Guide for Completing a Privacy Impact Assessment

Appendix B.ii of Protection of Personal Information Policy CORP.1-08

Notes:

- This Guide is intended to assist you with the completion of the Privacy Impact Assessment.
- When completing the Assessment, keep in mind that not all questions will be relevant to your project at this time.
- If a question is not applicable, answer “Not applicable,” but do not delete the question from the Assessment.
- Add additional questions and/or explanations as required by your project.
- Attach any relevant documents.
- Where appropriate, provide information on both the current plan, and future intentions for the program/service.
- “Change” means a change to a program or service that affects the collection, use, disclosure or retention of personal information and includes the implementation of an information system.
- It is important to remember your audience for this assessment. It is not intended to be an assessment of the technical architecture of the system, but an assessment of privacy issues arising from a change. Make an effort to keep information straightforward and understandable by a reader who does not have expertise in information system technology, law, or the background to the system.
- Avoid jargon and acronyms unless they are explained.
- Explain any terms, positions and organizations that are not commonly understood.
- Although information must be comprehensive, make an effort not to include information that is not necessary to the reader’s understanding of the change and its impacts.

1. Introduction

a) Name of Program or Service

b) Name of Department, Branch and Program Area

c) Name of Program or Service Representative

d) Key Program or Service Dates

This may include program or service initiation date, implementation date(s), project completion date, and other key milestones, if applicable.

2. Description

a) Summary of the New Program or Service or Change

i. General Description

Provide a brief explanation of the new program or service or change and include a brief explanation of the existing program, service or change.

ii. Purposes, Goals and Objectives

What are you trying to accomplish with this new program or service or change? For example:

improving client services
making program more efficient, saving on time and other resources
improving protection of privacy
standardization of a program component
tracking incidence of a specific event
obtaining sufficient information to administer the program

iii. The Need

Why are you making this new program or service or change?
Is it required by law, policy or standards?
Is it to fulfill a governmental/departmental commitment or mandate?

b) The Intended Scope

Outline both the planned and anticipated scope of the program or service. The "scope" may include:

Conversion from a paper based information system to an electronic information system.

Who is able to use the system? (e.g. in the current plan, only Department of XXX staff will have access to the system. In future it is anticipated that other Departments will have access). Note that the identification of specific users (e.g. clerks) will be covered in question 3 (g).

Linkages with other systems or programs (e.g. an example of anticipated linkage is a plan to "link data collection system X with billing system Y by 2007").

The type of information collected (e.g. in the first year the system will collect only name, address and contact information; by year three the system will include additional identifiable financial information).

Future enhancements to the system (e.g. remote access).

Future uses of the information (e.g. secondary use of data research or analysis).

c) **Conceptual Technical Architecture (if applicable)**

Identify and describe the types of applications, platforms, and external entities involved in the information flow. Describe their interfaces, services, and the context within which the entities interoperate.

This document is not intended to assess the technical security aspects of an electronic system. This section should be brief and clear to all readers. It is not intended to be or to replace a Threat Risk Assessment if one is required.

d) **Description of Information Flow (include text and diagram to describe flow as necessary)**

This section should include a diagram, but also requires a written description of any manual procedures and an identification of the staff who will be users of the system or who will receive information from the system.

3. Collection, Use and Disclosure of Personal Information

NOTE: Tables would be helpful to organize the answers to (a), (b), (c), and (d)

a) **Authority for the Collection, Use and Disclosure of Personal Information**

Is there a law, regulation or authorized policy that allows you to **collect** the personal information as outlined in the new service or program or change?
Is there a law, regulation or authorized policy that allows you to **use** the personal information as outlined in the new program or service or change?
Is there a law, regulation or authorized policy that allows you to **disclose** the personal information as outlined in the new program or service or change?

b) **List of Personal Information to be Collected, Used and/or Disclosed, the Method of Collection and Disclosure, and the Rationale for each.**

There must be a reason or intended use for each item of personal information.

List each item or field to be collected, and the reason or intended use for the collection.

For example:

Telephone number: To contact clients to update them on program changes
Financial information: To verify income

In general, good privacy principles mandate that the minimum amount of information necessary for the purpose is collected, used and disclosed. Is it necessary to collect each item of personal information to fulfill your purposes?

For example: do you need date of birth or would month and year of birth or age in years be sufficient?

In some cases it may be necessary to include information which may not appear to the writer to be “personal information”. This can be discussed with the reader; there may be information that in combination with other information would be categorized as “personal information”.

Do not exclude data elements on the basis that you think there are no privacy issues with the data elements. The data, in combination with other data held on this system or others may raise privacy issues.

Example of a table for this section:

Data Element	**Rationale for Collection, Use and/or Disclosure**	**Method of Collection and Disclosure**	**Comments**
Name	Collected to identify clients	Provided by client on application form Disclosed by email to approved vendors	

c) The Sources and Accuracy of the Personal Information

Who is providing the information – the individual or another source (e.g. another government department, a family member)?
Is the information as accurate and up to date as is necessary for the purposes for which it would be used and disclosed?
Are there any data quality issues that are linked to user and system performance?

d) The Location of the Personal Information

Is the information on servers or in a data repository? Will it be recorded on paper only and maintained in files?
Where will the information be located? List all locations
Will the information be stored in multiple locations? For example, will users be permitted to store information on other devices (e.g. laptops) or produce information from system (e.g. print and store in files)? If “Yes”, do you have a policy on protection of information held on electronic devices?
Will the data be interfaced with data from other systems?
If there is a data repository, give the name, description and geographical location of the repository.

e) The Retention Schedule and Method of Destruction or De-identification for Personal Information

Is this information currently addressed in the Classification and Retention Schedule or is there a timetable for keeping the information in its identifiable form?

Is retention monitored for compliance to the schedule?

What is the plan and method of destruction (if any)?

f) Identification of Consent Issues

Are you required by law, regulation or policy to obtain consent for the collection, use or disclosure of personal information?

For example:

Sections 29, 31, 32 of MFIPPA outline the circumstances under which a municipality body may use and disclose personal information with and without consent.

Do any of these sections apply?

Please note that consent is not always required for collection, use and disclosure. It is important for you to confirm whether or not consent is required.

Has the individual consented to the collection, use and disclosure anticipated in the new program or service or change? If yes, what is the method of requesting consent? Attach any consent form(s), and outline the process for obtaining consent.

If consent has not been collected, have the subject individuals been notified (either specifically or generally) of the new program or service or change?

g) Users of Personal Information

List the users (positions, not names) who will have access to the information.

Describe the level of access each user group will have to personal information

Include a brief rationale for each user's need to access the information.

A table would be very helpful for completion of this section:

User Group	Level of Access	Rationale	Comments
Clerical Staff	Demographic information only (Name, Address)	To address Letters and forms to clients	

4. Access Rights for Individuals to their Personal Information

Will individuals have access to their personal information on the system?

Note: MFIPPA gives individuals the rights of access to their own personal information with certain restrictions.

If yes:
Describe your process for allowing individuals access to their personal information; and
Indicate if individuals will be informed of the following: the information source(s) of their personal information?
The uses and disclosures of their personal information? (see notice of collection template)

5. Privacy Standards: Concerns and Security Measures

a) Security Safeguards

Administrative Safeguards

Do contracts with external service providers contain privacy provisions, which meet or exceed the privacy standards of the Municipal Freedom of Information and Protection of Privacy Act?
Has staff received training on privacy and confidentiality policies and practices?
Is access to the personal information restricted on a “need to know” basis? How is this determined?
What controls are in place to prevent and monitor misuse of the personal information)?
Is there a process in place for access or role changes for system users (e.g. users who leave employment or change jobs)?
Describe the process in case of a breach of privacy.

Basic Technical Safeguards

Note: This section is intended to capture information related to basic technical safeguards (e.g. passwords, security related to the location of the information (e.g. locked filing cabinets). It is not intended to capture and assess the security elements of an information system which would be more properly assessed in a Threat/Risk Assessment.

How is the personal information collected and transferred from the individual to the system/program?
For example: electronic, paper, fax, and courier
If the information is transmitted in electronic format, is it being transmitted within a secured server, is it encrypted?
Are all accesses to the system password protected?
Are all users trained on good password practices?
Is there an automatic prompt for users to change their passwords?
If yes, how often are they asked to change the password?
Is remote access to the information permitted? If yes, what is the method for access? Is the information secure on transfer?
Will the system be tested to ensure privacy controls are functioning?
Are fax machines located in a secure, private area?

Are paper files secured in a locked area with controlled access?

Auditing

Does the level of sensitivity of the information require that use of this system be audited? If "No", why not?
Does the system have the capability to audit access and/or view the system?
What is the level of information that audit can produce (e.g. can it identify individual patients/clients, pieces of information etc. that the user viewed)?
Does the audit always run, or is it a system that must be switched on and off?
Is there a limit to the time audit information is kept?
Will an auditing plan be developed?
Are resources being committed to the auditing and follow-up function?

b) Avoidance of Unintentional Disclosure

Is the information reviewed prior to disclosure to prevent unintentional disclosure of personal information?
When statistical information about a small group of individuals is disclosed outside the Department, there is a risk that these individuals could be identified.
As a general guideline, do not disclose statistical information about groups (cells) containing less than 5 individuals.
Are small cell sizes (e.g. cells of less than five) disclosed?
If small cell sizes are to be disclosed, what is the rationale for doing so?

6. Conclusions

a) An Assessment of the Impact on Privacy, Confidentiality and Security of Personal Information as a Result of the New Program or Service or Change

Assess the privacy, confidentiality and security impact on personal information as a result of: The new program or service; Changes to the current program or service; Or anticipated future changes to the program or service. Discuss both negative and positive impacts

b) Strategy for Mitigation of Privacy Risks

Outline any plans or proposals for reducing or eliminating any negative impacts on privacy.

c) Additional Comments

Make any additional comments related to the privacy impact(s).