information technology be used to transmit, process, and/or store PI/PHI?				
If information technology will be used, is your security department involved to ensure security policies and procedures are in place?				
Will electronic PI/PHI be stored within the province?				
If electronic PI/PHI will not be stored in the province, then have you determined what applicable legislation will apply to the electronic PI/PHI that would impact the safety of the data?				

If electronic PI/PHI will be stored in a different jurisdiction, what agreements are in place to ensure that your organization retains control over the electronic PI/PHI in order to comply with the legislation?				
Are policies and procedures in place, or being developed, to guide employees in handling the PI/PHI in this project? **Policies and/or procedures should include identifying the types of PI/PHI they will manage in the project, and the acceptable (and unacceptable ways they are to handle the PI/PHI)**				
Will training be given to employees on how to manage PI/PHI?				
Is your records management office involved to ensure records management policies and/or procedures are in place to manage the records in this project?				
Identify other activities that may present a privacy impact?				
Other comments:				

STEP 3 |PRIVACY ANALYSIS

PART 1: Collection, use, and disclosure

The following tables will ask a series of questions to assist organizations in determining if it is in compliance with the legislation. These following tables will deal with the:

- Collection,
- Use,
- Disclosure.

> **Collection** occurs when a public body gathers, acquires, receives or obtains PI/PHI.
>
> **Use** indicates the internal utilization of PI/PHI by a public body and includes sharing of the PI/PHI in such a way that it remains under the control of that public body.
>
> **Disclosure** is the sharing of PI/PHI with a separate entity, not a division or branch of the public body in possession or control of the PI/PHI.

The tables will also ask about safeguards that organizations can put into place to protect PI/PHI.

> Examples of **administrative safeguards** include policies, procedures, agreements, contracts, training resources.
>
> Examples of **technical safeguards** include protecting information through strong passwords and encryption, automatic log off features for computers (after a short time of user inactivity), and firewalls.

Examples of **physical safeguards** include locked filing cabinets, restricted access to areas containing personal information/personal health information, computer monitor privacy screens, and alarm systems.

If a visualization of the project was created in Step 2, it can be used to help with identifying where PI/PHI is collected, used, and disclosed. The tables below will assist in determining whether there is authority for each flow of PI/PHI. **The questions in the table should be applied to each flow of PI/PHI identified in the visualizations. If the flow deals with collection, then the collection table should be filled out. If the flow of the PI/PHI deals with use, then the use table should be filled out. If the flow of the PI/PHI deals with disclose, then the disclosure table should be filled out.**

A. Collection

Privacy Requirement Questions	Yes	No	Unknown	Explanation	Privacy Impact	Action Items
Name of Flow (example: Flow #1, Flow #2, etc.)						
Authority for flow (example: FOIP, LA FOIP, HIPA)						
Does the legislation authorize the collection of PI/PHI?						
Is there legislation besides FOIP, LA FOIP, and/or HIPA that addresses the collection of PI/PHI?						
Purpose of Collection						
Has the purpose of the collection been defined? What is the purpose of the collection?						
Notice to Individual						

Will notice of collection be given to the individual(s)? Explain timing, method of notification. If notice won't be given to the individual, give reasons and explain why the lack of notice is in compliance with subsection 26(3) of FOIP, 25(3) of LA FOIP, or 25(1)(c) of HIPA.						
Manner of Collection						
Will PI/PHI be collected directly from the individual?						
Will p PI/PHI be collected indirectly from another source? If so, explain the authority for the indirect collection.						
Data Minimization						
Is the project only collecting those pieces of PI/PHI it requires to achieve the project's purpose?						
What controls are in place to ensure the project only collects the information it requires? (Examples: Forms that asks for the PI/PHI hat is required, processes are in place to return extra PI/PHI						

that was collected, etc.)						
SAFEGUARDS						
Are there administrative safeguards in place to ensure only the PI/PHI that is required for the project is being collected? (Examples: Forms that only ask for the PI/PHI that is needed; policies, procedures, and training are in place so staff know what PI/PHI is to be collected. Attach copies of the policies, procedures and training material).						
Are there technical safeguards in place to ensure only the PI/PHI that is required for the project is being collected? (Examples: Forms that only ask for the PI/PHI that is needed.)						
Are there physical safeguards in place to ensure only the PI/PHI that is required for the project is being collected?						

B. USE

Privacy Requirement Questions	Yes	No	Unknown	Explanation	Privacy Impact	Action Items
Name of Flow (example: Flow #1, Flow #2, etc.)						
Authority for Flow (example: FOIP, LA FOIP, HIPA)						
Does the legislation authorize the use of the PI/PHI?						
Is there legislation besides FOIP, LA FOIP, HIPA that addresses the use of PI/PHI?						
Purpose						
Will the PI/PHI be used for the same purpose as the collection of PI/PHI?						
Will the PI/PHI be used for a purpose that is consistent with the purpose for the collection of PI/PHI?						
Will the PI/PHI be used for a secondary purpose? (ie, a purpose that is not the same as the purpose for the collection of						

PI/PHI). If so, please explain the authority for the secondary purpose.						
Standard of Accuracy						
Are there procedures in place so that your organization can verify that it has the most accurate and complete PI/PHI of an individual that it needs?						
Are there procedures in place so that individuals are able to request that their PI/PHI is corrected?						
Safeguards						
Are there administrative safeguards in place to ensure that PI/PHI will be used only for authorized purposes? (Examples: Policies, procedures, and training are in place so staff know how PI/PHI is to be used. Attach copies of the policies, procedures and training material).						
Are there technical safeguards in place to ensure PI/PHI will be used only for authorized purposes? (Example: staff are only given access to parts of databases that contains PI/PHI it needs to						

complete job duties; documents can be encrypted and/or password protected to ensure only intended recipients can open the documents; audits are completed to ensure staff only accessing PI/PHI it needs for job duties, etc.)						
Are there physical safeguards in place to ensure PI/PHI is used for authorized purposes? (Example: Only staff who require PI/PHI are given physical access to areas where PI/PHI is stored such as records rooms, filing cabinets, etc.).						

C. DISCLOSURE

Privacy Requirement Questions	Yes	No	Unknown	Explanation	Privacy Impact	Action Items
Name of Flow (example: Flow #1, Flow #2, etc.)						
Authority for Flow (example: FOIP, LA FOIP, HIPA)						
What is the authority for the disclosure of PI/PHI?						
Safeguards						

Are there administrative safeguards in place to ensure only the PI/PHI that needs to be disclosed is disclosed? (Example: Policies, procedures and training are in place so staff know how PI/PHI is to be disclosed. Attach copies of the policies, procedures and training material.)						
Are there technical safeguards in place to ensure PI/PHI will be used only for authorized purposes? (Example: staff is only given access to parts of databases that contains PI/PHI it needs to complete job duties; documents can be encrypted and/or password protected to ensure only intended recipients can open the documents; audits are completed to ensure staff only accessing PI/PHI it needs for job duties, etc.)						
Are there physical safeguards in place to ensure PI/PHI is disclosed for authorized purposes? (Example: consideration is given to how records containing PI/PHI is transported or delivered to recipient).						

PART 2: REMAINING PRIVACY CONSIDERATIONS

A. RECORDS MANAGEMENT

Privacy Requirement Questions	Yes	No	Unknown	Explanation	Privacy Impact	Action Items
RECORDS MANAGEMENT						
RETENTION						
Has your organization determined how the PI/PHI being collected, used, and/or disclosed is incorporated into the organization's records management system?						
Has the medium and format of the PI/PHI been defined?						
Has the organization determined how long it needs to retain the PI/PHI to be in compliance with applicable legal requirements?						
DISPOSITION						
Does the organization have procedures to guide the secure						

disposal of PI/PHI?						
Will details of the disposal of PI/PHI be recorded?						
If a third party is retained to dispose of PI/PHI, are contracts or agreements in place to ensure the secure disposal of PI/PHI? Attach copies of the contract or agreements to this PIA.						
If a third party is retained to dispose of PI/PHI, will the third party issue a certificate of destruction after the PI/PHI has been disposed of?						
Are there policies or procedures in place that guide employees on how to dispose of PI/PHI? Attach copies of those policies/procedures.						

B. PRIVACY MANAGEMENT

Privacy Requirement Questions	Yes	No	Unknown	Explanation	Privacy Impact	Action Items
ACCOUNTABILITY						
What tools are in place to monitor those involved in the management of PI/PHI in carrying out their roles and responsibilities? Explain. (Examples: contracts, agreements, policies, procedures, etc)						
Is there an employee within your organization that staff can report to if there are questions about the management of PI/PHI?						
Is there an employee that members of the public can contact if they have questions about the collection, use, disclosure, retention, or disposition of PI/PHI? This employee should be a person who is part of the program area who is leading the project. How is this employee's contact information made known to the						

public?						
Is there an employee that members of the public can contact if they want to request correction to their PI/PHI? How is this employee's contact information made known to the public?						
Is there an employee that members of the public can contact if they want to request access to their PI/PHI? How is this employee's contact information made known to the public?						
TRAINING						
Is training available to staff so that they understand the policies and procedures are in place to ensure the proper collection, use, disclosure, retention and disposition of PI/PHI?						
AUDITING						
Will your organization conduct audits to ensure that PI/PHI is being collected, used, disclosed, retained, and disposed of in accordance with the legislation?						

STEP 4 | PIA REPORT

The PIA Report should include the following:

1) Background/Summary of project

This section of the PIA Report should describe the project and establish the scope of the PIA.

2) Identify privacy impacts of project

Through the first three steps of the PIA process, privacy impacts such as areas where there is not adequate protection for PI/PHI and/or there are parts of the project that are not in compliance with the legislation. This section of the PIA Report should identify the privacy impacts.

3) Rate the privacy impact as high, medium, or low

Although not all privacy impacts can be eliminated, each privacy impact should be mitigated as much as possible. Rate each privacy impact as high, medium, or low to assist your organization in prioritizing action to mitigate privacy impacts.

4) Recommendations to mitigate privacy impacts

Recommendations should be made to address each privacy impact that has been identified. From these recommendations, a privacy risk mitigation strategy can be developed.

You might want to consider creating a table, such as the one below, which lists the privacy impact and the recommendation to mitigate the privacy impact.

Privacy Impact	Level of Privacy Impact (High/Medium/Low)	Recommended action to mitigate the privacy impact

Once the PIA Report is complete, the PIA should be given to the project lead so that the privacy risk mitigation strategy can be approved and implemented. As the project evolves and the privacy risk mitigation strategy is implemented, progress should be monitored and documented. Key questions to be asked are:

1) Has the privacy impact(s) been mitigated?
2) Has changes to the project introduced new privacy impacts?

The PIA process should be ongoing. As mitigation strategies are implemented, then the project should be evaluated to determine if the privacy impact has been addressed sufficiently or if new privacy impacts have been introduced.