PRIVACY IMPACT ASSESSMENT (PIA) GUIDE

FOR USE WITH
PRIVACY IMPACT ASSESSMENT (PIA) TOOL

Introduction
(Refer to Section 1.0 in the PIA Tool)

What is a PIA?

A Privacy Impact Assessment is a risk management process in which potential risks to the privacy of personal information and/or personal health information are identified and compliance with applicable legislation is assessed.

When is a PIA required?

- **SOUTHERN HEALTH-SANTÉ SUD policy**

  Southern Health-Santé Sud Policy ORG.1411.PL.301 requires that a PIA be conducted:

  - in conjunction with the initiation, planning, development and implementation of a new electronic information system, including but not restricted to databases developed in Access, Excel, etc..
  - prior to implementing modifications to an existing electronic information system that may contain personal health information and/or personal information.
  - on electronic information record system initiatives for which Manitoba Health is the trustee, and on electronic information system initiatives for which Manitoba Health is a partner.

- **Good business practices**

  Conducting a PIA is a sound business practice. Protecting the privacy and security of personal information and/or personal health information engenders trust and contributes to a positive business reputation.

Who does a PIA?

Most PIAs are conducted in the context of a project and the responsibility for it will be assigned by the Project Manager. Although one person will have the responsibility, he or she will need input from a variety of different people involved in the project. Examples are: representatives from the business that will have responsibility for the system at the end of the project, technical experts, security advisors and privacy advisors.

When should a PIA be started?

- **Conceptual PIA**

  A PIA ***can*** be done when the concept for the project has been developed but before any firm requirements have been set. This is referred to as a 'conceptual PIA'. The purpose is to establish a general understanding of what the initiative intends to do and to identify privacy and security risks at the conceptual stage before any final decisions have been made as to the specific design of the technical

solution. The findings from a conceptual PIA can inform the project mandate as well as the technical design.

- **Logical PIA**

  Generally speaking, the best stage to do a logical PIA is after all business requirements and major features of the project have been determined in principle, but before completing detailed design or development work to implement those requirements and features. One of the benefits of getting involved at this stage is the ability to attempt to influence project design from a privacy perspective.

  A PIA ***should*** be started once the design of the solution is generally established and the required personal information and/or personal health information has been determined. Starting the PIA process does not have to wait until all decisions have been made. A PIA can be started once:

  ☐ the project mandate is clear,
  - There is no point in attempting to do a PIA until you know the extent of the project mandate and understand the project outcomes.

  ☐ the nature and extent of the information to be collected in the solution is known, **and**
  - you need to know how all the information fits into your project and understand how the data elements will be collected, used and disclosed.

  ☐ the technical design has been determined.

  Some examples of privacy design elements that could be considered at this stage are:

  - Access controls to enforce the need to know principle (Strong User Roles within the system).
  - Mechanisms to produce the Record of User Activity as required by PHIA
  - Ability to limit access to health information at an individual's request (e.g. Disclosure Directives or Masking)
  - Encrypting health information transmitted over public networks or stored on mobile devices.
  - Commitment to conduct audits of the system on a regular basis at a minimum of every two years.

  This means the PIA is best positioned after the completion of overall project definition but before the project is executed. Within these general parameters, the timing of the PIA will depend on factors specific to your project.

The PIA should be completed, reviewed and, where possible, signed off before the project go-live date

Who Has to Review the PIA?

Once the PIA has been completed it must be submitted for review in accordance with the applicable trustee/public body practice.

Specific information on trustee/public body practices can be detailed in this section

Who has to Sign-off?

There can be different levels of sign-off. Signing off is evidence of accepting accountability for having carried out the due diligence. The organization is responsible for the level of sign off required.

Where does the signed PIA go?

This will vary according to the practice of the trustee/public body. It is the business owner's responsibility to maintain the signed PIA and the number of copies should be kept to a minimum.

When should a PIA be reviewed and revised?

New practices and technologies evolve after projects are implemented. New threats to privacy may also develop over time. The PIA should be periodically reviewed to identify any additional risks resulting from these changes.

The following events are examples of triggers for a PIA revision to be reviewed, and, if necessary, revised:

- Relevant legislation (eg. PHIA, FIPPA or the Regulations) is amended
- There is a significant upgrade to the system planned
- There is collection of new or expanded personal information and/or personal health information
- There is a new category of user who will be given access to the system
- The system will be deployed to a new site, program or to another trustee

Depending on the anticipated effect of these events on the system it may be possible to amend the original PIA by preparing an addendum to it that clearly indicates the changes and their impact on the privacy of the information. For a major upgrade that adds new functionality to the system, a completely new PIA may be required. Contact your Privacy Office to discuss what approach to take.

Terminology - In this Guide and the PIA Tool,
"System" refers to an Electronic Information System or Application.

This guide is for use with the accompanying PIA Tool.
The PIA Tool provides references to the applicable sections in this guide.

PIA TOOL

A. TITLE PAGE

The Title or Cover Page provides basic information relevant to the PIA and contact information for people involved in the PIA process. It should include:

- The project name
- The name of the system, or module (refers to the portion of the system to be implemented)
- Expected implementation date ("go-live")
- The trustee of the system
- The vendor (if applicable) – this should be the person who would have authority to sign an IMA if the vendor is going to be providing ongoing support services.
- The location of the server(s) – e.g. Primary Data Centre (do not include specific address location)
- The site(s)/program(s) in which the system will be implemented at go-live
- Future implementation site(s)/program(s) (if applicable)
- The name, title and contact information of the person responsible for completing the PIA
- The name, title and contact information of the Business Owner(s)
- The name, title, and contact information of the Application Administrator (or other individual tasked with ongoing system maintenance)

1.0 PROJECT SUMMARY

Provide a full description of the proposed project, including its objectives. State why the system must collect, use and/or disclose personal information and personal health information.

Your overview should answer some basic questions about the project that triggered the PIA. For example:

1. What is the business rationale for the project (i.e. what problem are you trying to solve)?
2. Why does personal information and personal health information need to be collected, used or disclosed?
3. Where will the information be stored?
4. How will the information flow within the system? A high level diagram must be included with the PIA submission and should include any interfaces with other systems (See Section 2.0 below).
5. Who will have access to the information?
6. Where will the system be deployed?

This information is usually included in the Project Initiation Documentation. Consult with the Project Manager if necessary.

2.0 Information Flow Analysis

(Refer to Section 2.0 in the PIA

This part of the PIA has two components:

1. A Data Element Table; and
2. An Information Flow Diagram

COMPONENT #1 - Data Element Table (APPENDIX 1)

Both *The Personal Health Information Act* (PHIA) and *The Freedom of Information and Protection of Privacy Act* (FIPPA) set out specific and limited purposes for the collection, use and disclosure of personal health information and personal information respectively. Both Acts require that only the minimum amount of information reasonably necessary to accomplish the purpose be collected, used or disclosed.

The Data Element Table is a detailed description of all data elements that will be contained in the system. This table forms the basis for determining if the system contains personal information or personal health information; it helps to assess whether only those data elements necessary to achieve the purpose of the system are to be collected, used and disclosed (minimum amount).

The Data Element Table may contain the following:

1. A listing of the data elements contained in the system;
2. A definition of each data element;
3. An explanation of the purpose for which the data element is collected;
4. Identification of those data elements that are disclosed from the system (e.g. reports generated by system and disclosed, auto faxing, interface with another system, etc.); and
5. A description of the information source for the data elements. (e.g. the individual the information is about, interface with another system, etc.)

COMPONENT #2 - Information Flow Diagram (Appendix 2)

An information flow diagram follows the information from its collection, to its use and its disclosure.

There is no universally accepted format for information flow diagrams, but work flow diagrams, technical data flow diagrams, such as those prepared during the design of computer applications, or network diagrams, are not likely appropriate for PIA purposes. The example given provides one approach to health information flow diagrams; you may use another method if it makes sense for your project.

Information Flow Diagram Examples

Appendix 2 is an example of an information flow diagram for a project proposed by Hospital ABC. This project will:

- collect health information from three different sources:
  - the individual the information is about, the individual's Family Physician, and an external lab
- use this information to make health care decisions
- give results and feedback to the individual for on-going care
- send health information to the hospital's database server
- send health information to an information manager

3. Collection
(Refer to Section 3.0 in the PIA Tool)

A. Type and Extent of Information Collected

Refer to the Data Element Table (Appendix 2)

3.1 In making a determination as to the "type of information", ***it is important:***

- ***To remember,*** when the data elements contain personal **health** information, the provisions under PHIA apply.
- When the data elements contain personal information, the provisions under FIPPA may apply (see the box below).
- ***To use*** PHIA and FIPPA as primary reference sources.
- ***To consult*** with PHIA and FIPPA experts if there is any uncertainty in determining whether the data elements contain personal health information and/or personal information.

FIPPA only applies to public bodies; health care facilities such as private medical clinics are not public bodies and therefore are not subject to FIPPA.

B. Information Source and Authority

Identification of the source or sources of the information is required, and as applicable, identification of the authority. The Information Flow Diagram and the Data Element Table will provide this information.

The Acts (PHIA Section 14 and FIPPA Section 37) authorize collection of the information:

- directly from the individual.
- indirectly, where the individual the information is about has consented.
- indirectly, without consent, in accordance with authorities under the applicable Act. If selected, please ensure the **authority** is specified.

From the choices provided in the PIA tool, please select **all** sources that apply.

4. Use
(Refer to Section 4.0 in the PIA Tool)

USE refers to handling, dealing with, applying or reproducing the information **within** the trustee's organization.

When completing this section, it is necessary to identify all intended uses for the information in the system **AND** indicate how each intended use complies with the authorities outlined in the applicable Act.

Section 21 of PHIA sets out the authority for use of personal health information. (Refer to Section 4.0 in the Tool).

Section 43 of FIPPA sets out the authority for the use of personal information. (Refer to Section 4.0 in the Tool).

Section 45 of FIPPA explains consistent purposes:

Consistent purposes

45 For the purpose of clauses 43(a) and 44(1)(a), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure

(a) has a reasonable and direct connection to that purpose; and

(b) is necessary for performing the statutory duties of, or for delivering an authorized service or program or carrying out an activity of, the public body that uses or discloses the information.

Note:

In the PIA Tool:

- Boxes 4.6, 4.7 and 4.8 are only applicable if the information being used is demographic information which is defined in subsection 1(1) of PHIA to be an individual's name, address, telephone number and email address.
- Box 4.8 only applies if the trustee does its own debt collection.
- Boxes 4.9 and 4.10 are only applicable if the trustee is a public body or a health care facility.

5. Disclosure

(Refer to Section 5.0 in the PIA Tool)

DISCLOSURE refers to sharing information **outside** the trustee organization by any means e.g. faxing, mailing, electronically.

Section 22 of PHIA sets out the authority for disclosing personal health information.

Sections 43 and 45 of FIPPA set out the authority for disclosing personal information.

When completing this section, it is necessary to identify the authority for all intended disclosures identified in the data element table (Appendix 1).

You must consider all possible disclosures, including any extra-provincial disclosures.

For example:

A. If your system is being supported by a vendor located outside of Manitoba:
   - personal health information may be viewed from outside the province during help desk calls where you allow remote access ("over the shoulder");
   - it is a disclosure if the vendor is performing backup or archiving of the information and maintaining the backup and/or archive in its own jurisdiction.

B. Your system sends personal health information and/or personal information to another jurisdiction

6. Requirement Compliance
(Refer to Section 6.0 in the PIA

In completing section 6.0 of the PIA Tool;

- **Consider policies, procedures, guidelines, forms etc. as examples of supporting documents referred to in the tables in the Tool;**
- **For any requirement where the "NO" or "N/A" box is ticked, an explanation must be provided and the risks that arise must be identified and documented**.

A. Personal Notification and Access

A1 Method to inform individuals about why the information is collected and about their rights to access the information. PHIA subsection 15(1) and Section 9.1

PHIA requires that Trustees notify individuals about why they are collecting their information and of their right to access their information. The Act sets out the minimum requirements these notifications **must** include:

1. Notice of Right to Access Information: (PHIA Section 9.1)
   - Trustees must take reasonable steps to inform individuals of their right to examine and receive a copy of their personal health information the trustee maintains; and
   - How the individual can exercise that right.

   PHIA Regulation Section 1.4 the notification can be in the form of a sign, poster, brochure or other similar type of notice to inform individuals and the notice **must**:

   - Set out the information clearly in a manner that the individual can reasonably be expected to understand;
   - State that the individual has a right to examine and receive a copy of his or her personal health information; and
   - State that the individual has a right to authorize another person to examine and receive a copy of the information.

2. Notice of collection practices: (PHIA Section 15)
   - This notice must inform individuals about the purpose for which their information is being collected; and
   - How to contact someone within the trustee who can answer any questions about the collection.

   These two notices may be combined into one notice and may contain other information about the trustees collection, practices and procedures relating to personal health information.

A copy of the notice, poster, brochure etc., should be attached to the PIA Tool.

A2 Method that provides individuals with access to their own records contained in the system (e.g. printed copy).

PHIA Section 5 gives individuals the right to examine and if requested receive a copy of their personal health information.

Right to examine and copy information
5(1) Subject to this Act, an individual has a right, on request, to examine and receive a copy of his or her personal health information maintained by a trustee.

Describe how the individual can exercise this right of access.

PHIA Section 60 allows other persons to exercise the rights of the individual.

Exercising rights of another person
60(1) The rights of an individual under this Act may be exercised

(a) by any person with written authorization from the individual to act on the individual's behalf;

(b) by a proxy appointed by the individual under *The Health Care Directives Act*;

(c) by a committee appointed for the individual under *The Mental Health Act* if the committee has the power to make health care decisions on the individual's behalf;

(d) by a substitute decision maker for personal care appointed for the individual under *The Vulnerable Persons Living with a Mental Disability Act* if the exercise of the right relates to the powers and duties of the substitute decision maker;

(e) by the parent or guardian of an individual who is a minor, if the minor does not have the capacity to make health care decisions; or

(f) if the individual is deceased, by his or her personal representative.

If person unavailable
60(2) If the trustee reasonably believes that no person listed in subsection (1) exists or is available, the adult person listed first in the following clauses who is readily available and willing to act may exercise the rights of an individual who lacks the capacity to do so:

(a) the individual's spouse, or common-law partner, with whom the individual is cohabiting;

(b) a son or daughter;

(c) a parent, if the individual is an adult;

(d) a brother or sister;

(e) a person with whom the individual is known to have a close personal relationship;

(f) a grandparent;

(g) a grandchild;

(h) an aunt or uncle;

(i) a nephew or niece.

Ranking
60(3) The older or oldest of two or more relatives described in any clause of subsection (2) is to be preferred to another of those relatives.

Things to consider:

- Are individuals required to complete a form to make the request or can the request be made verbally?
- Describe how the individual is given access to his or her information. For example, is the information viewed at a computer or is it printed and then provided to the individual? Does an employee review the information with the individual?
- Is there a fee for permitting an individual to examine their phi and to receive a copy?
- If the individual examines their information, how and where is the access documented in the system?
- Is there the ability to capture information on those persons entitled under Section 60 of PHIA to exercise the right of the individual?
- Is there a mechanism to verify the authority of another person to exercise the rights of the individual?

A3 Method to provide individuals with the ability to request corrections to their own records, and how a statement of disagreement is managed if the requested corrections are not made.

PHIA Section 12 gives individuals the right to request a correction to their personal health information and to file a statement of disagreement if the requested corrections are not made. The request must be in writing.

Describe the method used to make the change or to file the statement of disagreement.

Things to consider:

- How are individuals informed that they have a right to request corrections? E.g. a poster, brochure
- What method is used to process and record a request from an individual to have information changed? For example, is the individual required to complete a form detailing the requested change or the statement of disagreement? Attach a copy of the form.

A4 Method to notify any other public body or third party to whom the records have been disclosed, in the preceding 12 months, of corrections being made or a statement of disagreement filed.

PHIA Section 12 requires the trustee to, when practicable*; notify any other trustee or person who has received the information, of a correction or statement of disagreement.

***"Practicable"** means capable of being done (Encarta dictionary)

Describe the method to inform others outside the organization of a correction to personal health information or a statement of disagreement filed by the individual

B. INFORMATION ACCURACY AND INTEGRITY

B1 Method to ensure the information in the system is accurate, up to date, complete and not misleading prior to use or disclosure.

PHIA Section 16 requires a trustee to ensure that information is accurate, up to date, complete and not misleading:

> **Duty to ensure accuracy of information**
> 16 Before using or disclosing personal health information, a trustee shall take reasonable steps to ensure that the information is accurate, up to date, complete and not misleading.

Things to consider

- Describe the business and/or technical processes to ensure information accuracy and integrity. For example:
  - does the system prevent accuracy errors?
  - does the organization confirm demographic information with the individual?
  - does the system log changes to the personal health information?

C. DISCLOSURE

C1 Method to ensure an individual's instruction not to disclose their information is recorded.

An individual can instruct a trustee not to disclose their personal health information under clause 22(2)(a) of PHIA:

Disclosure without individual's consent

22(2) A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is

(a) to a person who is or will be providing or has provided health care to the individual, to the extent necessary to provide health care to the individual, unless the individual has instructed the trustee not to make the disclosure;

Things to consider

- If an individual makes a request under clause 22(2)(a) how is the request managed in the system? For example, can the system hide/mask the information, can it flag the information?
- How is the request communicated to other users of the system?
- Is there an ability to override any mask or flag? If so, under what circumstance:
    - by whom,
    - is there an alert triggered?
    - Are all overrides audited?

C2 There is a written ***Agreement*** between the trustee and an Information Manager in accordance with the requirements of the *Act.*

Personal health information can be disclosed to an Information Manager. Information Managers provide information management or information technology services and may process, store and/or destroy personal health information.

Examples of an Information Manager are: A third Party billing agency, a Vendor or other person providing system support, a business that provides off-site storage or document destruction, a transcription service.

Disclosure without individual's consent

22(2) A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is

(f) in accordance with section 25 (disclosure to an information manager);

Trustee may provide information to an information manager

25(1) A trustee may provide personal health information to an information manager for the purpose of processing, storing or destroying it or providing the trustee with information management or information technology services.

Restrictions on use

25(2) An information manager may use personal health information provided to it under this section only for the purposes and activities mentioned in subsection (1), which must be purposes and activities that the trustee itself may undertake.

Agreement required

25(3) A trustee who wishes to provide personal health information to an information manager under this section must enter into a written agreement with the information manager that provides for the protection of the personal health information against such risks as unauthorized access, use, disclosure, destruction or alteration, in accordance with the regulations.

Information manager must comply with Act

25(4) An information manager shall comply with

(a) the same requirements concerning the protection, retention and destruction of personal health information that the trustee is required to comply with under this Act; and

(b) the duties imposed on the information manager under the agreement entered into under subsection (3).

Information deemed to be maintained by the trustee

25(5) Personal health information that has been provided to an information manager under an agreement described in subsection (3) is deemed to be maintained by the trustee for the purposes of this Act.

There is no need to attach a copy of the Agreement to the PIA, however a notation should be included that the agreement has been entered into, signed by both parties and where the document is maintained.

Things to consider

- Do you use third party providers to support your systems (hardware or software)? Do you have Agreements in place with them?
- Do you use a third party billing company? Do you have an Agreement in place with this company?
- Name any other companies that have access to your systems and indicate whether or not you have an Agreement in place with them.

D. AUDIT OF USER ACTIVITY

D1 Ability to create and maintain a record of user activity.

The Personal Health Information Regulation requires that an electronic system be able to create and maintain a "record of user activity".

> **"record of user activity"** means a record about access to personal health information maintained on an electronic information system, which identifies the following:
>
> (a) individuals whose personal health information has been accessed,
>
> (b) persons who accessed personal health information,
>
> (c) when personal health information was accessed,
>
> (d) the electronic information system or component of the system in which personal health information was accessed,
>
> (e) whether personal health information that has been accessed is subsequently disclosed under section 22 of the Act;

Additional safeguards for electronic health information systems

4(1) In accordance with guidelines set by the minister, a trustee shall create and maintain, or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information.

4(2) A record of user activity may be generated manually or electronically.

4(3) In the following circumstances, a record of user activity is not required under this section:

(a) if personal health information is demographic or eligibility information listed in Appendix B, or is information that qualifies or further describes information listed in Appendix B;

(b) if personal health information is disclosed under the authority of clause 22(2)(h) of the Act (disclosure to a computerized health information network) in a routine and documented transmission from one electronic information system to another;

(c) if personal health information is accessed or disclosed while a trustee is generating, distributing or receiving a statistical report, as long as the trustee

(i) maintains a record of the persons authorized to generate, distribute and receive such reports, and

(ii) regularly reviews the authorizations.

Things to consider

- Can the system produce a record of user activity by user and by patient? Please provide a copy ensuring that any personal health information is severed.
- Does the system fall within any of the exceptions set out in subsection 4(3)? If so, describe.

Include a de-identified copy of a Record of User Activity.

D2 There is an organizational audit plan.

There is no express requirement for an audit plan in PHIA or the Regulation. However there is an obligation on the trustee to audit the record of user activity to detect security breaches and there are additional requirements set out in the guideline set by the Minister dated November 21, 2008.

Personal Health Information Regulation

Additional safeguards for electronic health information systems
4(4) A trustee shall audit records of user activity to detect security breaches, in accordance with guidelines set by the minister.

4(5) A trustee shall maintain a record of user activity for at least three years.

4(6) A trustee shall ensure that at least one audit of a record of user activity is conducted before the record is destroyed.

Note: There are Ministerial Guidelines with respect to auditing the record of user activity. Please refer to Guidelines for Records of User Activity (RoUA). The Guidelines are attached as Appendix 5.

Things to consider

- Does the organization have a documented audit plan in place to regularly review the record of user activity to determine whether there has been any unauthorized activity?
- Does the plan designate someone as responsible for reviewing the record of user activity?
- Does the plan describe things to look for when reviewing the record of user activity (e.g. a user looking up their own personal health information; that of relative or other employees they work with/)
- Provide a copy of the documented audit plan.

Include a copy of your organizational audit plan.

D3 Access to the audit logs is restricted to a limited number of persons who require this access to do their job.

The audit logs contain personal health information and must be protected from unauthorized access and from alteration. Access to the logs must be based on the need to know principle.

E. SECURITY SAFEGUARDS

E1 Access Control

A method for:

a. establishing who is authorized to access the system (need to know principle), what level of access is required (e.g. demographics only, medications only – minimum amount principle) and what permissions are granted. (e.g. read only, add, change, update, modify)
b. managing user accounts that includes provisioning, modifying and de-provisioning
c. controlling access by users and vendors

The Personal Health Information Act requires the following:

Duty to adopt security safeguards

18(1) In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.

Specific safeguards

18(2) Without limiting subsection (1), a trustee shall

(a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so;

(b) implement controls to ensure that personal health information maintained by the trustee cannot be used unless

(i) the identity of the person seeking to use the information is verified as a person the trustee has authorized to use it, and

Limit on the trustee's employees

20(3) A trustee shall limit the use of personal health information it maintains to those of its employees and agents who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 21.

The Personal Health Information Act Regulation requires the following:

Authorized access for employees and agents

5 A trustee shall, for each of its employees and agents, determine the personal health information that he or she is authorized to access.

PHIA Sub-section 20(3) requires the trustee to limit the amount of personal health information its employees and agents have access based on the "need-to-know" principle. Personal health information should only be accessible to those who have a business need and who have been properly authorized. It is important that you describe the user access roles, the type of access and the form of access.

Create a user access role table based on the following example to provide this information. The table below is for illustration only; you may need to adjust it to provide room for your responses, or provide a table that contains the necessary information.

Example Table:

Role Name	User Title	Functionality Assigned to User			
		Read/View	**Add**	**Delete**	**Modify**
User Level I	Booking Clerk Intake Coordinator	X	X	X	X
User Level II	Nursing	X	X		
User Level III	Physicians	X			
App Admin	App Administrator	X	X	X	X

Things to consider

Account Management

- Does the user account provisioning process include:
  - formal approval by an authorized person?
  - verification of user role?
  - maintenance of records of access privileges (which systems, level of access in each system and permissions for each system)?
  - auditing of inactive user accounts?
- Is each user of a system that processes personal information uniquely identified?
- When assigning a unique identifier for users, does the organization ensure the proper identification of the individual to whom the identifier is being issued, before giving the user access to the system?
- Is there record of who approved a user account?
- Is a current, accurate inventory of user accounts maintained and is it reviewed on a regular basis to identify dormant, fictitious or unused accounts?
- Is there a documented process for de-provisioning user accounts?

User Access

- Are there password requirements set out in a policy or a standard? (e.g. passwords must be a certain number of characters and numbers, certain number of days when passwords expire, 3 attempted logins before the system locks out the user).
- Are passwords known only to the authorized user of the account?
- Are the users instructed to lock their screen before they walk away from their computer or log out at the end of their day?

Vendor Access

- Is there a managed process for allowing vendors to access the system? (e.g. requires the system owner to confirm that the vendor needs access to the system, puts a limit on the timeframe in which the vendor can access the system, identity of the vendors users who will be accessing the system, audit of the record of user activity)

Attach any supporting documents.

E2 Notification to Users

The system notifies users of the sensitivity/confidential nature of the records and their responsibilities for safeguarding the records (e.g. "splash screen" or similar method).

Things to consider

- What mechanisms does your organization have in place to alert staff of the sensitivity of the information they are working with and their responsibilities for safeguarding the information? For example, does the login page display a message reminding staff of the confidential nature of the information they are about to access?
- Are users required to accept "terms of use" before they can access the system for the first time?

E3 Safeguards

There are reasonable administrative, technical and physical safeguards in place that ensure the confidentiality, security, accuracy and integrity of the information maintained in the system.

The Personal Health Information Act requires the following:

Duty to adopt security safeguards

18(1) In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.

Things to consider

Administrative Safeguards

- Does your organization have an IT security policy?
- Are staff trained on the policy?
- Have users with access to the system signed a Pledge of Confidentiality?
- Are users required to sign or accept (electronically) Terms of Use for the system?
- Is there an inventory list of all computer assets and other items that can hold information (e.g. Computers, laptops, smartphones, USB keys, CD's, portable hard drives, fobs, door keys, swipe cards)

Technical Safeguards

- How is personal health information protected during transmission (e.g. Email) and at rest?
- What technical safeguards prevent unauthorized access to the system?
- Is there a forced log out after a period of inactivity?
- Is there a mechanism to monitor all successful and unsuccessful attempts to access the system?

Physical Safeguards

- Are computer screens placed so they are not visible to the public or authorized persons?
- Will servers be located in secure, climate controlled locations?

Where information is going to be stored off site eg: with the Vendor or in a "Cloud" environment, there are special security considerations. Consultation should be undertaken with organizational information technology, security, legal and privacy experts.

E4 Threat Risk Assessment (TRA)

A TRA is a process for identifying threats and risks to information assets (e.g. personal information, personal health information and confidential business information). It looks at the impact of threats and risks on the confidentiality, integrity and availability of the information.

There is no requirement in PHIA or the Regulation to have a Threat Risk Assessment completed. However for systems that contain or will contain large amounts of personal health information or that have multiple connections to other systems a TRA should be considered.

The TRA will identify Security Risks. Privacy Risks are dealt with in Section 7.

E5 Portable Electronic Devices and Removable Electronic Storage Media

Portable Electronic devices can include but are not limited to laptops, Blackberries, Smartphones or Tablets used to access information maintained in the system. Removable electronic storage media can include but are not limited to USB Keys, external hard drives and writable CD/DVD's used to store and transport information.

PHIA requires that the Trustee take reasonable safeguards to protect personal health information. The Personal Health Information Regulation references removable electronic storage media and requires that policies address appropriate security for such devices.

The Personal Health Information Regulation requires the following:

Written security policy and procedures

2 A trustee shall establish and comply with a written policy and procedures containing the following:

> (a) provisions for the security of personal health information during its collection, use, disclosure, storage, and destruction, including measures (i) to ensure the security of the personal health information when a record of the information is removed from a secure designated area, and
>
> > (ii) to ensure the security of personal health information in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose;

Things to consider

- Do you have a policy on properly securing portable electronic devices and removable electronic storage media (e.g. requiring a password and encryption if any personal information or personal health information is to be stored on such a device)?
- Do you have an asset list that includes portable electronic devices and removable electronic storage media that will be/may be used with this system?

E6 An Audit of Security Safeguards is conducted at least every two years.

The Personal Health Information Regulation requires the following:

AUDIT

8(1) A Trustee shall conduct an audit of its security safeguards at least every two years.

8(2) If an audit identifies deficiencies in the trustee's security safeguards, the trustee shall take steps to correct the deficiencies as soon as practicable.

Things to consider

- For a new system please provide a brief plan on the steps that would be taken to ensure this requirement is met.
- For an existing system, has an audit of security safeguards been done? If so, please provide a summary. If not, provide a brief plan on the steps that would be taken to ensure this requirement is met.

F. BREACH REPORTING AND MANAGEMENT

The Personal Health Information Regulation requires the following:

Written security policy and procedures

2 A trustee shall establish and comply with a written policy and procedures containing the following:

(a) provisions for the security of personal health information during its collection, use, disclosure, storage, and destruction, including measures

(i) to ensure the security of the personal health information when a record of the information is removed from a secure designated area, and

(ii) to ensure the security of personal health information in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose;

(b) provisions for the recording of security breaches;

(c) corrective procedures to address security breaches.

Additional safeguards for electronic health information systems

4(4) A trustee shall audit records of user activity to detect security breaches, in accordance with guidelines set by the minister.

Things to consider

- Is there a policy regarding reporting of privacy or security breaches?
- Is staff aware of the breach reporting policy?
- Does the policy include a process for managing and responding to a breach?
- Are vendors required to report all security incidents or breaches as part of their contractual requirements?

F1 There is an organizational policy and applicable procedures for reporting and management of breaches.

G. RETENTION AND DESTRUCTION

G1 There is a policy and applicable procedures respecting the retention and destruction of personal health information.

The Personal Health Information Act requires:

Retention and destruction policy

17(1) A trustee shall establish a written policy concerning the retention and destruction of personal health information and shall comply with that policy.

Compliance with regulations

17(2) A policy under subsection (1) must conform with any requirements of the regulations.

Method of destruction must protect privacy

17(3) In accordance with any requirements of the regulations, a trustee shall ensure that personal health information is destroyed in a manner that protects the privacy of the individual the information is about.

There is currently nothing in the Personal Health Information Regulation that sets further requirements for retention or destruction.

It is likely that the organization has a policy dealing with retention and destruction of paper records but it may need to be updated to address electronic records.

Things to consider

- Does the organization have a policy on retention and destruction of personal health information main maintained electronically?
- Does the system have the ability to destroy personal health information?
- Does the project address secure destruction of personal information and personal health information that may be stored on portable electronic devices, and removable electronic storage media used with this system?
- If personal health information in the system will be retained indefinitely, is there a process for archiving information once available space is used up?
- Is the archived information easily retrievable?

Include a copy of your organizational policy and procedures.

7. Identified Privacy Risks
(Refer to Section 7.0 in the PIA

Every project involving the collection, use or disclosure of personal health information has some privacy risk. The organization needs to identify risks and apply reasonable privacy protection measures. The response to this section should describe the measures being taken to address specific privacy risks associated with this project. Mitigation measures could include a combination of administrative, technical and/or physical measures taken to reduce privacy risks.

7.1 Specific privacy risks have been identified for this project

7.2 There is a process for transferring unresolved project privacy risks to the business owner on completion of the project

This is an example of a completed Appendix 4 – Risk Management Table. **You should consult with experts in risk management when completing the table.**

Description of the Risk	Mitigation Measures	Status	Resolution Timeline
1. Unauthorized access by user	• Working with the Vendor to define access roles to minimize unauthorized access. • System privacy and security training to include examples of appropriate /inappropriate access. • Implement an electronic Terms of Use requirement for first log on.	Complete In Progress In Progress	 Will be completed by go-live* Will be completed by go-live*
2. Unauthorized access by unauthorized person - no idle session time out	Application was configured for a 15 minutes idle session time out	Complete	Resolved
3. The application cannot produce a Record of User Activity	Vendor will make available in next version upgrade	In Progress	To be determined*

* Any risks that are not resolved prior to completion of the project must be formally transferred to the business owner.

The PIA will identify Privacy Risks. Security Risks are dealt with in the TRA (see Section 6.0, E4).

8. PIA Review and Revisions

8.1 There is a person or a position identified to maintain the PIA?

8.2 There is a plan to review and revise the PIA as necessary.

New practices and technologies evolve after projects are implemented. New threats to privacy may also develop over time. The PIA should be periodically reviewed to ensure any risks caused by these changes are mitigated.

The following events are examples or triggers for a PIA review and where necessary, revision:

- Amendments to relevant legislation (eg. PHIA, FIPPA or the Regulations)
- There is a significant upgrade required to the application
- There is collection of new or expanded personal information and/or personal health information
- There is a new category of user who will be given access to the system
- The application will be deployed to a new site, program or to another trustee

Depending on the anticipated effect of these events on the application it may be possible to amend the original PIA by preparing an addendum to it that clearly indicates the changes and their impact on the privacy of the information. For a major upgrade that adds new functionality to the system, a completely new PIA may be required.

Include a copy of the plan to review and revise the PIA.

9. Sign Off

(Refer to Section 9.0 in the PIA

There can be different levels of sign-off. Signing off is evidence of accepting accountability for having carried out the due diligence. The organization is responsible for the level of sign off they require. The following page is an example of a sign off section.

Example of Sign Off sheet

Completed by:

Name _____ _____

Signature **Date**

Position Title
Organization

Certified Complete and Accurate:

Name _____ _____

Signature **Date**

Position Title
(eg: Privacy Officer)
Organization

Reviewed by:

Name _____ _____
Position Title **Signature** **Date**
(eg: Site determined)
Organization

Approved by:

Name _____ _____
Position **Signature** **Date**
Organization

Accepted by:

_____ _____

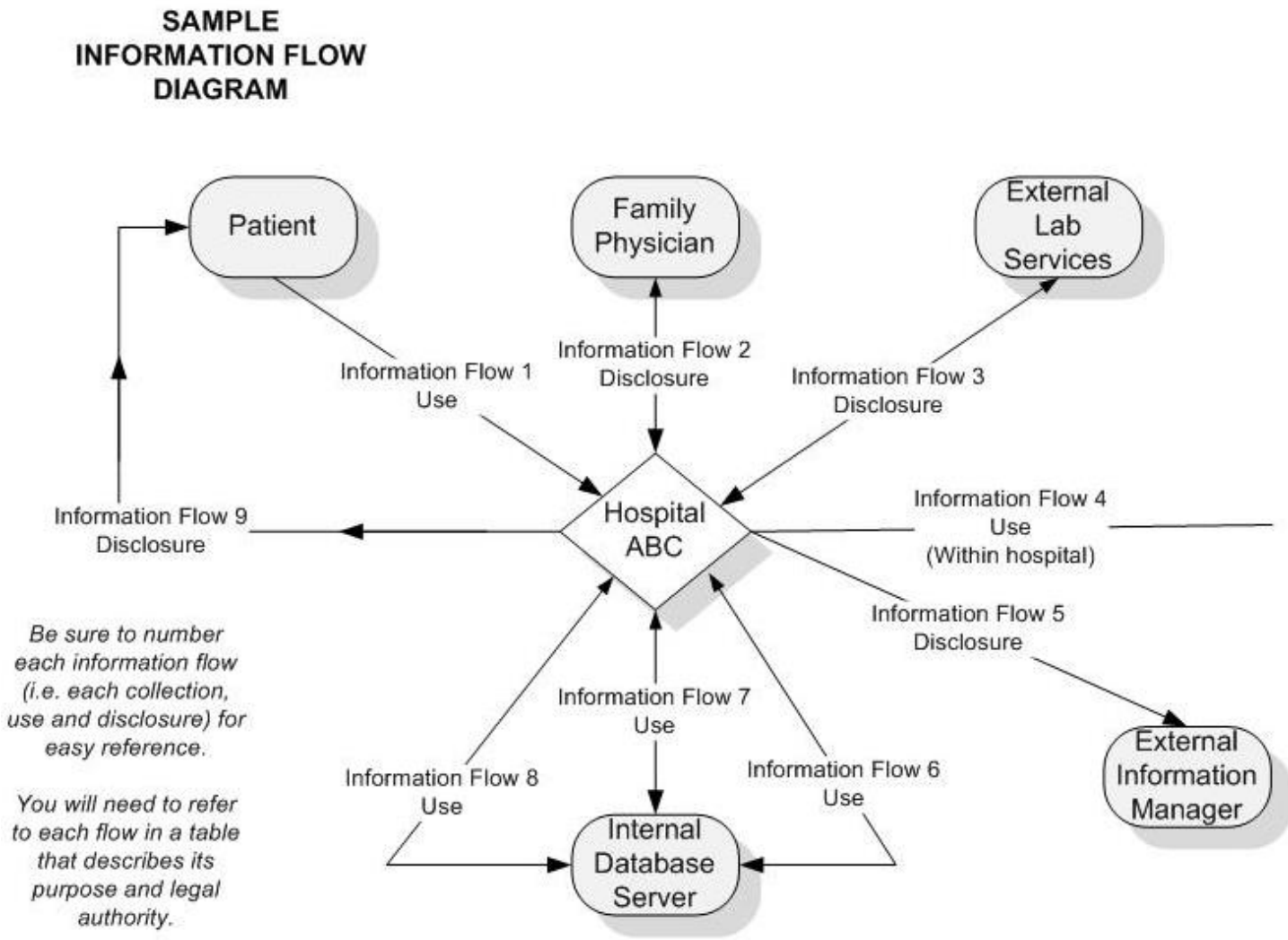
Name **Signature** **Date**
Position
Organization

Add Others as necessary

Appendix 1 – Data Element Table

Record (Data Element)	Definition	Rationale	Disclosed To (if applicable)	Information Source
Name	Name of Patient	Identify patient, Provide health care to patient	Patient's general practitioner, other jurisdiction (if patient from out of province)	Patient Referral Form Intake Form

Appendix 2 – Information Flow Diagram



LEGEND:

Information Flow	Type of Information	Method of Transmission
1	Demographic & personal health information	Direct from patient, entered into system
2	Treatment history	Two way electronic flow of information, system to system
3	Diagnostic information/results for treatment	Two way electronic flow of information, system to system
4	Personal health information	Direct care provider electronic entry and access
5	Data dictionaries, data tables	Electronic access by information manager
6	Personal health information	Electronic archiving, real time
7	Personal user information	Electronic access provisioning, real time
8	Personal user & activity information	Electronic system monitoring, real time
9	Personal health information care instructions	Direct to patient, verbally or via hard copy

Appendix 3 – User Roles (Refer to Section 6.0, B1 in the PIA Guide)

Role Name	User Title	Functionality Assigned to User			
		Read/View	Add	Delete	Modify

Appendix 4 – Issues / Follow-up Identification Sheet

Issues/Concerns	Legislation	Policy	Southern Health-Santé Sud Response	Update
Follow-up				

Appendix 5 – Ministerial Guidelines – Record of User Activity (RoUA).

Please see http://www.gov.mb.ca/health/phia/docs/gfroua.pdf for details.