PRIVACY IMPACT ASSESSMENT TOOL

CONTENTS

September 2015

Manitoba Ombudsman
750 - 500 Portage Avenue
Winnipeg, MB R3C 3X1

204-982-9130 (phone)
1-800-665-0531 (toll-free in Manitoba)
204-942-7803 (fax)
ombudsman@ombudsman.mb.ca (general email inquiries)

www.ombudsman.mb.ca

Introduction

Under *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA), public bodies and trustees (organizations) have specific privacy obligations. These include how you collect, use and disclose the public's personal and personal health information.

Protecting privacy is more than just upholding the law, it also involves taking a proactive approach to safeguarding the public's personal (health) information.

Risks to privacy can arise in many circumstances. Collecting excessive information, using intrusive means of collection, or obtaining sensitive details in unexpected circumstances all represent risks to the individual. The use or disclosure of that information, or its retention for an unduly long period, puts privacy at risk.

Many organizations use privacy impact assessment (PIA) tools to assist in safeguarding Manitobans' personal (health) information.

To support organizations in achieving this goal, Manitoba Ombudsman has developed a PIA tool that "tells the story" of a project from a privacy perspective. Simply, it encourages organizations to think about privacy when evaluating an existing or proposed program, service or activity.

It is our intent that this PIA tool will assist organizations in identifying potential privacy risks and as a result, they will be in a better position to address those risks early on.

This PIA tool is not intended to replace any processes you may already have or be a substitute for complying with FIPPA and PHIA. Our office encourages you to review the information gathered through this process with an access and privacy representative (access and privacy coordinator, privacy officer, lawyer, etc.) so that you can address specific privacy requirements.

Acknowledgments

We gratefully acknowledge the contributions of the Nova Scotia department of Justice, British Columbia Office of the Chief Information Officer, University of Manitoba, Office of the Information and Privacy Commissioner of Alberta and New Zealand's Privacy Commissioner's Office to our *Privacy Impact Assessment Tool*. Our tool incorporates much of their collective advice and knowledge.

Frequently Asked Questions

What is a privacy impact assessment (PIA)?

A PIA is a process that an organization can use to identify and address potential privacy risks when contemplating a new, or evaluating an existing, program, service or activity. The PIA process examines potential impacts to privacy and considers reasonable measures to lessen these impacts.

When should I complete a privacy impact assessment?

You should consider completing a PIA for any new systems, projects, programs, services or activities that may involve personal (health) information.

If your initiative will not involve the collection, use or disclosure of personal (health) information, consult your access and privacy representative to determine whether a PIA is recommended. For example, a PIA may be useful in assessing risks regarding personal (health) information that has been de-identified (a record in which identifying information has been removed).

Does Manitoba law require that a PIA be completed?

No, it is not currently a legal requirement under FIPPA and PHIA to complete a PIA. However, some organizations may have policies in place that require a PIA be completed in some circumstances. A PIA is recommended to:

- Determine when and how a project will impact privacy
- Assist organizations in exercising due diligence
- Address any privacy risks
- Save time and money by identifying privacy issues early in the design stage
- Assure the public that their personal (health) information will be managed and safeguarded appropriately

What is considered personal (health) information?

Personal information* is any recorded information about an individual. Examples include a person's name, address, telephone number, a number that can identify them (for example, case file number, credit card number or social insurance number), and financial information.

Personal health information* is recorded information about an individual that relates to the individual's health, such as diagnosis and treatment information, or relates to or was collected in the provision or payment of health care such as an individual's name, address, telephone number or personal health identification number (PHIN).

It is important to note that personal (health) information includes information that can be combined with other information to identify a specific individual. For example, if information such as gender were linked to health information and only one individual in a small office was of that gender, that individual will be able to be identified.

** For complete definitions as outlined in FIPPA and PHIA, please refer to Appendix A at the end of this guide.*

Before Getting Started

If a question is not applicable, answer "Not Applicable". Do not delete the question from the assessment.

Add additional questions and/or explanations as required by the details and scope of your program/activity.

Attach any relevant documents.

Where appropriate, provide information on the current plan, and also the future intentions for the program/service/change.

"Change" means a change to a program or service that affects the collection, use, disclosure or retention of personal (health) information and includes the implementation or modification of an electronic information system.

It is important to remember your audience for this assessment. It is not intended to be an assessment of the technical nature of a system, but an assessment of privacy issues arising from a change. Make an effort to keep information straightforward and understandable by readers who do not have expertise in information system technology, law, or the background to the system undergoing the change.

Avoid jargon and acronyms unless they are defined or explained.

Explain any terms that are not commonly understood.

Although the assessment must be comprehensive, make an effort not to include information that is not necessary for the reader's understanding of the proposed change.

Once completed, please review and/or consult with your access and privacy representative to ensure the proposed or existing program meets the requirements of applicable privacy legislation.

Note: Please answer the questions in the PIA tool on the following pages in a separate document. Fillable versions of the PIA tool are available on the Manitoba Ombudsman website at www.ombudsman.mb.ca (navigate to the Access and Privacy Division and select "Privacy Impact Assessment" on the left navigation menu).

Privacy Impact Assessment Tool

Part 1: Summary of program or activity

Who?

Name of project
Name of department, branch, and/or program area
Name(s) of project representatives
List any external entities that may be involved

What?

Summary of the new program, service, software, or change
Provide an explanation of the new program, service or change and include an explanation of the current state.

Purposes, goals and objectives
Describe what you are trying to accomplish with the new program, service or change. For example: improving client services, improving efficiencies, improving privacy protection, streamlining processes.

Describe the type of application
Identify and describe the types of applications, platforms and external entities involved in the information flow (collection, use and disclosure).

Why?
Explain why you are implementing the new program, service or change, and describe the benefits.

Where?
Where is the data flow taking place? Is it online, in person, paper-based, in Manitoba, in Canada or the United States?

When?
Outline any key dates such as project deadlines, key milestones, implementation timeframes, contract parameters.

Part 2: Describe the scope

1. **Describe the flow of personal (health) information**

Provide a description of how the information will flow within the organization, including any disclosures (information provided outside the organization). This section should include a brief description (written or visual) showing the flow of personal (health) information through the system from collection to use within the organization, and disclosures (sharing) outside the organization (if applicable). Refer to Appendix B for an example of a data flow chart.

2. **Who manages, accesses and uses the system?**

Describe who manages the system. Outline who are the intended users of the system within the organization and their connection(s) to the new program, service or change.

3. **Are there any linkages to other systems?**

Explain any linkages to other programs or services. For example, will data be collected from other systems and/or will data be shared with other systems? Provide timelines and explanation if future linkages are planned but won't be implemented immediately.

4. Do you anticipate any potential future enhancements to the system?

Will the system expand to include more users? Is a series of upgrades part of the contract for a new service or system?

5. Are there any potential future uses of information?

Are there any planned secondary uses for the personal (health) information in the system such as research or analysis? A secondary use of the information is any use that is different from the reason the information was collected in the first place.

Part 3: Collection, use and disclosure of personal (health) information

1. Authority for the collection, use and disclosure of personal (health) information

Indicate the specific provision of the law, regulation or authorizing policy that allows you to collect, use and disclose personal (health) information. Such laws and regulations could include FIPPA, PHIA or the governing legislation for the organization. Please indicate your authorization for:

- Collection
- Use
- Disclosure

2. Categories of personal (health) information to be collected, used and/or disclosed

i. Complete chart (see an example in Appendix C)
List the personal (health) information that will be collected and briefly explain the intended use and the potential disclosures of the information. Personal (health) information can be categorized based on the listing provided in Appendix D.

ii. Describe decisions and approval processes regarding collection, use and disclosure decisions
Briefly describe the decision-making and approval process that governs the collection, use and disclosure of personal (health) information in the system. For example, how is management involved in the decision-making process?

3. Source and accuracy of personal (health) information

Briefly describe who is providing the personal (health) information to your program. For example, is it the individual or another source such as a government department or a family member?

How do you ensure that the information received is accurate? How do you ensure the information remains accurate and can be updated?

4. Notification statements

Please provide a sample of your privacy notification statement(s) used to inform individuals about the collection, use and disclosure of their personal (health) information, your legal authority, and contact information for questions. Indicate if you think any changes need to be made or the statements updated.

If the data is held and/or managed outside of your organization and/or in another jurisdiction (for example, when an organization collects personal (health) information that flows directly to and is held and managed by a company in the United States), please indicate if and how you intend to notify individuals of where their data is stored. This would not include situations where there is a routine transfer of personal/health information.

Part 4: Access rights for individuals

Under FIPPA and PHIA individuals have a right to:

- request access to and obtain a copy of their personal (health) information held by a public body or trustee, and
- request a correction.

Ability to provide an individual access to their own personal (health) information held in either an electronic or hard copy system

Explain how you will provide individuals with access to their own personal (health) information, including how you will provide copies if requested.

Describe how you will correct personal (health) information of an individual if required.

Part 5: Privacy and security measures

1. Security safeguards

i. Administrative safeguards

Describe the internal policies, procedures, and guidelines that are applicable to this program, service or system.

Explain how the policies, procedures or guidelines address privacy protection and security standards.

If the service or system includes personal health information, describe how the PHIA orientation sessions and the signing of the PHIA pledges of confidentiality will be managed.

Describe any additional confidentiality agreements in place that relate to security.

Describe the process of what would happen if there is a privacy/security breach.

ii. Technical safeguards

Will the system be used by internal (staff) and/or external users (program participants)?

Will the system be capable of providing role-based profiles and passwords for all users?

If the system can be accessed by external users, describe the identity authentication process that will be used.

How is personal (health) information collected from individuals? (Paper, electronic, both)

How is personal (health) information used, accessed and/or transported within the department, branch, or program area?

How is personal (health) information disclosed outside the organization?

iii. System audit functions

Does the level of sensitivity of the personal (health) information in the system require the system to be audited?

Does the system have audit functionality? If yes, describe.

Will there be regular audits of the system to detect security/privacy breaches?

Who will conduct the audits and who will follow up on the results?

2. The location of the personal (health) information

Describe where the paper/electronic records will be held. For example, onsite offices/servers, offsite storage facilities, and/or offsite servers.

i. Paper
ii. Electronic

3. Will any personal (health) information be stored by organizations outside Manitoba? Canada?

Describe the location of the personal (health) information.

If personal (health) information is stored outside Manitoba or Canada, please provide the rationale.

4. Records retention and destruction

Are there records retention schedules in place for the organization?

Do the schedules include the retention and destruction of both paper and electronic records?

Is records retention monitored by the organization to ensure compliance with schedules?

What is the plan and method of destruction? Paper? Electronic?

5. Information Managers

Under FIPPA and PHIA, an organization must enter into an information manager agreement if it discloses personal (health) information to an information manager (a third party outside the organization) for the purpose of:

- processing, storing or destroying the information, or
- providing the organization with information management or information technology services.

If your program/activity requires the use of an information manager, describe how the written agreement provides for the protection of the personal (health) information against such risks as unauthorized access, use, disclosure, destruction or alteration.

What is the length of the agreement?

Will the agreement be reviewed by legal counsel?

Part 6: PIA summary and findings

Conducting a PIA is primarily about the process of identifying and reducing privacy risks. To assist you in this process, the checklist below outlines information to include in your summary.

- √ A description of the proposal including: objectives, parties involved, timing and key milestones, resource requirements, benefits to the organization or public, and any relevant privacy requirements (applicable law, policies and procedures).
- √ The identified risks to privacy.
- √ How individuals may be affected by the identified risks.
- √ The likelihood of those risks occurring.
- √ Outline any plans or proposals that may eliminate or lessen the privacy risks.
- √ Identification of any residual risks (that cannot be addressed through the proposed options) and, the likely implications of those residual risks in terms of public reaction, project success and other organizational interests.
- √ Determine whether the impact on privacy is proportional to the anticipated outcomes.

Additional Comments:

Submitted to: [access and privacy representative]

Submitted by:

Date:

Appendix A

Definition of Personal (Health) Information under FIPPA and PHIA

Definition of Personal Information under FIPPA:

"personal information" means recorded information about an identifiable individual, including

(a) the individual's name,
(b) the individual's home address, or home telephone, facsimile or e-mail number,
(c) information about the individual's age, sex, sexual orientation, marital or family status,
(d) information about the individual's ancestry, race, colour, nationality, or national or ethnic origin,
(e) information about the individual's religion or creed, or religious belief, association or activity,
(f) personal health information about the individual *,
(g) the individual's blood type, fingerprints or other hereditary characteristics*,
(h) information about the individual's political belief, association or activity,
(i) information about the individual's education, employment or occupation, or educational, employment or occupational history,
(j) information about the individual's source of income or financial circumstances, activities or history,
(k) information about the individual's criminal history, including regulatory offences,
(l) the individual's own personal views or opinions, except if they are about another person,
(m) the views or opinions expressed about the individual by another person, and
(n) an identifying number, symbol or other particular assigned to the individual

The Freedom of Information and Protection of Privacy Act (FIPPA) can be reviewed online:
http://web2.gov.mb.ca/laws/statutes/ccsm/f175e.php

* The privacy requirements of PHIA applies to this information.

Definition of Personal Health Information under PHIA:

"personal health information" means recorded information about an identifiable individual that relates to

(a) the individual's health, or health care history, including genetic information about the individual,
(b) the provision of health care to the individual, or
(c) payment for health care provided to the individual, and includes
(d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and
(e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care

The Personal Health Information Act (PHIA) can be reviewed online:
http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php

Appendix B

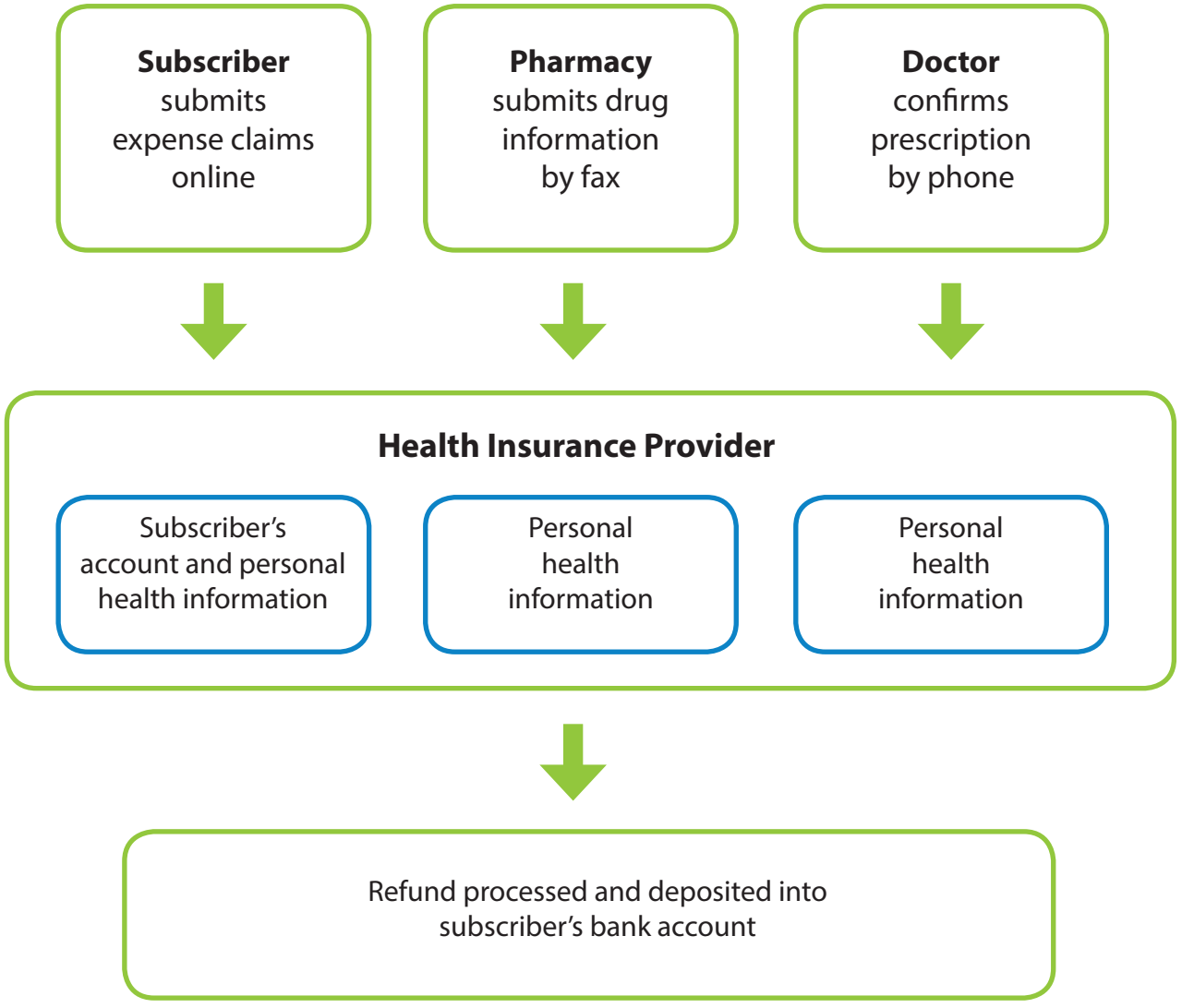
Example of Data Flow Chart

The key to an effective information flow chart is to break down your initiative into its most basic parts. Explain the way information moves through your initiative as if you were explaining it to someone who doesn't work for the organization and isn't familiar with what you do.

Focus should be given to when you are either collecting information from someone/somewhere, whenever you are using the personal (health) information within your organization and when you are disclosing or sharing information with someone/somewhere else.

In your flow chart or diagram, you should also describe when your initiative uses personal (health) information that has been collected or is already in your possession.

Example
Data Flow Chart for Claiming Health Expenses



Appendix C

Collection, Use, Disclosure
Personal (Health) Information Inventory –
University Admission Process Example

COLLECTION			
Category	**Types**	**Source**	**Purpose**
Contact Information	Name Address Telephone number Email address	Individual	To maintain contact with the individual regarding the status of their application
Educational Information	Levels of schooling completed Previous connection with university	Individual	To determine eligibility for program To determine previous connection with university To reinstate previous student file
Employment or Occupational Information	Member of the Canadian Forces	Individual	For research and analysis purposes
Personal Health Information	Immunization records	Individual or Physician's Office	Required for admissions to programs including Faculty of Dentistry

USE		
Category	**Types**	**Uses of the personal (health) information within the university and why**
Contact Information	Name Address Telephone number Email address	Provided to faculties and programs so they may proceed with the admissions process
Educational Information	Levels of schooling completed	Provided to faculties and programs so they may proceed with the admissions process
Employment or Occupational Information	Member of the Canadian Forces	Provided to central administration in the form of statistical reporting on an annual basis to analyze university admissions (data is de-identified)

DISCLOSURE			
Category	**Types**	**To Whom and the Purpose**	**Method of Transfer**
Contact Information	Name Address Telephone number Email address	Provided to the Alumni Association to maintain a lifelong relationship with the student	Annual disclosure – data transfer

Appendix D

Categories of Personal Information

Under FIPPA, any information about an identifiable individual is considered to be personal information, except when the information is personal health information to which PHIA applies. For the purpose of the *Privacy Impact Assessment Tool*, the definition of personal information under FIPPA has been broken down into the following categories. Examples of the types of personal information have been provided for each category.

Contact information: name, address, telephone number, fax number, email address

Individual information: age, gender, marital status, family status, sexual orientation, ancestry, race, skin colour, nationality, national origin, ethnic origin, citizenship

Unique personal identifiers: SIN (social insurance number), driver's license number, birth certification number, passport number, treaty number, student number, signature, fingerprint

Education information: education level, educational history

Employment or occupational information: current employment, employment history, occupational history

Financial information: salary, source of income, credit history, credit card details, bank account details, purchase transactions, financial activities

Religious information: religious beliefs, activities, association

Political information: political beliefs, activities, association

Legal information: record of criminal convictions, sentencing information, probation, criminal checks

Opinions: an individual's own personal views or opinions, view of opinions expressed about the individual by someone else

Other (potentially) identifying information: any other recorded information about an identifiable individual, including information that could potentially identify an individual if combined with other available information

Categories of Personal Health Information

Under PHIA, personal health information includes specific types of information about an identifiable individual. Personal information, such as contact information about an individual, is considered personal health information when collected in the course of health care. For the purpose of the *Privacy Impact Assessment Tool*, the definition of personal health information under PHIA has been broken down into the following categories. Examples of the types of personal health information have been provided for each category.

Demographic information: an individual's name, address, telephone number and email address

Health or health care history: medical background, patient notes, lab results, x-rays, medical diagnosis, blood type, prescriptions, health information related to employment or occupation, genetic information

Unique personal identifiers: PHIN (personal health identification number), patient file number, fingerprint

Financial information: health-care receipts, payment information, billing information

Other (potentially) identifying information: any other recorded information about an identifiable individual collected in the provision or payment of health care, including information that could potentially identify an individual if combined with other available information