Privacy Impact Assessment

Prepared for:

Prepared by:

Version Control

Version:

Date:

Primary Author:

Signature:

Table of Contents

[Introduction 3](#_Toc95914869)

[Section I – Overview and PIA Initiation 3](#_Toc95914870)

[Section II — Risk Area Identification and Categorization 3](#_Toc95914871)

[Risk Scales 4](#_Toc95914872)

[Type of Program or Activity 4](#_Toc95914873)

[Type of Personal Information Involved 4](#_Toc95914874)

[Program or Activity Partners 5](#_Toc95914875)

[Duration of Program 5](#_Toc95914876)

[Program Population 5](#_Toc95914877)

[Technology and Privacy 6](#_Toc95914878)

[Personal Information Transmission 6](#_Toc95914879)

[Breach Impact - Individual 6](#_Toc95914880)

[Breach Impact - Institutional 7](#_Toc95914881)

[Section III–Analysis of Personal Information Elements for the Program or Activity 7](#_Toc95914882)

[Section IV–Flow of Personal Information for the Program or Activity 7](#_Toc95914883)

[Section V–Privacy Compliance Analysis 8](#_Toc95914884)

[Section VI–Summary of Analysis and Recommendations 9](#_Toc95914885)

[Section VII–Supplementary Documents List 9](#_Toc95914886)

[Section VIII–Formal Approvals 9](#_Toc95914887)

# Introduction

*Provide a background introduction and/or overview of the program being assessed and the need for the PIA.*

*The following sections and their information requirements make up the minimum content of a core Privacy Impact Assessment (PIA). In the case of a multi-institutional PIA, each institution involved should be responsible for contributing to or completing the core PIA in a manner that is consistent with the approach outlined by the lead institution.*

# Section I – Overview and PIA Initiation

*Identify the institution or, in the case of a multi-institutional PIA, the lead government institution and the partner institutions.*

*Identify the head of the institution or delegate or, in the case of a multi-institutional PIA, the head or delegate of each institution involved in the program or activity.*

*Identify the appropriate senior official or executive for the new or substantially modified program or activity.*

*Provide the name and description of the program or activity of the institution or, in the case of a multi-institutional PIA, of the lead institution.*

*Identify the legal authority for the program or activity or, in the case of a multi-institutional PIA, the legal authority for each institution involved in the program or activity.*

*Provide a short description of the project or initiative, or the proposed change(s) to existing ones.*

*In the case of a multi-institutional PIA, the lead institution should describe the approach for the completion and approval of the PIA in support of the program or activity. At a minimum, a multi-institutional PIA will identify the institutions involved and ensure that the role of each institution with respect to the program or activity is adequately documented, unless otherwise determined by the approach.*

# Section II — Risk Area Identification and Categorization

*The core PIA must include a completed risk identification and categorization section as outlined below. To have consistent risk categories and risk measurement across partner institutions, standardized risk areas (itemized below) and a common risk scale should be maintained as the basis for risk analysis.*

*The numbered risk scale is presented in an ascending order: the first level (1) represents the* ***lowest*** *level of potential risk for the risk area; the fourth level (4) represents the* ***highest*** *level of potential risk for the given risk area.*

*The initial step of the analysis consists of evaluating each risk area independently. The second step consists of grouping the individual results to determine if a more in-depth analysis is required. The greater the number of risk areas identified as level 3 or 4, the more likely it is that specific risk areas will need to be addressed in a more comprehensive manner.*

## Risk Scales

### Type of Program or Activity

|  |  |
| --- | --- |
| **Type of program or activity** | **Risk scale** |
| Program or activity that does NOT involve a decision about an identifiable individual | 1 |
| Administration of program or activity and services | 2 |
| Compliance or regulatory investigations and enforcement | 3 |
| Criminal investigation and enforcement or national security | 4 |

### Type of Personal Information Involved

|  |  |
| --- | --- |
| **Type of personal information involved and context** | **Risk scale** |
| Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program. | 1 |
| Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source. | 2 |
| Social Insurance Number, medical, financial or other sensitive personal information or the context surrounding the personal information is sensitive; personal information of minors or of legally incompetent individuals or involving a representative acting on behalf of the individual. | 3 |
| Sensitive personal information, including detailed profiles, allegations or suspicions and bodily samples, or the context surrounding the personal information is particularly sensitive. | 4 |

### Program or Activity Partners

|  |  |
| --- | --- |
| **Program or activity partners and private sector involvement** | **Risk scale** |
| Within the institution (among one or more programs within the same institution) | 1 |
| With other government institutions | 2 |
| With other institutions or a combination of federal, provincial or territorial, and municipal governments | 3 |
| Private sector organizations, international organizations or foreign governments | 4 |

### Duration of Program

|  |  |
| --- | --- |
| **Duration of the program or activity** | **Risk scale** |
| One-time program or activity | 1 |
| Short–term program or activity | 2 |
| Long-term program or activity | 3 |

### Program Population

|  |  |
| --- | --- |
| **Program population** | **Risk scale** |
| The program's use of personal information for internal administrative purposes affects certain employees. | 1 |
| The program's use of personal information for internal administrative purposes affects all employees. | 2 |
| The program's use of personal information for external administrative purposes affects certain individuals. | 3 |
| The program's use of personal information for external administrative purposes affects all individuals. | 4 |

### Technology and Privacy

|  |
| --- |
| **Technology and privacy** |
| Does the new or substantially modified program or activity involve implementation of a new electronic system or the use of a new application or software, including collaborative software (or groupware), to support the program or activity in terms of the creation, collection or handling of personal information? |
| Does the new or substantially modified program or activity require any modifications to information technology (IT) legacy systems? |
| Specific technological issues and privacy  Does the new or substantially modified program or activity involve implementation of new technologies or one or more of the following activities:   * enhanced identification methods; * surveillance; or * automated personal information analysis, personal information matching and knowledge discovery techniques? |
| A **YES** response indicates the potential for privacy concerns and risks, which will require consideration and, if necessary, mitigation. |

### Personal Information Transmission

|  |  |
| --- | --- |
| **Personal information transmission** | **Risk Scale** |
| The personal information is used within a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled). | 1 |
| The personal information is used in a system that has connections to at least one other system. | 2 |
| The personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed. | 3 |
| The personal information is transmitted using wireless technologies. | 4 |

### 

### Breach Impact - Individual

|  |  |
| --- | --- |
| **Breach Impact – Individual** | **Risk Scale** |
| No impact to individuals or employees in the event of a privacy breach | 1 |
| Small impact to individuals or employees in the event of a privacy breach | 2 |
| Large impact to individuals or employees in the event of a privacy breach | 3 |

### Breach Impact - Institutional

|  |  |
| --- | --- |
| **Breach Impact - Institutional** | **Risk Scale** |
| No impact to the institution in the event of a privacy breach | 1 |
| Small impact to the institution in the event of a privacy breach | 2 |
| Large impact to the institution in the event of a privacy breach | 3 |

*A tools such as a Risk Scoring Summary Matrix can also be created to summarize and visualize program risks. Please see Privacy Assessment Guide Appendix A for more information.*

# Section III–Analysis of Personal Information Elements for the Program or Activity

*Identify each element of personal information collected (for example: 1) name, 2) address) and sub-elements associated with each element of personal information collected (for example: 1) first name / middle initial / last name, 2) street name / street number / city / province /postal code).*

*Identify how the personal information will be recorded: on paper, electronically, audio recordings, visual image recordings, human biological samples or other (specify).*

*In the case of a multi-institutional PIA, each institution involved is, at a minimum, responsible for identifying the elements of personal information collected or disclosed in relation to their involvement in the multi-institutional program or activity.*

# Section IV–Flow of Personal Information for the Program or Activity

*Identify the source(s) of the personal information collected and / or how the personal information will be created.*

*Identify both internal and external sources for the personal information's use and disclosure, that is, identify the areas, groups and individuals who have access to or handle the personal information and to whom it is provided or disclosed. Where relevant, include the following information:*

* + *Primary institution responsible for the program or activity;*
  + *Other institutions responsible for the program or activity; or*
  + *Other institutions (e.g., governments or councils, international organizations/NGOs or private sector organizations) involved.*

*Identify where the personal information will transit and will be stored or retained.*

*Identify where areas, groups and individuals can access the personal information.*

*The institution may determine the preferred format for representing the flow of personal information.*

*In the case of a multi-institutional PIA, each institution involved is, at a minimum, responsible for outlining the flow of personal information under its control. The lead institution will be responsible for outlining the flow of personal information between or among institutions.*

# Section V–Privacy Compliance Analysis

*At a minimum, the privacy compliance analysis should cover the following areas and identify specific compliance actions taken or to be taken to meet with each area's requirements:*

* + *Authority to collect Personal Information*
  + *Policies for direct collection, notification and consent, as appropriate*
  + *Retention policy*
  + *Accuracy policy*
  + *Use of data*
  + *Disclosure of data*
  + *Administrative, physical and technical safeguards and security measures*
  + *Technology and privacy issues*
    - *Indicate any changes to the business requirements that have an impact on the system, software or program application and, consequently, may affect the current access controls and privacy practices related to the creation, collection, retention, use, disclosure and disposition of personal information.*
    - *Determine whether the current IT legacy systems and services that will be retained or those that will be substantially modified are compliant with privacy requirements.*
    - *Identify any awareness activities related to protection of privacy requirements in the new electronic environment.*

*In the case of a multi-institutional PIA, each institution involved is, at a minimum, responsible for outlining the privacy practices for the personal information under its control.*

# Section VI–Summary of Analysis and Recommendations

*Document the conclusion drawn or recommendations resulting from the risk identification and categorization in a manner that is commensurate with the risk identified.*

# Section VII–Supplementary Documents List

*List any additional documents that were used or are related to the core PIA; these documents do not need to be appended to the core PIA.*

# Section VIII–Formal Approvals

*Indicate that the PIA was formally approved in accordance with the institution's approval process.*

*In the case of a multi-institutional PIA, indicate that the lead government institution determined the PIA was formally approved.*

Completion of the above sections with the information requested fulfills the recommended minimum content requirements of a core PIA.