

Conducting a Privacy Impact Assessment

Companion Guide for the Process and Documentation

April 2024

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

CAI Commission d'accès à l'information du Québec

Version 3.1 – April 2024

This guide was developed in 2021 by Commission d'accès à l'information du Québec. It takes into account *An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information* (Bill 25).

This version 3.1 has been revised visually and structurally, but the content remains essentially the same.

This guide concerns the Access Act and the Private Sector Privacy Act

This guide deals with the *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* (Access Act) and the *Act Respecting the Protection of Personal Information in the Private Sector* (Private Sector Privacy Act).

The text of this guide does not take into account any future changes that may be made by bills being studied or not yet in force on the date of the guide's publication. Public and private organizations must comply with existing legislation on the protection of personal information.

This guide is explanatory and does not replace the legislation

This guide is a helpful tool. The content is informative and intended to aid in understanding. In the event of any inconsistencies between the information being presented and the actual wording of the legislation, the latter will take precedence.

Icons used in the guide

The guide contains four types of information strips identified by their respective icons:

Terminology

Legal aspects

Recommendation or best practice

Disclaimer

The masculine refers to both women and men and is used only for ease of reading.

This guide may be reproduced in whole or in part provided the source is acknowledged and it is not used for commercial purposes.

If you have any comments about this guide, please contact us at veille@cai.gouv.qc.ca.
Please note that we will not necessarily respond to your comments, but they will be taken into consideration as we reflect on future updates to the guide.

For general questions on this guide, contact the Commission.

Note that the Commission does not provide legal advice or opinions.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Introduction

Purpose of the guide

This guide is designed to help you:

- Determine if you are required to complete a Privacy Impact Assessment (PIA) for a given project
- Complete the PIA
- Prepare a PIA report, as required
  – The guide enables better use to be made of the generic report template proposed by the Commission.

In this guide, the term "project" refers to any project, technological or not, that may involve the collection, use, disclosure, retention or destruction of personal information.
A project may include, for instance, cloud-hosting of personal information outside Quebec, the purchase of an information system, or a project involving the disclosure of personal information to a researcher.

Target audience

This guide is primarily intended for **privacy officers** in all organizations. It also applies to **members of a committee on access to information and privacy** in the public sector.

In this guide, the term "**organization**" refers to private companies and organizations and public bodies subject to privacy laws.

Secondarily, this guide may also be useful to several other persons, as the case may be, such as the organization's president, directors of legal affairs, risk management, security, ethics or document management, or even researchers.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Does this guide have to be followed?

No. The manner in which a PIA is to be done is not specified in legislation, nor is the content and form of the PIA report. Therefore, this guide does not have to be followed to the letter. However, it contains key information that will help you structure your PIA process and, if applicable, your report.

What is a PIA?

A PIA[1] is a **preventive measure aimed at protecting personal information and the privacy of natural persons (individuals)**. It is a type of impact assessment[2]. It is evolving and needs to be reviewed during the course of the project.

It involves considering, before starting a project and throughout its duration, **all the factors that have a positive or negative effect on the privacy** of the persons concerned. These factors are:

A. Compliance with legislation and principles



Compliance of the project with applicable legislation on the protection of personal information and the observance of the underlying principles

B. Risk assessment



Identification of privacy breach **risks** generated by the project and the assessment of their impact

C. Mitigation strategies



Setting up **strategies** to avoid or effectively reduce these risks and maintain these strategies over time.



Typically, the PIA is documented in a report, which can be updated as it evolves. **The Commission is proposing a generic PIA report template, which you benefit from using in conjunction with this guide**.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[1] The PIA is also known as a *Data Protection Impact Assessment* (DPIA).
[2] Like other similar processes, it provides an opportunity to examine the impact of a project on a particular area of human life. For example, it can be compared, in spirit, to an environmental assessment, algorithmic impact assessment, or human rights impact assessment, all of which involve similar steps.

Why is a PIA needed?

A PIA is a legal requirement in many situations, thus often making it a question of compliance. However, it can be carried out as a best practice.

The PIA is used to protect the persons involved in a project, from the time their personal information is collected until it is destroyed[3] It also results in setting up appropriate strategies to meet your obligations to protect such information. Lastly, it is an important tool to avoid or mitigate the consequences of improperly managing this information (e.g., privacy incidents, lawsuits, damage to image).

In essence, the PIA is thus a valuable tool for reflecting on and demonstrating the necessity and proportionality of your project, based on its objectives and the privacy risks it entails. These two concepts are fundamental to privacy protection and are unavoidable conditions of legality.

If you are unable to justify the necessity and proportionality of your project at the end of the PIA, based on the proposed mitigation strategies, you will have to make more substantive changes to it or make a decision to terminate the project.

When should a PIA be done?

You should initiate a PIA at the beginning of your project:

- To be able to influence how it is conducted along the way
- To act in a timely manner and choose the solution that best protects and respects privacy

Waiting before starting would put you at risk of having to make significant changes late in the process, with the associated costs and delays. However, it is never too late to start the PIA if you realize it is required.

The PIA must evolve throughout the project, according to the changes you make. If a PIA has already been done in the past for the same project, you can update it.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[3] The law now provides for the possibility of anonymizing personal information rather than destroying it, in certain cases.

Overview of PIA process



Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Determine whether an assessment is required	Define your project and the purpose of the assessment	Prepare the assessment	Assess privacy considerations and adopt appropriate strategies	Draft a report	Keep the assessment up-to-date
Pages 10-13	Pages 14-18	Pages 19-30	Pages 31-42	Pages 43-46	Page 47
This step will help you determine whether an assessment is required.	It will allow you to get off to a good start by defining your project and deciding what to include in your assessment.	This step will enable you to make an inventory of personal information, map out its path, and determine the scope of your assessment. You will also need to identify your organization's obligations.	This step will allow you to assess your project's compliance and the associated risks, as well as identify the measures that need to be implemented to eliminate or mitigate those risks.	This step will enable you to document your approach and demonstrate compliance with your obligations.	This step will allow you to review and update your assessment over time.

Step 7 | Specific aspects for certain situations Pages 48-59

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Table of Contents

1. Determine whether an assessment is required 10

1.1 An assessment is mandatory in five main situations 11

1.2 If you have already completed an assessment, update it 13

1.3 If your project does not involve personal information, an assessment is not required 13

2. Define your project and the purpose of the assessment 14

2.1 Define your project and the related objectives 15

Present the project and its context 15

Describe the project objectives 15

Assess the necessity and proportionality of the project from the outset 16

2.2 Determine the scope of the assessment 17

2.3 Define the roles and responsibilities 17

Who is responsible for performing the assessment? 18

Who should be involved in the assessment? 18

3. Prepare the assessment 19

3.1 Make an inventory of the personal information involved 20

Why should you make a personal information inventory? 20

How to structure the inventory 21

How can personal information be grouped? 22

When should the personal information inventory be updated? 22

3.2 Map the path of personal information 23

Identify points of interaction with personal information 23

Chart the path taken by personal information throughout the project 24

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

3.3 Determine the scope of the PIA to be completed 26
Determine the sensitivity of the personal information 27
Assess the reason for the use or disclosure of personal information 27
Assess the quantity of personal information 28
Assess the distribution of personal information 28
Assess the storage media for the personal information 28
3.4 Draw up a list of your obligations 29
Provincial obligations 29
Federal and international obligations 30
Organizational practices 30
Standards 30

4. Assess privacy considerations and adopt appropriate strategies 31

4.1 Comply with the obligations and principles regarding the protection of personal information 32
4.2 Identify the privacy breach risks and assess their impact 32
Identify the privacy breach risks generated by your project 32
Describe the causes and potential consequences of each risk 34
Consider some of the specific aspects of your project 35
Assess the initial level of each identified risk 36
4.3 Implement strategies to prevent or reduce risks 40
Study several strategies and select the best ones 40
Reassess the level of each risk 41
Reassess the necessity and proportionality of your project 41
4.4 Draw up an action plan 42
Prepare your action plan 42
Identify those in charge of managing the residual risks 42
Inform the executives in your organization 42

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

5. Draft a report **43**

5.1 Why draft a report? 44

5.2 What should the report contain? 44

5.3 Does the report have to be released? 46

5.4 Does the report have to be sent to the Commission? 46

6. Keep the assessment up-to-date **47**

7. Specific aspects for certain situations **48**

7.1 Communication outside Quebec 49

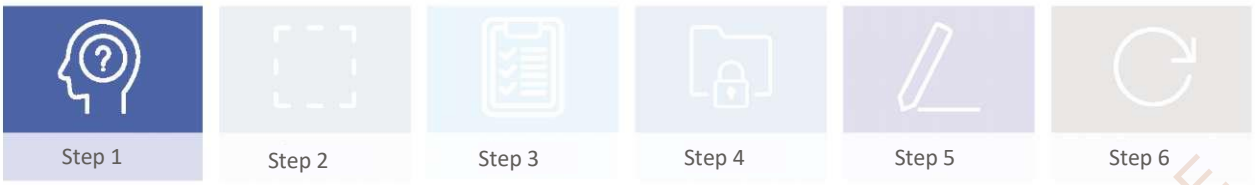
7.2 Information or electronic service delivery system 51

7.3 Disclosure for study, research or statistical production purposes 52

7.4 Collection by a public body on behalf of another 56

7.5 Other types of disclosures without consent (Public sector) 57

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE



1. Determine whether an assessment is required

1.1 An assessment is mandatory in five main situations 11

1.2 If you have already completed an assessment, update it 13

1.3 If your project does not involve personal information, an assessment is not required 13

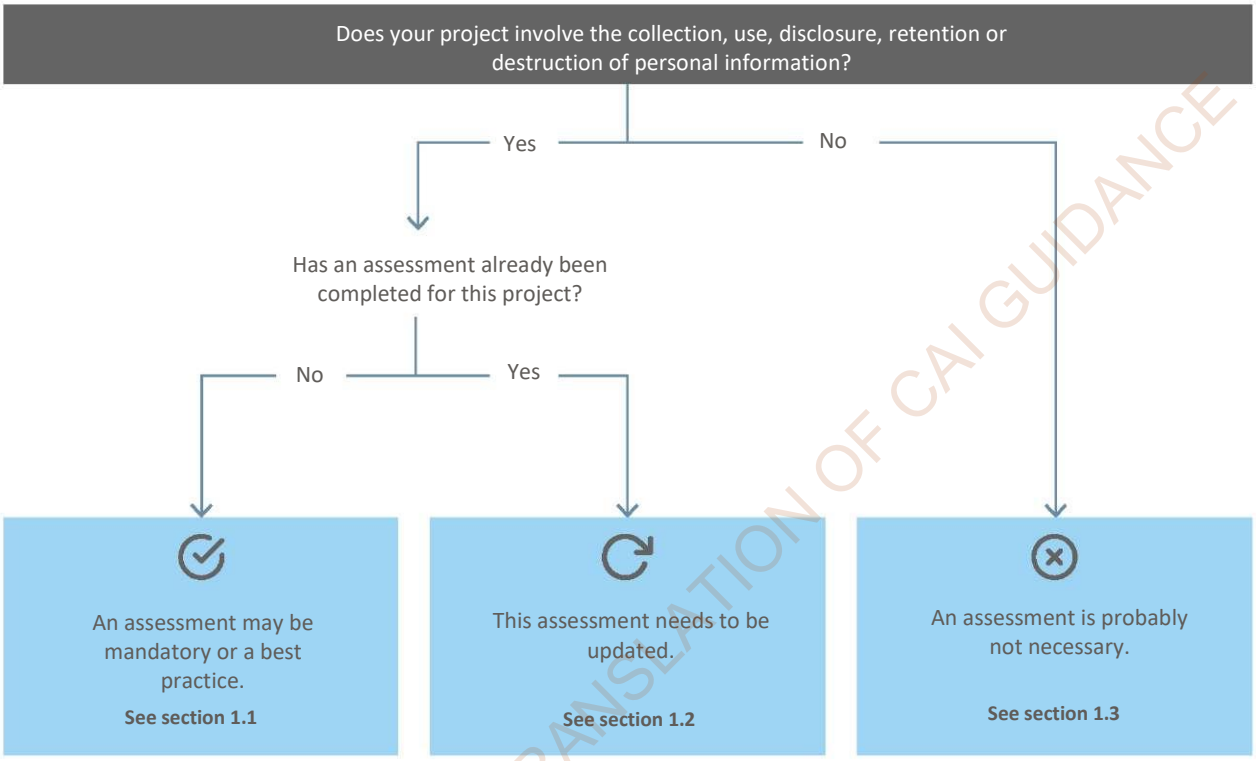
Before initiating a PIA, you must make sure it is required. During this stage, you will determine whether your project is legally required to complete a PIA. If not, you may still choose to conduct a PIA as a best practice.

Include in the summary section of your report:

- The reason you are conducting a PIA, with the legal reference, if required.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

The first step in a PIA process is to determine if it is required.



OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

1.1 An assessment is mandatory in five main situations

This section outlines all cases where the PIA is mandatory by law as of the date of publication of this guide (April 2024).

The steps in the approach proposed in this guide apply to all of these situations. However, your analysis must take into account the specific legal framework of your situation. The details and particulars of each situation can be found in Section 7 of this guide.

The Access Act and the Private Sector Privacy Act require you to conduct a PIA in five situations[4].
You must therefore complete a PIA if:

Situation	Sectors	
	Private	Public
1. You are planning on disclosing personal information outside Quebec See section 7.1 Coming into force: September 22, 2023	Section 17 Private Sector Privacy Act	Section 70.1 Access Act
2. You intend to acquire, develop or redesign an information or electronic service delivery system involving personal information. See section 7.2 Coming into force: September 22, 2023	Section 3.3 Private Sector Act	Article 63.5 Access Act
3. You intend to disclose personal information under an agreement, without the consent of the persons involved, for purposes of study, research or statistical production. See section 7.3 Coming into force: September 22, 2022	Section 21 Private Sector Privacy Act	Section 67.2.1 Access Act
4. You intend to collect personal information on behalf of another public body under an agreement. See section 7.4 Transitional provisions apply for existing agreements. Coming into force: September 22, 2023		Section 64 Access Act
5. You intend to disclose personal information to a person or organization without the consent of the persons involved as part of an agreement. See section 7.5 Transitional provisions apply for existing agreements. Coming into force: September 22, 2023		Section 68 Access Act

- You are starting a new project
- Your project was not finalized when the obligation to complete a PIA came into effect
- If you modify a project (e.g., changes to the agreement, system redesign)
- Your project involves the disclosure of personal information outside Quebec made after September 22, 2023.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[4] This guide only covers situations provided under the Access Act and the Private Sector Privacy Act. The general approach it presents is still applicable in the following cases:
- Project involving information resources of interest to the government (section 9 of the *Act to Facilitate the Public Administration's Digital Transformation*)
- Collection, use or disclosure for the functions of a public body designated as the official source of government digital data (section 12.16 of the *Act Respecting the Governance and Management of the Information Resources of Public Bodies and Government Enterprises*)
- Disclosure by Revenu Québec to a public body designated as the official source of government digital data (section 69.1.1 of the *Tax Administration Act*).



However, you are not required to complete a PIA if your project was already completed by the date the obligation became effective[5]. For example:

- Communication outside Quebec was completed (Situation 1)
- The information system was already implemented (Situation 2)
- The communication agreement was already in place (situations 3, 4 and 5).



We still recommend that you complete a PIA:

- If you are not in one of the five situations where a PIA is mandatory
- If your project was already completed by the date the obligation became effective.

As soon as a project involves personal information, conducting a PIA is a recommended practice to protect that information and the privacy of individuals. It can therefore be useful to review the situation in light of your legal obligations.

1.2 If you have already completed an assessment, update it

If you have already completed a PIA for a previous version of this project and there have been changes, **you must update or redo the PIA to reflect these changes**. Take into account the specific characteristics of your situation based on the details provided in Section 7 of the Guide.

1.3 If your project does not involve personal information, an assessment is not required

If your project does not involve personal information and clearly poses no privacy risk, **you do not need to complete a PIA**. Important note: Some information may, when combined with other data, reveal information on the persons concerned. Don't rule out the PIA too quickly.



If you do not complete a PIA, we recommend that you still prepare a very simple report outlining your thought process, in which you describe:

- Outline of your project
- Reasons why you are not conducting a PIA.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[5] These dates are entered under each situation on the previous page.



2. Define your project and the purpose of the assessment

2.1 Define your project and the related objectives 15
2.2 Determine the scope of the assessment 17
2.3 Define the roles and responsibilities 17

Once you have determined that a PIA is required, you must prepare it. At this stage, you will need to properly document the project as a whole and ask yourself the right questions to properly target the aspects of your project that need to be considered. You will also need to make an initial assessment of the necessity and proportionality of your project.

Based on these elements, you will need to anticipate the involvement of the right persons in the assessment and clarify their responsibilities.

Include in your report:

- A description of your project
- The purpose of your assessment
- A description of the roles and responsibilities

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

2.1 Define your project and the related objectives

First, define your project and the associated objectives.

Present the project and its context

This step is mainly descriptive. The aim is to gather key information to enable you to assess the risks and the ways to eliminate or reduce them (see section 4.2 and section 4.3).

For example:

- What does your project consist of?
- What was the situation when the idea for the project was formed?
- What is or was the situatio n when the project is starting or was started?
- What is the timeline for completing it?
- How does the project benefit your organization?

Describe the project objectives

These objectives are used to explain why you are starting the project and why personal information is involved in the project.

Examples of project objectives:

- Provide a new public service
- Make an existing service available online
- Increase security at a facility
- Combat fraud
- Improve the screening of a rare health condition
- Comply with regulations
- Maintain competitiveness
- Enhance the customer experience by creating a new version of a platform

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Assess the necessity and proportionality of the project from the outset

Necessity and **proportionality**[6] must be assessed throughout the PIA process and implementation of the project. At this stage, you can think about it in a preliminary way by looking at the likely risks associated with your project at a high level and intuitively.

The terms "**necessity**" and "**proportionality**" refer to important legal concepts when a project affects a fundamental right, such as privacy.

A project is considered necessary and proportional if:

- The objectives being pursued are legitimate and address significant and real concerns
- There is a rational link between the project and these objectives, i.e., it is an effective means of achieving them – this effectiveness must be based on concrete and evidence-based data
- The breach of privacy is minimized or there are no other efficient solutions that are less intrusive
- The tangible advantages for the organization outweigh the harm for the persons concerned.

If the necessity and proportionality of your project are uncertain at this stage, the remainder of the PIA will help clarify this. You will reassess them at the end of the process, based on the strategies being considered to mitigate or eliminate privacy risks.

Note that a project that is not necessary and proportional is not legal.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[6] For more information, visit the Web pages on necessity intended for private companies and organizations and government departments and agencies.

2.2 Determine the scope of the assessment

It is in your interest to clearly define what your PIA will pertain to and to keep your analysis at a level appropriate for your project. You should be able to justify what you choose to include in your assessment.

Example 1 – Overly narrow purpose

You have decided not to include a review of the procedures for identifying individuals in your virtual online assistant project. You do not consider this to be important since your current system works well with your in-person and telephone customer service. **The purpose of your assessment may be too narrow**. Your assessment could be missing key elements since online identification may not be the same as identification in person or on the telephone.

Example 2 – Overly broad purpose

For the same project, you ultimately decide to review the identification procedures, the hosting of your customers' data, confidentiality forms of your customer service employees and all your system infrastructure. **The purpose of your assessment is probably too broad**. Separate assessments could no doubt be produced for certain sub-processes.

Example 3 – Analysis level is too high

For the same project, you only review your customer service policies and directives, without focusing on the technical details of the software solution you purchased or the procedures for identifying individuals. **Your analysis may be too high-level**. You will miss key aspects in terms of the software solution or identification procedures.

Example 4 – Alignment with pre-existing PIAs

For the same project, separate PIAs were recently prepared by your organization regarding the procedures and processes for identifying persons who contact customer service. **You decide not to redo that part of the analysis and you only review the part that is added concerning identification by the virtual assistant**. You clearly indicate this in your report so people are aware of the limits you are placing on your assessment.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

2.3 Define the roles and responsibilities

For your approach to be successful, you will generally need to involve others in the assessment. Specify the roles and responsibilities of each person and make sure to determine when they will need to be involved.

Who is responsible for performing the assessment?

The organization holding the personal information is responsible for completing the PIA. This is not the responsibility of potential subcontractors, suppliers or partners (e.g., researchers who request access to information), even though they may help you review and analyze certain aspects.

Within this organization, coordination of the PIA may fall upon the person responsible for the protection of personal information, but may, depending on the project, be assigned to or shared with other staff members.

Who should be involved in the assessment?

Certain individuals must be consulted as part of a PIA:

- The public body must consult, at the start of the project, the members of its **Access to Information and Privacy Committee**, which includes the access and privacy officer.
- On its end, the company must consult its **privacy officer**.

You may involve certain other persons, based on their specific expertise, depending on the scope of the project (see section 2.2) and the assessment of the scope of the PIA to be completed (see section 3.3). For example, you may wish to consult the following individuals in your organization:

- Project leads
- Legal affairs directors
- Document management coordinators
- Human resources directors
- Client relationship managers
- Your organization's executives who must take a position on risk management at the end of the process (see section 4.4).

You may also wish to consult with external stakeholders, depending on the context of your project, such as:

- Representatives of the persons concerned
- Clients or corporate partners
- Subcontractors
- The researcher requesting access to the information.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE



3. Prepare the assessment

3.1 Make an inventory of the personal information involved 20

3.2 Map the path of personal information 23

3.3 Determine the scope of the PIA to be completed 26

3.4 Draw up a list of your obligations 29

Preparing the PIA ensures that you are investing your efforts in the right place and covering the right aspects. Since the assessment concerns personal information, you first need to know what information your project will involve. You will also need to chart the path to understand how the information will be exchanged among systems or players.

This inventory and path will allow you to determine the scope of the PIA to be completed, since it must be proportional to the context: it must be tailored to the sensitivity, quantity, purpose, distribution and medium of the personal information.

Lastly, you will list your legal obligations, which will guide you through the assessment itself.

Include in your report:

- Overview of personal information inventory
- Flow chart of the personal information
- Rationale for the scope of the completed PIA
- Appropriate tables, headings or analysis tools based on the applicable obligations.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

3.1 Make an inventory of the personal information involved

First, identify all the personal information involved in your project based on the scope of your assessment (see section 2.2).

Why should you make a personal information inventory?

Your inventory allows you to collect, use and disclose only the personal information required to complete the project.

Even with the consent of the persons concerned, you cannot collect personal information that is not necessary for your project. You must be able to show that the information collected, used or disclosed is necessary to carry out your project[7].

An inventory of personal information also lets you know its:

- **Sensitivity**
- **Quantity**
- **Purpose**

This information will help you assess the scope of the PIA to be completed (see section 3.3).

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[7] For more information on the necessity criterion, refer to the pages for companies or public bodies and **Section 2.1**.

How to structure the inventory

To structure your inventory, you can answer the following questions:

Questions	Sub-questions
What?	• What types of personal information will be collected, disclosed, used, or retained as part of this project? • What is the nature of the information? Is it **sensitive** due to this nature or the context in which it is being used?
Why?	• Why do you want to collect, use, disclose or retain personal information? • This information will be used for your project for what **purpose** (objective)? • In what way do the individuals who will have access to personal information need it in the performance of their duties?
How much?	• **How much** personal information will be involved in your project? • How many persons will be affected by your project (absolute number or proportion of the population involved)? • What is the volume or extent of the personal information involved? • What is the expected duration of the project? • What is the geographic range of the project?

Remember to include in your inventory **all the information involved**, including:

- Information you will **create** or **deduce** from other information, such as a credit score or interest profile
- Information **collected automatically** by computer devices and systems, such as a device identifier or connection history
- Information that is **grouped** (also called aggregated information), even if it no longer identifies a specific individual, such as statistics[8]
- Information that no longer directly or indirectly identifies an individual (i.e., **de-identified** information and **anonymized** information).[10]

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[8] You will need to assess the risk of the re-identification of aggregated, de-identified or anonymized information, i.e., the risk that the link between a piece of information and the individual will be restored. This is often made possible through new technology. For more information, visit the Web pages on anonymization and de-identification intended for private companies and organizations and government departments and agencies.

How can personal information be grouped?

You will not always have to prepare a complete list of all personal information at all stages of the PIA. For example, a list of groupings of personal information may be sufficient in your PIA report. However, even if you are presenting groupings, you must be able to know the scope of the personal information involved in the project.

You can group personal information in different ways. For example, you could group information:

- With shared characteristics
- That enables the same function or goal to be achieved.

If you are unsure whether a group contains personal information, keep it and consider it for your PIA.

Note that a list of groups must still provide a short description of the content of the groupings. In the examples below, this listing is in brackets.

Examples of groupings:

- Identification and contact information (e.g., last name, first name, address, user ID, password)
- Medical information in electronic form or on paper (e.g., test results, consultation summaries, health data, medical imaging)
- Employee disability files held by Human Resources (e.g., identity information, medical reports, communication with insurers)
- E-mails and telephone recordings from the call centre (e.g., discussions with customers, content of questions and answers, voice sample)
- Website usage data and web analysis tools (e.g., history of pages viewed, IP address, browser and device used, display settings)

When should the personal information inventory be updated?

The inventory of personal information is evolving. Keep it up-to-date to report any changes that may occur within your organization (e.g., new collection of personal information for a project). This will allow you to properly plan your actions and meet all your obligations.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

3.2 Map the path of personal information

Once you know the information involved in your project, you need to specify its path.

The term "**path**" refers to a structured representation or description of the stages involved in the processing of information from collection to destruction, that identifies the organizations, individuals, systems and media involved. Terms that are sometimes used include "data mapping" or "data flow chart."

The path of personal information namely allows you to identify:

- The **distribution**
- The **medium**.

This information will help you assess the scope of the PIA to be completed (see section 3.3).

Identify points of interaction with personal information

First, based on your inventory (see section 3.1), identify the **points where your organization (or another organization/individual) interacts** with personal information. The interaction points may include:

- **Persons**, groups of persons or partners and third parties with access to the personal information, in charge of collecting it, approving its destruction, etc. (e.g., employees, customers, subcontractors, consulting firms, external researchers, building or computer system maintenance teams, telecommunication providers)
- **Means** used to **collect** personal information (e.g., subscription forms, e-mail folders, telephone messages, social network platforms, surveys, questionnaires)
- **Means** used to **disclose** personal information (e.g., electronic service delivery, e-mails, customer service, websites, application programming interfaces [API] or secure electronic links)
- **Means** used to **process** and **store** personal information (e.g., computer systems, databases, cloud services, backup copies, telecommunication tools, storage rooms and filing cabinets for paper files)
- Means used to **destroy** or **anonymize** personal information.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

To help you, you can answer the following questions:

Questions	Sub-questions
Who?	• What categories of individuals will have access to the personal information within or outside the organization (third party)?
How?	• How or by what means will the personal information be collected, used, disclosed and retained within (or outside) the organization? • How will the organization dispose of the information once the objective for which it was collected (or disclosed or used) is met? • What method of destruction (or anonymization) will be used?
Where?	• Where will this information be **distributed** and stored within (or outside) the organization? • On what type(s) of **media** and under what conditions will it be kept?
When?	• When will the information be destroyed or anonymized?

Chart the path taken by personal information throughout the project

Starting from the interaction points you have identified, show the path taken by personal information during the process covered by your project.

This path can take many forms, such as a table, a schematic process or a descriptive text. Here is an example of a table to depict a path in a simple project:

Information or grouping of information	Collection (e.g., managers, source, time, place, means)	Use (managers, time, place, means, purpose)	Communication (e.g., managers, recipients, situations, means, reasons)	Retention (managers, means, duration, location)	Destruction (managers, time, place, means, trigger)
Grouping 1					
Grouping 2					
...					

You may also wish to create a table to list the individuals and organizations that will have access to the information during its life cycle, while indicating the type of access and the reasons for the access[9].

[9] An example of such a table can be found in section 3 of the generic report template proposed by the Commission.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

The path will be more complex for larger projects, so a breakdown by process may be preferable in such cases.

For instance, the **development phase** of your project may involve privacy risks that are different from those found in the **operating phase**:

- **Development** phase. Your project takes shape, you develop solutions to emerging problems; people intervene on an ad hoc basis during this phase (such as consultants); you test various products; the project can be modified along the way.
- **Operation** phase. Your project is under way, you make sure that it produces the expected results; specific events may occur during this phase, such as system updates; employees may leave your company; people may request access to information.

If your project includes such phases and they differ significantly in terms of personal information management, you should represent the path of the information separately for each phase.

Example 1: You run a company that manufactures custom-made clothing. You would like to offer your customers an online purchasing tool. You will hire a specialized firm during the **development phase**. You must anticipate that the consultants will come in contact with certain information concerning your salespeople and customers while the system is being set up. However, they will no longer have access to the information once the system is operational, during the **operating phase**. You must also take into account that the risk of computer bugs will be higher during this time.

Example 2: You head the human resources department of a large government organization. You are planning on changing the human resources management software. The software vendor has told you that the system is frequently updated and that more significant redesigns are to be expected within the next year. You must anticipate that these redesigns will happen during the **operating phase**. You must set up mechanisms to prevent these maintenance operations from impacting employees' personal information.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

3.3 Determine the scope of the PIA to be completed

If there is a situation that legally requires you to complete the PIA (see section 1), **you must do so without fail**. However, the scope of the PIA must be in line with the size of the project, its objectives, the type of personal information involved, and how the information is used and disclosed. Hence, there may be variations in:

- Number of players to involve (see section 2.3)
- Time to be invested
- Level of detail of a potential report (see section 5)
- Associated documentation to be developed
- Number of planned strategies to mitigate or eliminate the risks (see section 4.3);
- Level of detail of the strategies

For example, the Access Act and the Private Sector Privacy Act require that the PIA be proportionate[10] to:

1. **Sensitivity** of the information concerned
2. **Purpose** of its use
3. **Quantity**
4. **Distribution**
5. **Medium**

It is up to you to determine the scope of your PIA. It is important to document the reasons for your decision in this regard.

While not exhaustive, this section provides relevant insights to help you determine the scope of your PIA. The inventory (see section 3.1) and personal information path (see section 3.2) that you have drawn up should greatly assist in you in this thought process.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[10] Access Act, section 63.5; Private Sector Privacy Act, section 3.3.

Determine the sensitivity of the personal information

How **sensitive** is the personal information involved?

Personal information is sensitive when it raises a high level of a reasonable expectation of privacy due to its nature or context of use or disclosure[11].

Examples of sensitive information:

- Information about a person's ethnic background
- Information about a person's philosophical or religious beliefs
- Information about a person's health or sexual orientation
- Biometric information
- Certain unique identifiers.

Information may also be considered sensitive if it is used in a project that specifically affects a vulnerable population (e.g., minors, ethnocultural minorities, sexual minorities).

Assess the reason for the use or disclosure of personal information

For **what purpose(s)** will the personal information be used or disclosed? Are these purposes generally risky for individuals? Do they have a significant impact (e.g., legal) on the individuals?

Examples of purposes:

- Verifying the identity of clients when they wish to access their file and perform transactions
- Calculating employees' pay and paying them
- Profile an individual (e.g., consumer, driver) in combination with other information
- Make an automated decision in relation to an individual
- Conduct a study or research or produce statistics
- Improve an artificial intelligence model.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[11] Access Act, section 65.1; Private Sector Privacy Act, section 12.

Assess the quantity of personal information

How much personal information will your project involve? Does the quantity influence the magnitude of the foreseeable risks?

Examples of questions to ask:

- How many persons are affected by your project (absolute number or proportion of the population involved)?
- What is the volume or extent of the personal information involved (all categories: collected, observed, inferred, created)?
- What is the expected duration of the project? Is the project permanent or temporary?
- What is the projected geographical coverage?

Assess the distribution of personal information

How will the personal information **involved** in your project be distributed? Consider the following aspects:

- **Spatial**. For example, where will the personal information be located (within or outside the organization [centralized, decentralized retention])? In which country will the personal information involved in your project be held?
- **Human or administrative**. For example, to whom will the personal information involved in the project be disclosed (e.g., service provider)?
- **Quantitative**. For example, how many people will have access to the information? How many media will the information be stored on?

Assess the storage media for the personal information

What type(s) of **media** will be used to view, record or access, temporarily or in the long term, the personal information involved in your project?

Examples of media characteristics:

- Physical (tangible) or digital (e.g. cloud hosting)
- Secure or non-secure
- Connected to other systems or not

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

3.4 Draw up a list of your obligations

In order to assess the first privacy factor, you would benefit from first drawing up a list of your obligations with respect to the protection of personal information. Depending on the nature and size of your project, these obligations may come from different sources.

Identifying your obligations and understanding the issues involved can be a complex process, especially if your project is also complex. **When in doubt, we recommend that you consult a lawyer**.

Provincial obligations

In Quebec, the protection of personal information is primarily regulated by the Access Act and the Private Sector Privacy Act. General information on the obligations under these statutes can be found on the Commission's website, in the relevant sections:

- Government departments and agencies
- Private companies and organizations

These sections are structured around the life cycle of personal information, from its collection to destruction, and outline the cross-cutting obligations relating to responsibility, consent and security.

The term "**life cycle**" refers to all the phases through which personal information passes through an organization[12]. These phases consist of collection, use, disclosure, retention and destruction. Each phase entails specific obligations for the organization.

You may also be required to enforce obligations under other statutes or regulations. To assist you, please consult those listed on the Commission's website.

Examples of special provisions and exceptions set out in statutes:

- The collection and use of a driver's licence and health insurance number are governed by laws, regulations or sector-based directives.
- The use and collection of biometric information[13] is regulated specifically and in a complementary manner by the *Act to Establish a Legal Framework for Information Technology*.

[12] For more information, visit the Web pages on life cycle intended for private companies and organizations and government departments and agencies.
[13] For more information, see the Biométrie section of the Commission's website [in French only]..

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Lastly, depending on the reason for completing a PIA (see section 1.1), you may need to ensure that your assessment enables you to meet specific criteria or provide for a formal agreement. Be sure to include these obligations in your list.

For more information on the specifics of each of the five situations that require the completion of a PIA in the Access Act and Private Sector Privacy Act, see Section 7.

Federal and international obligations

The federal government and certain Canadian provinces have their own laws and regulations on the protection of personal information. If your company operates in one or more other provinces, make sure you are fully aware of your obligations under the respective provincial laws.

Remember that the disclosure of personal information outside Quebec and Canada is subject to special rules under provincial and federal laws.

For international activities, be aware that the laws may differ greatly from one country to another. Also, additional obligations may apply to certain categories of personal information, including sensitive information.

Lastly, some legislation applies if an organization collects, uses, discloses or keeps the personal information of persons in the jurisdiction covered by the legislation, even if the organization is not in that jurisdiction. The European Union's *General Data Protection Regulation* is one such example. Failure to comply with such legislation can lead to heavy financial penalties.

If your services are intended for a foreign market or citizens in another country, make inquiries and consider the effects that such laws could have on your project.

Organizational practices

Your organization can guide the management of personal information in various ways, including policies, processes, procedures, work methods, a retention plan and schedule, etc.

Although such internal documents do not have legal force, it is important to take account of them in your assessment so you do not stray from your organization's current practices. Your effort could even help you identify shortcomings within your organization.

Standards

Different international standards could guide your reflection about your practices, such as certain ISO standards or the documentation produced by the European Union or the Organisation for Economic Co-operation and Development (OECD). Refer to them if you want to adopt best practices relating to safeguarding privacy and personal information.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE



4. Assess privacy considerations and adopt appropriate strategies

4.1 Comply with the obligations and principles regarding the protection of personal information 32

4.2 Identify the privacy breach risks and assess their impact 32

4.3 Implement strategies to prevent or reduce risks 40

4.4 Draw up an action plan 42

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

You have now described your project and the purpose of the assessment, identified the individuals and organizations you need to consult, drawn up an inventory of the personal information involved, mapped out its path, established the scope of your PIA, and identified your obligations. You are finally ready to perform an in-depth analysis of the privacy factors, i.e., all those that will have a positive or negative impact on the privacy of the individuals concerned.

During this stage, you will assess whether everything is in place in your project to comply with applicable privacy laws and principles. You will also reflect on the risks that may arise for the persons concerned as a result of your project and identify strategies (e.g., legal, technical, administrative) to mitigate or eliminate such risks.

Taking into account the strategies already in place and those that are planned, you will then reassess the residual risks and, consequently, observance of the notions of necessity and proportionality in order to make a decision on the project's future. If you are able to continue with the project, you will finally establish an action plan to implement the strategies identified in the assessment.

Include in your report:

- A description of the means set up to comply with the obligations and principles regarding the protection of personal information
- A demonstration that the specific criteria to be addressed in the PIA are met, if applicable;
- A risk assessment (events, causes and consequences, risk level)
- A description of the strategies required to eliminate or mitigate the risks
- An action plan to implement these strategies.

4.1 Comply with the obligations and principles regarding the protection of personal information

To assess the first privacy factor, you must ensure that your project complies with applicable privacy legislation and the principles supporting it.

Go down your list (see section 3.4) and assess how well you are meeting your obligations. This may involve legal analyses, documenting certain practices within the organization, etc.

Ask yourself the following questions:

- Do you comply with the obligations and principles[14] for the protection of personal information for each category of personal information, at each interaction point throughout the life cycle of the information?
- Can you show that you meet the specific criteria associated with the legal situation that is leading you to conduct a PIA, if applicable (see section 7)?
- If not, what changes should you make to your project in order to meet your obligations and the principles?

Document the means that will be put in place to meet your obligations and these various principles.

When in doubt about compliance with your legal obligations, do not hesitate to consult a lawyer.

4.2 Identify the privacy breach risks and assess their impact

To assess the second privacy factor, you must identify the privacy risks associated with the project and assess their impact on the individuals involved.

Identify the privacy breach risks generated by your project

As soon a project involves personal information, it necessarily poses a risk of a breach of the privacy of the persons concerned.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[14] For an overview of the generally accepted privacy principles, see **section 7.1**.

The term "**privacy risk**" refers to a situation or event that could cause harm to a person in terms of privacy or in relation to another right, but in connection to the person's privacy. Risk is a *potential threat* to the right to privacy which may materialize in the future.

Risks may result, for instance, from non-compliance with the law, but also from an external action (e.g., cyber attack). They may also occur if a person's reasonable expectation of privacy is not observed. **Note that certain legally compliant aspects of a project may still be perceived as a breach of privacy by the persons concerned.**

To draw up risk scenarios for your project, ask yourself the following questions:

- What **situations** or **events** could reasonably occur for each type of personal information, at each interaction point, throughout the life cycle of the information?
- What situations or events could generate a loss or harm for the persons concerned with respect to their privacy?

Draw up a list of your answers to these questions and briefly describe these situations.

Examples of privacy risks:

- Excessive collection of information
- Excessive or unjustified creation of information
- Lack of information provided to individuals when information is collected
- Unauthorized disclosure of personal information
- Decision based on inaccurate or ambiguous personal information
- Theft of personal information
- Invasion of privacy that is disproportionate in relation to the objective of the project
- Retention of information when it is no longer useful
- Re-identification of previously anonymized information

Your organization may already have legal opinions or the results of computer security analyses. If any non-compliance or information security risks were discussed in those documents, **we recommend that you draw on them to prepare your PIA**.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Describe the causes and potential consequences of each risk

Identify the possible causes of the risks you have identified, within the context of your organization. Note that the same risk can be caused by multiple factors.

Examples of causes:

- Deficient process
- Error in handling information
- Lack of knowledge or training
- Inadequate or non-existent oversight mechanisms
- Inadequate distribution of responsibilities
- Malicious behaviour
- Excessive collection of information
- Defective or obsolete technology
- Unjustified or unnecessary use of sensitive information
- Lack of consent
- Inadequate mechanisms to ensure personal information is accurate
- Less intrusive and sufficiently efficient alternative means of reaching the objective in question

Each risk, if realized, may have consequences for the individuals involved. Describe and assess potential harm to the individuals' rights.

A consequence does not have to be tangible in order to be considered: it can be obvious and external (e.g., in the event of damage to the reputation of the persons concerned), or it can be experienced from within by the persons concerned (e.g., a sense of intrusion). Similarly, it can be linked to an invasion of privacy, but it can also affect other rights of individuals, such as the right to independence or freedom of expression.

Important note: Depending on the scope of your PIA, you should also consider the relatively small consequences, especially when they are likely to be experienced by large numbers of people. Indeed, individual harm on a small scale can become very significant when its effect on a group of people is taken into account.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Examples of consequences:

- Identity theft and fraud
- Danger to a person's life and safety (such as the possibility of harassment)
- Interference with autonomy (e.g., manipulation)
- Financial loss or lost opportunities
- Discrimination
- Reputational damage
- Psychological distress
- Self-censorship due to a deterrent effect
- Unwanted solicitation
- Intrusions and other nuisances in a person's personal life

The consequences for your own organization should not be considered in the PIA, which is intended to protect the rights of the **persons concerned**. Although these consequences are significant, do not consider the following in the PIA:

- Any potential damage to your organization's reputation
- Legal disputes that may arise
- Potential costs you may incur, etc.

Consider some of the specific aspects of your project

In identifying the risks, their causes and their potential consequences, take into account the context of your project, particularly if it involves new technology, is large in scale, or involves ethical issues.

Projects involving new technology

Some technology creates special issues, and emerging technology can also bring up new issues.

To adequately assess the risks involved with technology, it must be properly understood before being released, especially if it has never been used before.

The use of biometric data is an example of technology that raises specific questions and issues[15]. There is also artificial intelligence, particularly generative AI[16].

Ask for the help of a specialist if you cannot conduct an adequate assessment yourself.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[15] For more information on the use of biometric systems, refer to the guide produced by the Commission.
[16] For more information on the use of generative AI, refer to the https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/ document of principles drawn up by the Commission and its Canadian counterparts.

Large-scale projects

Larger projects often involve more risk, which can affect more people.

For projects involving several phases, it may be useful or necessary to produce a PIA for each phase (see section 3.2). The environment and risks of each phase will be different.

The PIA should be regularly updated for long-term projects.

Projects involving ethical issues

Certain types of projects require that an ethics committee conduct an assessment. This is the case in particular with scientific research involving humans. These committees sometimes make privacy-related recommendations. These recommendations should normally be considered in your assessments (see section 7.3).

Ethical assessment reports for new technology are frequently issued by independent organizations, such as the Commission de l'éthique en science et en technologie, or university researchers. These documents often address privacy issues. They are relevant sources of information that can help you assess the issues and risks presented by technological projects.

Assess the initial level of each identified risk

To obtain an initial view of the magnitude of the risks associated with your project, assess their level. This will guide you in choosing mitigation strategies and provide you with a useful point of comparison when assessing their potential effectiveness.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Set up a method to qualify the risks

The law does not prescribe a method for qualifying or assessing risks or for presenting the results of your analysis. Nonetheless, an assessment based on the potential severity of the impact of an event and the likelihood that it will occur may meet the objectives of the PIA. For example, you can use a rating system and a risk level grid, as shown in the following graph:



Assessing the level of risk is a subjective process. It is often useful to set up a committee for this purpose.

If privacy risk management practices are already in place in your organization, **we recommend that they be favoured**. You can then use a methodology that is proven in your context.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Assess the severity of the potential impact of each of the identified risks

The first component of the risk level is the severity of the consequences that could affect the persons concerned if it were to occur. The level of severity may can be assessed using a rating system.

Example of a rating system to assess the **severity of a risk**:

- **Very low and/or non-existent (1)**: the risk has no impact on individuals, or only very minor impacts for a single individual.
- **Low (2)**: the risk generates minor impacts for one individual or a small number of individuals.
- **High (3)**: the risk generates a significant impact for one individual or minor impacts for a large number of individuals.
- **Very high (4)**: the risk generates a major impact for one individual or significant impacts for a large number of individuals.
- **Unacceptable (not rated)**: the risk would generate an overly significant impact and/or is not compliant with the law. If you identify a risk with such a level of severity, you must eliminate it in order to continue your project.

Some variables, including those you considered when determining the scope of the PIA (see section 3.3), could influence the severity of the potential consequences. Consider, for example:

- **Quantity** of information involved
- **Nature** and **sensitivity** of the information involved
- **Type of harm** that may be caused (**examples**: major consequences for the personal or professional life of the individuals concerned, impact on their finances, legal proceedings or action they need to take to resolve the situation, danger to their life or safety)
- **Number of persons** potentially affected or their **profile** (**examples**: children, persons living with a disability, immigrants).

Estimate the likelihood of the risks occurring

The second component of the risk level is the likelihood that the situation or event that constitutes the risk will occur. Likelihood may also be assessed using a rating system.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Example of a rating system to assess **likelihood**:

- **Very low and/or non-existent (1)**: the risk has no chance of occurring
- **Low (2)**: little likelihood of the risk materializing or a similar event has never occurred
- **High (3)**: high likelihood of the risk materializing or a similar event has occurred one or more times in the past
- **Very high (4)**: very high likelihood of the risk materializing or a similar event has occurred numerous times in the past

Since there is no such thing as zero risk, estimating the likelihood of risk can be difficult.
We recommend that you be realistic: avoid being overly confident or too conservative.

Estimate the level of risk

Once risk severity and likelihood have been estimated, you should assign an overall risk level. If you use a rating system, one simple way to do this is to multiply the severity rating by the probability rating, as illustrated in the risk level grid on page 37.

Consider existing strategies and means of control

Your organization may have already set up measures such as tools, policies, guidelines, procedures, technical means, etc., to mitigate or eliminate the risk without additional measures being adopted.

List them and re-assess the risks in view of that information.

Determine the acceptable tolerance level for each risk

Put yourself in the shoes of the persons concerned and ask yourself how they might expect their personal information to be used and protected when it is:

- Collected
- Used
- Disclosed
- Retained
- Destroyed.

Set thresholds to be reached according to what might seem acceptable for those persons.

You must establish these thresholds while considering the context of your project. For example, a person who provides medical information has different expectations of a hospital centre than of an advertiser.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

4.3 Implement strategies to prevent or reduce risks

To assess the third privacy factor, you will need to select strategies to effectively avoid or reduce the risks that your project presents for the persons involved.

Study several strategies and select the best ones

The strategies may aim at reducing either the severity of the potential consequences associated with the risk or the likelihood of a risk materializing, or both at once.

Reducing the amount of personal information you collect reduces the potential consequences of data theft. While adding safety measures will reduce the likelihood of such a theft.

Your strategies can be legal or administrative, physical or technical.

Examples of strategies:

- Plan a periodic review of the collection of personal information.
- Set up a document management system that provides for an automated retention schedule.
- Review the computer access allocation and management processes.
- Periodically review electronic service delivery security parameters.
- Review confidentiality contract clauses.
- Set a schedule for employee training and awareness activities.
- Restrict access to areas where documents containing personal information will be kept.
- Conduct an information campaign on your new use of personal information.
- Keep track of access and use logs to detect any anomalies.
- De-identify or aggregate the information if its use in a directly identifiable nominative form is not required for everyone.

From the range of strategies you will have considered, determine which ones you will implement to eliminate or reduce a risk. Think of feasible solutions for your organization.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Reassess the level of each risk

Based on the selected strategies and means, reassess the risk level by once again analyzing the severity of the potential consequences and the likelihood of the risk materializing. You can once again follow the process outlined in section 4.2.

Check whether you have reached the tolerance threshold you set. If the threshold has once again been exceeded, reassess your choice of strategies or means.

If, after reviewing your choice, you are still not able to eliminate a significant risk or reach the tolerance threshold you set for yourself, **consider conducting an in-depth review of this aspect of your project or removing it**.

Any risk that remains at the end of the process, once you have identified measures to reduce or eliminate the risks determined at the outset, becomes a **residual risk**. It is therefore possible, and even likely, that some privacy breach risks may remain even after most of them have been eliminated or reduced. If you accept the risks because of their low probability or low impact, your organization must still be able to take responsibility for them.



Even if a risk has been completely eliminated or a strategy is not retained, **we recommend that you keep a record of your process**. Your organization will be able to refer to it in the future. That way it will know why you made certain choices and can avoid having to needlessly repeat the process again.

Reassess the necessity and proportionality of your project

After completing the risk management exercise, redo it to assess the necessity and proportionality of your project in relation to the risks that it still creates for the persons concerned (see section 2.1).

Based on the entire PIA, **does the solution you are proposing to achieve your objectives still seem proportionate given the residual risks? Is all the personal information involved necessary?**

In case of a complaint by a person concerned or an audit by a regulatory body, **will you be prepared to answer questions about whether your solution is proportionate?**

If the residual risks are too significant, you should consider making substantial changes to your project. This may involve redoing the PIA in whole or in part, or even reconsidering the project.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

4.4 Draw up an action plan

Once the privacy factors have been assessed, you should prepare the concrete continuation of the PIA and of the project by planning to implement your chosen strategies.

Prepare your action plan

Preparing an action plan allows you to ensure that the strategies and means chosen are implemented. Incorporating the various actions into your regular activities will make the PIA concrete and allow you to benefit from it.

Your action plan should include ways to periodically re-assess the effectiveness of the strategies you will be implementing.

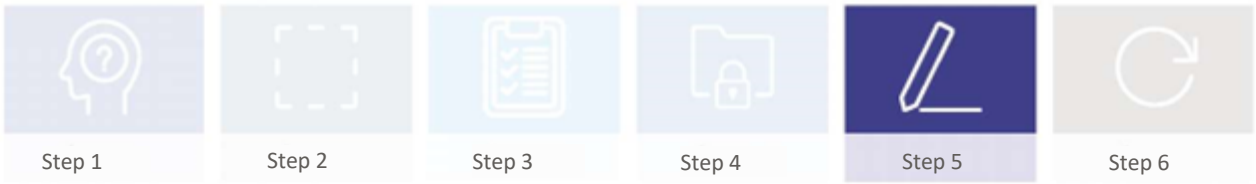
Identify those in charge of managing the residual risks

You should designate persons to monitor the evolution of the residual risks, otherwise they may be forgotten. These persons may also be responsible for managing the situation if it were to occur.

Inform the executives in your organization

Your organization's executives have a specific responsibility to observe privacy laws. You should therefore keep them informed of the PIA results. They must accept the conclusions of your analysis and endorse the risks that remain despite the means used to mitigate them.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE



5. Draft a report

5.1 Why draft a report? 44
5.2 What should the report contain? 44
5.3 Does the report have to be released? 46
5.4 Does the report have to be sent to the Commission? 46

You should be able to explain and justify your PIA approach, if required. Writing a report, even when not mandatory, is an excellent way to report on your thought process once it has been completed or when an important milestone has been reached. If you are writing a report, you should update it as your PIA evolves.

This report should be simple and easy to read: readers should be able to understand what the project is, how it is likely to affect privacy and how you have considered, measured and mitigated the risks identified.

The Commission has a generic PIA report template, which you can customize to fit your needs. However, it can take any other form that enables proper accountability.

Draft your report to document your approach.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

5.1 Why draft a report?

A PIA report is used **to document and consolidate** the results of your assessment. It lays out the actions you have taken and your thought process in the case of an audit, inspection, or investigation by a regulatory body, including the Commission. It is also a useful record for organizational memory. If you need to update the PIA or create a similar one, the report will then be a valuable source of information.

The report is the most common and comprehensive option for documenting your approach. It may be longer or shorter, depending on the magnitude of your PIA (see section 3.3). However, it is not mandatory, nor is it the only method available to you. For smaller projects, you may be able to report on the PIA in a variety of ways, such as through debriefings or emails reflecting your thought process.

Note, however, that increasing the number of supporting documents could be detrimental. It may be more difficult to monitor your assessment, changes in risk, and the implementation of the strategies you have established without a document that includes all the relevant information. Similarly, if the Commission has to verify your PIA, the many documents can complicate the process, which will be a disadvantage for you.

In most cases, you will benefit by opting for a report, especially if you need to attest to your PIA with the Commission, such as to support a disclosure agreement.

5.2 What should the report contain?

Your report should first present the essence of your project, the framework within which it is based, and your analysis. It should also include a note that your report was approved by your organization's executives.

Finally, your report should include additional information in the form of appendices, if applicable:

- A list of your relevant policies on the management of personal information and privacy protection
- A summary of the security opinions prepared in conjunction with suppliers or partners (such as a penetration test)
- A communication agreement entered into after the PIA
- Certifications obtained in connection with your project (when an assessment body certifies that your product or service complies with certain requirements); etc.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

The following table provides an overview of the elements that may be included in your report, with appropriate references to the sections of this guide and the generic report template proposed by the Commission.

Element	Section of the guide	Section of the generic report template
Legal situation underpinning the PIA, if applicable	Section 1.1	Assessment summary
Description of the project, what led to it (context) and the objectives	Section 2.1 Section 2.2	Section 1. Description of project and purpose of PIA
PIA stakeholders, including a description of their role and responsibilities	Section 2.3	Assessment summary Section 2. Roles and responsibilities
Summary of PIA consultations, if applicable	Section 2.3	Section 2. Roles and responsibilities
Overview of the inventory of personal information involved (e.g., categories, end uses, quantity)	Section 3.1	Section 3. Personal information involved and extent of the assessment
Overview of the path of the personal information involved (e.g., sources, media, recipients, systems used, persons with access to it)	Section 3.2	
Assessment of sensitivity, purpose, quantity, distribution and support criteria for the personal information and an explanation of the PIA scope	Section 3.3	
Description of the means set up to meet sector-based, situational, or other privacy obligations and principles	Section 3.4 Section 4.1	Section 4. Compliance with the obligations and principles regarding the protection of personal information
Rationale for meeting the specific criteria associated with the legal situation underpinning the creation of the PIA, if applicable	Section 7	
List and categories of the risks identified for the persons concerned	Section 4.2	Section 5. Identification of risks and strategies to mitigate them
Strategies, mechanisms and measures used to eliminate or reduce such risks	Section 4.3	
Individuals responsible for implementing these strategies and individuals or sectors responsible for managing residual risks	Section 4.4	Section 6. Plan of action
Action plan with a timetable, including a periodic reassessment of the measures implemented	Section 4.4	
Approval of the report by the organization's senior executives (including names, titles, signatures, date, etc.)	Section 4.4	Section 7. Approval of report and versions
Any relevant attachments	N/A	Enclosed documents

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

5.3 Does the report have to be released?

As a best practice in relation to transparency, your organization may decide to release an abridged version of the PIA report on its website or by any other means. This demonstrates your compliance with the law and respect for the information of the persons involved.

Public bodies, in particular, may consider proactively disclosing summaries of PIAs relating to projects directly affecting the public.

5.4 Does the report have to be sent to the Commission?

You are expected to provide a PIA report to the Commission when an agreement is first signed (see section 7.3, section 7.4, section 7.5). A written document confirming the PIA process allows your organization to prove that it has met its obligation. The document outlines how each criterion was analyzed and what elements were considered.

In other cases, there is no need to proactively provide a PIA report to the Commission. However, the Commission may request access to it as part of its oversight activities.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE



6. Keep the assessment up-to-date

Privacy protection is a long-term affair and a PIA is only effective if it continues to evolve. It may need to be reviewed throughout the life of the project.

To ensure that your strategies are effective, you must track how they are enforced and revise them based on emerging risks or changes made to your project, such as the development of a new business line, plans to set up a service ancillary to the transaction system, and so on.

Active control mechanisms, such as a security dashboard, will enable you to ensure that the strategies and measures you set up are consistently applied in an integrated manner.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE



7. Specific aspects for certain situations

7.1 Communication outside Quebec 49
7.2 Information or electronic service delivery system 51
7.3 Disclosure for study, research or statistical production purposes 52
7.4 Collection by a public body on behalf of another 56
7.5 Other types of disclosures without consent (Public sector) 57

The general approach for a PIA is always the same. However, you will need to take certain specific aspects into account depending on the legal situation that justifies your assessment.

This section contains details on certain concepts found in the legislation, on entering into agreements and on assessing specific criteria under certain circumstances.

Include in your report:

- **A demonstration that the specific criteria to be addressed in the PIA are met, if applicable.**

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

7.1 Communication outside Quebec

These clarifications relate to the situation set out in section 70.1 of the Access Act and section 17 of the Private Sector Privacy Act.

A PIA is required:

- Prior to **disclosing** personal information **outside Quebec**.
- Prior to **assigning a person or organization outside Quebec** to collect, use, disclose or retain such information on your behalf.

For the purposes of your assessment, in this situation, the following should be considered:

- The sensitivity of the information being disclosed
- What the information is to be used for
- Measures to safeguard the information, including those that are contractual
- The legal system applicable in the country in which the information would be disclosed, including the privacy principles applicable therein

You may disclose the information if the PIA shows that the information would be **adequately protected** with regard to **generally accepted privacy principles**.

What is meant by "generally accepted privacy principles"?

The notion of "generally accepted privacy principles" is not defined in the Access Act or the Privacy Act.

However, one may say that these are general rules that ensure the protection of personal information and respect for the rights and interests of the individuals concerned in this respect.

Although not exhaustive or definitive, the following list presents principles found in a number of privacy laws and other important privacy documents, such as standards and guidelines[17]:

- **Accountability**. Organizations are accountable for their management of personal information. They put policies and practices in place to protect personal information and use the financial and human resources necessary to do so, including by appointing a privacy officer. They document their compliance and privacy-related decisions.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[17] See, for instance, the OECD Privacy Guidelines, the US Federal Trade Commission's Fair Information Practice Principles (FIPPs), and the principles underlying legislation such as the Canadian *Personal Information Protection and Electronic Documents Act* and the EU's *General Data Protection Regulation*.

- **Determination of purpose**. The reasons why organizations are collecting the personal information are legitimate and established prior to the collection.
- **Limitations on collection**. Organizations collect only information necessary for the identified purpose. Collection is done by lawful and fair means. It minimizes the invasion of privacy.
- **Consent**. Individuals are adequately informed of and freely consent to the identified purposes, unless there are exceptions.
- **Data protection by design and by default**. Products/services are designed in keeping with individuals' privacy. If they include confidentiality terms, these protect privacy by default.
- **Limitations on use, disclosure and retention**. Organizations use and disclose personal information collected for a specified purpose or for a consistent purpose, unless there is consent or a legal exception. They limit access to such personal information to authorized persons only and do not keep it longer than necessary.
- **Accuracy**. Organizations keep personal information up to date and ensure it is accurate and complete when used or disclosed.
- **Safeguards**. Organizations take appropriate security safeguards to protect the information they hold at all times from loss, theft or unauthorized modification, disclosure or destruction. These safeguards are appropriate to the sensitivity of the information and the context. In the event of an incident, organizations respond promptly and notify the individuals concerned and authorities, with some exceptions.
- **Openness**. Organizations provide relevant information to the persons concerned at the time of the collection or consent. They release their contact information and clear information on their policies and practices on the management of personal information.
- **Rights of the individuals concerned**. Individuals can access their personal information and request that it be corrected or, in some cases, removed. Organizations establish accessible processes to enable these rights to be exercised.
- **Recourse**. If they are dissatisfied, people can contest a refusal to exercise a right or file a complaint with the organization or a competent body.

What is meant by "adequate protection"?

The notion of "adequate protection" is not defined in the Access Act or the Privacy Act.

It may be said that it consists of protection that provides **legal** (legislation of the receiving state) and **contractual** (agreement with the receiving organization) guarantees complying with all generally accepted and appropriate protection principles with regard to the sensitivity and purpose of the information involved.

If you conclude that the personal information will not have adequate protection, you must refuse to disclose it or refrain from entrusting it to a third party outside Quebec.

OSLER | UNOFFICIAL TRANSLATION OF CAI GUIDANCE

What should the written agreement that follows the PIA contain?

The disclosure of personal information outside Quebec must involve a written agreement between you and the third party. It should include the results of the PIA. Where necessary, it should include agreed-upon terms and conditions to mitigate the risks identified in the assessment in order to achieve adequate protection.

7.2 Information or electronic service delivery system

These clarifications relate to the situation set out in section 63.5 of the Access Act and section 3.3 of the Private Sector Privacy Act.

A PIA is required for every project associated with an **information or electronic service delivery system** that involves the collection, use, disclosure, retention or destruction of personal information. This can be a project involving:

- Acquisition
- Development
- Redesign

What is an “information or electronic service delivery system”?

An **information system** can take many forms. It is not necessarily computerized, although it frequently is. It may include:

- A computerized file processing system
- Videoconferencing or collaboration software
- A biometric system
- An artificial Intelligence system
- A smart card/RFID system
- A video surveillance system
- A statistical system
- A payroll management system

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Examples of **electronic service delivery systems** include a:

- Self-service terminal
- RFID/NFC payment service
- Website member area
- Electronic record
- Mobile app

7.3 Disclosure for study, research or statistical production purposes

These clarifications relate to the situation set out in section 67.2.1 of the Access Act and section 21 of the Private Sector Privacy Act.

The **disclosure of personal information without the consent** of the persons concerned to an individual or organization (hereinafter, the researcher) wishing to disclose the information for **study, research, or statistical purposes** (hereinafter, the research) is only permitted if a PIA determines that certain criteria have been met.

Who should conduct the assessment: the organization or the researcher?

The PIA should be done by **the organization holding** the personal information, based in part on the elements provided by the researcher. For example, the researcher is in a good position to describe how the personal information will be used after its disclosure, why it is necessary for the research and the security measures used on site.

Note that the decision of a research ethics board **cannot replace the PIA that must be completed by the organization holding** the personal information. However, its content and recommendations can be useful for the PIA.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

What should this PIA show?

The PIA may follow the general approach set out in this guide. However, it should allow you to show that each of the five criteria provided for by law has been met.

1. The purpose of the research can be achieved only if the information is disclosed in a manner that identifies the persons concerned

For example, if the research or study can be conducted using **anonymized information**[18] or synthetic data, the disclosure of personal information is not permitted.

If the research can be conducted using **de-identified information**[19], only that information should be disclosed. It is important to mention that this information is still confidential personal information. It is up to the researcher to convince you of the need to use personal information, whether de-identified or not. The use of non-de-identified information requires a compelling demonstration that the research cannot be conducted without "direct identifiers."

2. It is unreasonable to require the researcher to obtain the consent of the persons concerned regarding the protection of personal information and their right to privacy

Since this is an exception to the principle of consent, the organization must be able to conclude that it is unreasonable to require the consent of all the persons whose information is required for research purposes. This could be the case, for example, in the following situations (these examples are not exhaustive, and in all cases must be contextualized in relation to the specific research being evaluated):

- It may be unreasonable to obtain the consent of thousands of persons whose contact information is not up to date.
- The research could include information from persons who are unable to consent or who are deceased.
- The research could be based on de-identified information held by your organization, thus making it impossible for the researcher to obtain consent.
- In some cases, building a representative sample may require avoiding the bias caused by using only data from persons willing to consent.

Important note: The lack of human, financial or material resources is not sufficient reason to show that obtaining consent is unreasonable.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[18] Information is **anonymized** when it is reasonable to anticipate under the circumstances that it can no longer, at no time and irreversibly, directly or indirectly identify a person. Information must be anonymized in accordance with generally accepted best practices and the criteria and procedures determined by regulations.

[19] Information has been **de-identified** when it prevents the person concerned from being directly identified.

3. In terms of public interest, the sought-after objective overrides the impact of the disclosure and use of personal information on the privacy of the individuals concerned

This part of the PIA is intended to weigh the purpose of the research in terms of public interest and the impact of the disclosure and use of the personal information on the privacy of the persons involved.

The analysis must first identify and describe the various elements and factors to be considered in making this weighting.

You must then determine whether the objective of the research in terms of public interest outweighs its potential privacy implications.

Here are some sample questions to ask when assessing a researcher's request:

- What is the purpose of the research and how does it serve public interest?
- What benefits to society are expected?
- What are the different privacy implications for the persons concerned by the disclosure of information?
- Can these consequences be minimized in relation to the research? If so, how?
- Is the personal information being requested sensitive?
- Will the information be combined or compared with other information? If so, how will this affect the privacy of the individuals involved? Will these practices have an impact on the risk of disclosing personal information about one or more persons?
- What indication is there that public interest outweighs the impact of the disclosure and use of personal information on the privacy of the people concerned?

Important note: The evaluation of this criterion is not limited to stating the purpose of the research or simply stating a general impact, such as that it will increase knowledge in a certain field. **You must indicate the expected benefits from the research in relation to public interest and weigh them against the impact on the privacy of the persons whose information will be used for the research.**

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

4. The personal information is used in a manner that ensures its confidentiality

This part of the analysis must assess whether the intended use of the information and the various safeguards that will be put in place will ensure its confidentiality. This must be done when you disclose the information, but also at all stages of the research. This assessment should take into account the sensitivity and quantity of the personal information.

5. Only necessary information is disclosed

The PIA should indicate how the organization will ensure that only the information **needed** for the research will be provided to the researcher. There should be special focus on "direct and indirect identifiers" (related to the first criterion, such as full address with postal code, health insurance number, date of birth or age) and particularly sensitive information.

What steps come after the PIA?

You must enter into a written agreement with the researcher, the contents of which are specified in the Access Act and the Privacy Act. You must then forward the agreement to the Commission. The agreement takes effect 30 days after it has been received by the Commission.

Should a PIA report be sent to the Commission?

Yes, it is expected that a PIA report be included with the agreement sent to the Commission. A written document confirming the PIA process allows your organization to prove that it has met its obligation. The document outlines how each criterion was analyzed and what elements were considered.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

7.4 Collection by a public body on behalf of another

These clarifications relate to the situation set out in section 64 of the Access Act.

A PIA is required when a public body:

- Collects personal information required for the exercise of powers or the implementation of a program of another public body with which it is collaborating
- Collects this type of information for the purpose of providing services or carrying out a common mission
  - For example, an organization may collect personal information for the purpose of verifying the eligibility of persons for a program it is administering.

Transitional provisions apply for agreements already in force on the date the PIA becomes mandatory, namely, on September 22, 2023[20].

Who should conduct the assessment?

The PIA should be conducted by the organization that will ultimately hold the personal information, that is, the organization that requests another public body to collect personal information on its behalf, while collaborating, if necessary, with the organization assisting it. The latter is ideally suited, for instance, to describe how the personal information will be collected, what security measures will be implemented, etc.

What steps come after the PIA?

Cooperating organizations must enter into a written agreement, the contents of which are specified in section 64 of the Access Act. They must then forward the agreement to the Commission. The agreement takes effect 30 days after it has been received by the Commission.

Should a PIA report be sent to the Commission?

Yes, it is expected that a PIA report be included with the agreement sent to the Commission. A written document confirming the PIA process allows your organization to prove that it has met its obligation.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[20] Agreements entered into under sections 64 and 68 of the Access Act before September 22, 2023 will remain in force until September 22, 2025, or until their expiry date, whichever comes first (section 174 of Bill 25). A PIA will now be required to **renew** or **amend** the agreement.

7.5 Other types of disclosures without consent (Public sector)

These clarifications relate to the situation set out in section 68 of the Access Act.

A PIA must also be done and conclude that certain criteria have been met before a **public body discloses personal information without consent:**

- To another public body, in or outside Quebec:
  - For the exercise of its powers or the implementation of a program under its administration
  - Where the disclosure clearly benefits the person concerned
- To any person or organization:
  - When warranted by exceptional circumstances
  - For the provision, by a public body, of a service to the person concerned, such as for identification purposes

Transitional provisions apply for agreements already in force on the date the PIA becomes mandatory, namely, on September 22, 2023[21].

Who should conduct the assessment?

The PIA should be done by **the organization holding** the personal information, based in part on the elements provided by the recipient of the disclosure. The latter is ideally suited to describe, for instance, how the personal information will be used after its disclosure and what security measures applied on site.

What should this PIA show?

For these other types of disclosure to be made, the PIA must conclude that the following four criteria have been met:

1. The purpose can only be achieved if the information is disclosed in a manner that identifies the persons concerned

For example, if the purpose of the disclosure can be met using anonymized information or synthetic data, the disclosure of personal information is not permitted.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

[21] Agreements entered into under sections 64 and 68 of the Access Act before September 22, 2023 will remain in force until September 22, 2025, or until their expiry date, whichever comes first (section 174 of Bill 25). A PIA will now be required to **renew** or **amend** the agreement.

If the purpose of the disclosure can be met with **de-identified information**, only that information should be disclosed. It is important to mention that this information is still confidential personal information. It is up to the public body to justify the need to use personal information, whether de-identified or not.

The use of non-de-identified information requires a compelling demonstration that the research cannot be conducted without "direct identifiers."

2. It is unreasonable to require the consent of the person concerned

Since this is an exception to the principle of consent, you must be able to conclude that it is unreasonable to require the consent of all the individuals whose information is required for the disclosure being considered.



Important note: The lack of human, financial or material resources is not sufficient reason to show that obtaining consent is unreasonable.

3. In terms of public interest, the sought-after objective overrides the impact of the disclosure and use of personal information on the privacy of the individuals concerned

This part of the PIA is intended to weigh the purpose of the disclosure in terms of public interest and the impact of the disclosure and use of the personal information on the privacy of the persons involved.

This analysis must be preceded by an identification and description of the various elements and factors to be considered in making this weighting.

You must then determine whether the purpose of the disclosure in terms of public interest outweighs its potential privacy implications.

Here are some sample questions to ask when assessing disclosure to another public body:

- What is the purpose of the disclosure and how does it serve public interest?
- What benefits are expected for the persons concerned and for society?
- What are the different privacy implications for the persons concerned by the disclosure of information?
- Can these consequences be minimized in relation to the disclosure? If so, how?
- Is the personal information involved sensitive?

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

- Will the information be combined or compared with other information? If so, how will this affect the privacy of the individuals involved? Will these practices affect the risk of disclosing personal information about one or more people?
- What indication is there that public interest outweighs the impact of the disclosure and use of personal information on the privacy of the people concerned?

Important note: The assessment of this criterion is not limited to stating the purpose of the disclosure or simply describing a general impact, such as "improvement in services." **You must indicate the expected benefits from the anticipated disclosure in relation to public interest and weigh them against the impact on the privacy of the persons whose information will be disclosed.**

4. The personal information is used in a manner that ensures its confidentiality

In this part of the analysis, you must determine whether the intended use of the information and the safeguards that will be put in place when the information is disclosed by the organization will ensure its confidentiality. This assessment should take into account the sensitivity and quantity of the personal information.

What steps come after the PIA?

You must enter into a written agreement with the third party, the contents of which are specified in section 68 of the Access Act. You must then forward the agreement to the Commission. The agreement takes effect 30 days after it has been received by the Commission.

Should a PIA report be sent to the Commission?

Yes, it is expected that a PIA report be included with the agreement sent to the Commission. A written document confirming the PIA process allows your organization to prove that it has met its obligation. The document outlines how each criterion was analyzed and what elements were considered.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Was this information tool useful to you?
Complete our short satisfaction survey!

Montreal

2045 Stanley, Suite 900
Montreal, Quebec H3A 2V4
Telephone: 514-873-4196

Quebec City

525 Boul. René-Lévesque Est, Suite 2.36
Quebec City, Quebec G1R 5S9
Telephone: 418-528-7741

Commission d'accès à l'information du Québec

1-888-528-7741 | cai.gouv.qc.ca