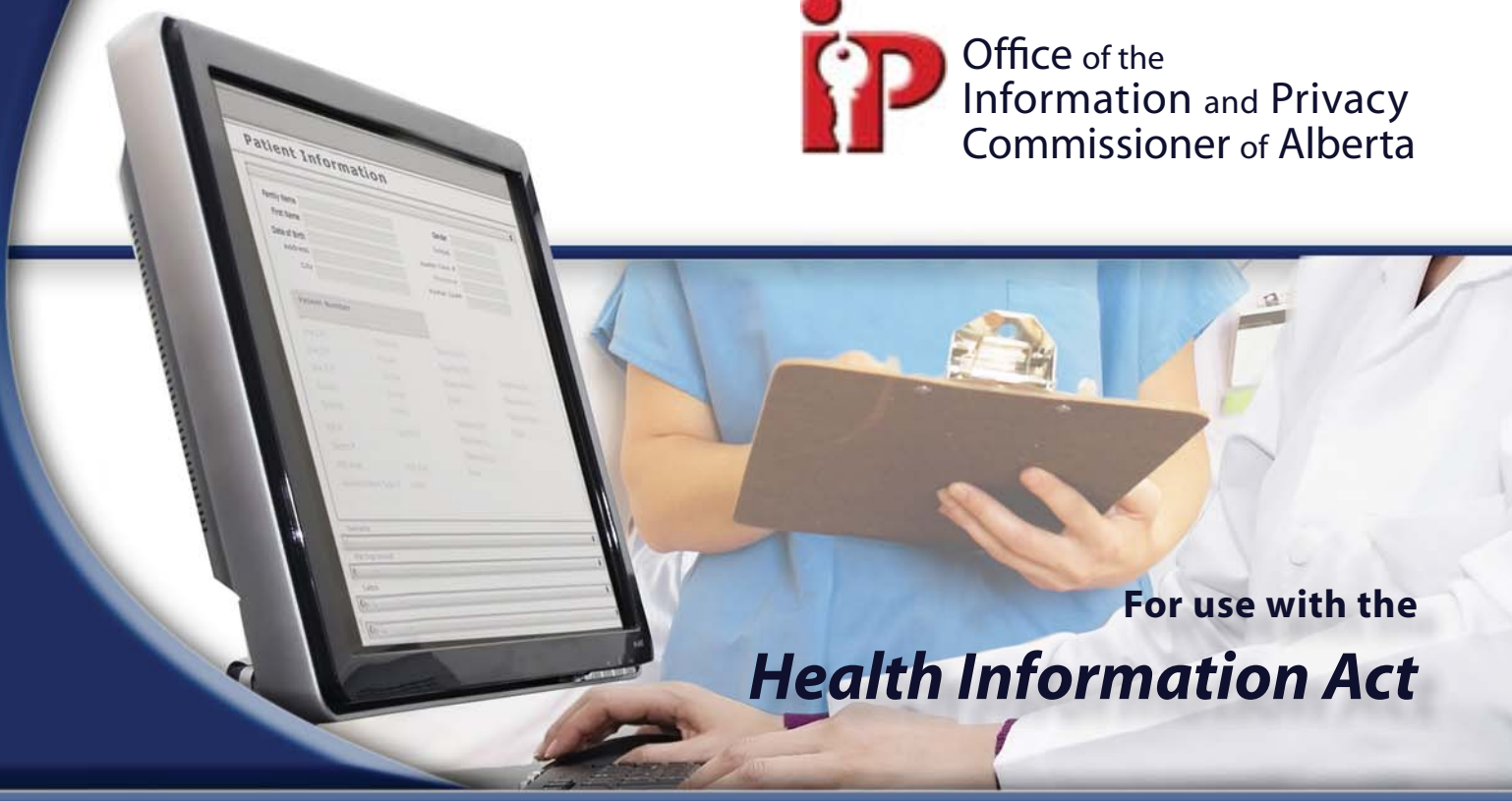
PRIVACY IMPACT ASSESSMENT REQUIREMENTS

Office of the Information and Privacy Commissioner of Alberta



For use with the

Health Information Act

Promoting a society where personal information is respected and public bodies are open and accountable

www.OIPC.ab.ca

Office of the
Information and Privacy
Commissioner of Alberta

410, 9925 - 109 Sreet
Edmonton, Alberta T5K 2J8
Phone: 780.422.6860
Fax:
780.422.5682

www.OIPC.ab.ca

CONTENTS

ABOUT the PRIVACY IMPACT ASSESSMENT (PIA) REQUIREMENTS

In 2001, the *Office of the Information and Privacy Commissioner* (OIPC) of Alberta introduced its first *Privacy Impact Assessment* (PIA) questionnaire. That questionnaire was used for more than eight years. During those eight years, the practice of conducting privacy impact asessments matured considerably and the volume of PIAs handled by the OIPC increased dramatically.

Privacy Impact Assessments (PIAs) are now commonplace, but those conducting them still ask for guidance to ensure their PIAs fully address privacy risks and describe reasonable risk mitigation measures. Further, the OIPC needs to efficiently review a large volume of PIAs under the *Health Information Act* (HIA) each year, making a consistent format with clear content guidelines even more important.

In January 2009, the OIPC decided to review and revise the OIPC PIA template and guidelines with the needs of the HIA as the main focus. This document is the result.

These requirements are mandatory for PIAs submitted under the *Health Information Act* (HIA). Organizations subject to the *Freedom of Information and Protection of Privacy Act* (FOIP) or the *Personal Information Protection Act* (PIPA) may also use these requirements as a reference tool to help draft PIAs. Please note, however, that all mention of legislation in these requirements refers to the HIA. Anyone using these requirements as guidelines to write a PIA under FOIP or PIPA will need to research these laws for proper legal authority to collect, use and disclose personal information.

Copies of these PIA Requirements, as well as links to other resources, are available from the OIPC website at **www.OIPC.ab.ca**.

You may also contact the OIPC by phone at **780-422-6860** or email at **generalinfo@oipc.ab.ca**.

The *Office of the Information and Privacy Commissioner* acknowledges the contribution of Excela Associates Inc**.** in helping to create these Guidelines.

THE PIA PROCESS

Throughout this document the term 'project' includes any term that refers to an initiative, program practice, scheme, plan, or endeavor for which a PIA may be appropriate.

The *Office of the Information and Privacy Commissioner* (OIPC) has developed these Privacy Impact Assessment (PIA) Requirements to help you review the impact a project may have on individual privacy. The process is also designed to ensure that you assess your project's compliance with relevant legislation.

The PIA is a due diligence exercise, in which you identify and address potential privacy risks that may occur in the course of your operations. The PIA process requires a thorough analysis of potential impacts to privacy and a consideration of reasonable measures to mitigate these impacts.

While PIAs are focused on specific projects, the process must also include an examination of organization-wide practices that have an impact on privacy. Your policies and procedures, or the lack of them, affect your ability to ensure that privacy protecting measures are applied to specific projects.

HEALTH INFORMATION ACT

Under Alberta's *Health Information Act* (HIA) custodians must submit PIAs to the Information and Privacy Commissioner before implementing practices or information systems that will collect, use or disclose individually identifying health information. This includes changes to existing practices or information systems.

MAKING A PIA SUBMISSION

Submit your PIA under the signature of the responsible custodian (or their authorized representative). The OIPC may return a PIA that has not been submitted by a person with appropriate authority.

Incomplete PIA submissions will be returned to the submitter un-reviewed. This applies particularly to submissions that are missing policy and procedure attachments listed in **Section E** of the Requirements.

PIAs submitted to the OIPC under the HIA must follow the format described in the PIA Requirements.

PIA REVIEW

After receiving a PIA, a Portfolio Officer is assigned to conduct a review. The Portfolio Officer may raise questions or seek clarification on certain points in your PIA. This may occur if the project's legal authorities are unclear or missing, if impacts to privacy are significant and unmitigated, or if the risks to privacy appear to outweigh the benefits of the project. The Portfolio Officer may contact you by phone, fax, email, or letter. For complex projects or those with major privacy implications the Portfolio Officer may ask you to make a presentation to the Commissioner or OIPC staff.

OIPC REVIEW TIME

Be sure to allow time for the OIPC to review and comment on your PIA so you can consider this feedback before you fully implement your project. If you leave it too late and the OIPC identifies privacy concerns, it may be necessary to make expensive and time-consuming changes to your project late in the development cycle.

The OIPC will try to provide the preliminary results of your PIA review within 45 calendar days. The time from preliminary review to final PIA acceptance depends on how quickly you resolve any questions raised by the Portfolio Officer.

PIA ACCEPTANCE

Once you address any questions and are committed to providing the necessary level of privacy protection, the Portfolio Officer accepts the PIA by sending you a letter to confirm. Acceptance is not approval; it reflects the Portfolio Officer's opinion that you have considered the requirements of the HIA and have made a reasonable effort to protect privacy.

*A PIA cannot be used to obtain a waiver of, or relaxation from, any requirement of the **HIA***

If you do not respond to all questions raised in the PIA review within the deadlines set by the Portfolio Officer, your PIA review file is closed without acceptance. It is difficult to demonstrate that you have taken reasonable measures to protect privacy when your PIA has not been accepted. This situation can put your project at risk, especially if you face privacy complaints from the public.

AFTER PIA ACCEPTANCE

New practices and technologies evolve after projects are implemented. New threats to privacy may also develop over time. You should periodically review your PIA to ensure any risks caused by these changes are mitigated. You should also advise the OIPC of any resulting changes to your PIA. In some cases a short letter is sufficient; in other cases, you may wish to resubmit a revised PIA.

If a member of the public makes a complaint against your organization, the Commissioner or OIPC staff may review previously submitted PIAs to gather information about your privacy practices.

EXPEDITED PIA PROCESSES

For major initiatives in the health sector that involve multiple custodians, the Commissioner has accepted alternate PIA processes to simplify reviews and accelerate turn-around time.

Past examples of this have included the Alberta Netcare Portal, the Physician Office System Program and the Pharmacy Practice Models Initiative. An expedited PIA process can only be developed in consultation with the OIPC and must still reasonably address privacy risk. If you believe your project would benefit from an expedited PIA process, contact the OIPC.

*The **OIPC** can advise you on complex projects or those involving multiple parties, prior to **PIA** submission.*

DO THESE REQUIREMENTS APPLY TO ME OR MY ORGANIZATION?

Before starting your PIA, you need to understand how the HIA applies to your situation. To determine how the HIA applies to you, here are a few questions you can ask yourself:

1. **Am I, or is my organization, a custodian under the HIA?**
   HIA custodians include Alberta Health and Wellness, Alberta Health Services, the Health Quality Council of Alberta, nursing homes, physicians, pharmacists, opticians, optometrists, midwives, podiatrists, dentists, dental hygienists, denturists, registered nurses and any other health services providers named in the regulations.

   To determine if you or your organization is an HIA custodian, you should refer to section 1(1)(f) of the HIA and the *Health Information Regulation*.

2. **Who am I working for?**
   You may sometimes fall under the definition of a custodian, while you may at other times work for a custodian, in which case you are known as an "affiliate" under the HIA. An example of this would be a physician who has admitting privileges with Alberta Health Services. When working in independent practice, the physician is a custodian in his or her own right. When working for Alberta Health Services, this physician must follow Alberta Health Services' rules regarding privacy and Alberta Health Services remains ultimately responsible for compliance with the HIA, including PIA requirements.

   If your project relates to work you perform for another custodian, that custodian will be responsible for submitting the PIA (even though you may assist in writing it). If your project relates to work done in your own independent practice, you are responsible for submitting your own PIA.

3. What are my contractual relationships?

You may be subject to one privacy law in the normal course of your operations, but may provide service to an organization that is subject to the HIA. For example, a national vendor of electronic medical records software may be subject to federal privacy law and other provincial laws for other parts of its operations and be subject to the HIA as an information manager for a custodian in Alberta.

While the custodian you work for is ultimately responsible for any PIAs, you may be asked to assist in writing a PIA on their behalf.

4. Do I have a dual role?

Some HIA custodians are also public bodies subject to the *Freedom of Information and Protection of Privacy Act*, for example, Alberta Health and Wellness, Alberta Health Services, and nursing homes.

If you work for these kinds of organizations, your project likely falls under the HIA if it relates to the provision of health services as defined in the HIA.

WHEN TO DO A PIA

HIA SECTION 64

Most PIAs are done to satisfy the requirements of section 64 of the *Health Information Act*. Under section 64 custodians must submit PIAs whenever they plan to implement new administrative practices or information systems that collect, use or disclose health information about identifiable individuals. This also applies to changes to practices or systems.

Here are a few examples of situations where you should consider a PIA under section 64 of the HIA:

- You collect, use or disclose new health information that you did not collect, use or disclose before.
- You give access to health information to new parties.
- You implement a new service delivery or management technology that stores, transmits, or retrieves health information.
- You implement a new or different electronic health record system, or make changes to an existing one, such as adding portable devices with wireless network connections.
- You enter into an agreement with a new business partner or vendor who will have access to health information in your custody or control.
- You establish a new healthcare delivery model, such as a new Primary Care Network or a new Telehealth initiative.
- You create a new organization that will collect, use or disclose health information.

PIAs are required for paper-based practices and administrative processes, as well as electronic ones.

If you are unsure whether a PIA is required, consult the OIPC or your privacy officer.

The OIPC is often asked how big changes have to be in order to trigger a PIA. The most important question to ask yourself is, “Does this project pose any new risks to the privacy of health information?”.

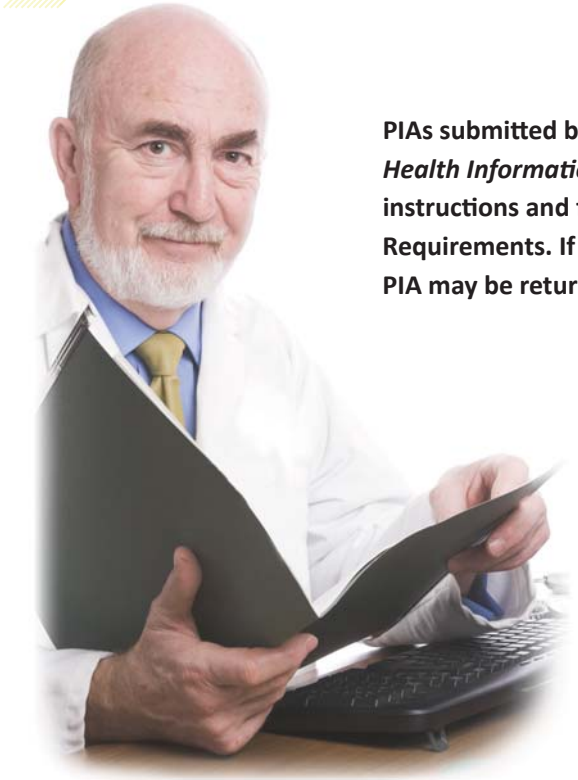
Some situations may not call for a PIA, for example moving your office to a new location, upgrading your computer operating system, software upgrades or bug-fixes that don't add new functionality. In some of these examples, you should still conduct an internal privacy threat-risk assessment, but you likely don't need to do a PIA.

DATA MATCHING PIAs

Data matching is the creation of new information by combining two or more sets of data. Sections 70 and 71 of the HIA require that custodians prepare a privacy impact assessment before performing data matching involving health information. The custodian that carries out the data matching is responsible for preparing the PIA.

PIA SUBMISSION MANDATORY

Under the HIA, submission of your PIA to the Office of the Information and Privacy Commissioner (OIPC) is mandatory and must precede implementation of your new system or practice.



PIAs submitted by custodians under the *Health Information Act* must follow the instructions and format set out in these Requirements. If you fail to do so, your PIA may be returned by the OIPC.

PERIODIC REVIEW

Section 8(3) of the *Health Information Regulation* says that custodians must periodically review the safeguards they have in place to protect health information privacy. This means that custodians need to regularly review the privacy risk mitigation plans set out in PIAs to ensure they continue to protect against reasonably foreseeable risks to the privacy of health information.

PIA AMENDMENTS

You may have already submitted a PIA for a particular project, but the circumstances have changed. As long as your original PIA was accepted by the OIPC, you may be able to account for the changes to the project by submitting a PIA amendment. In many cases, a letter to the Commissioner outlining the changes and what measures you have taken to mitigate any additional risks to privacy is sufficient.

If you are uncertain as to whether to submit a PIA amendment or a fully revised, new PIA, contact the OIPC for guidance.

PIA TIMING

It is important to conduct the PIA at the appropriate stage of the project lifecycle. Conducting a PIA too early in the project will be difficult because you will not have all the information you need to fully describe the project or to fully identify privacy risks and mitigation measures.

On the other hand, doing a PIA too late in the development process could mean having to make time consuming and expensive changes to applications, business processes or other features of the project that have already been completed.

Generally speaking, the best stage to do a 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 influence project design from a privacy perspective.

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

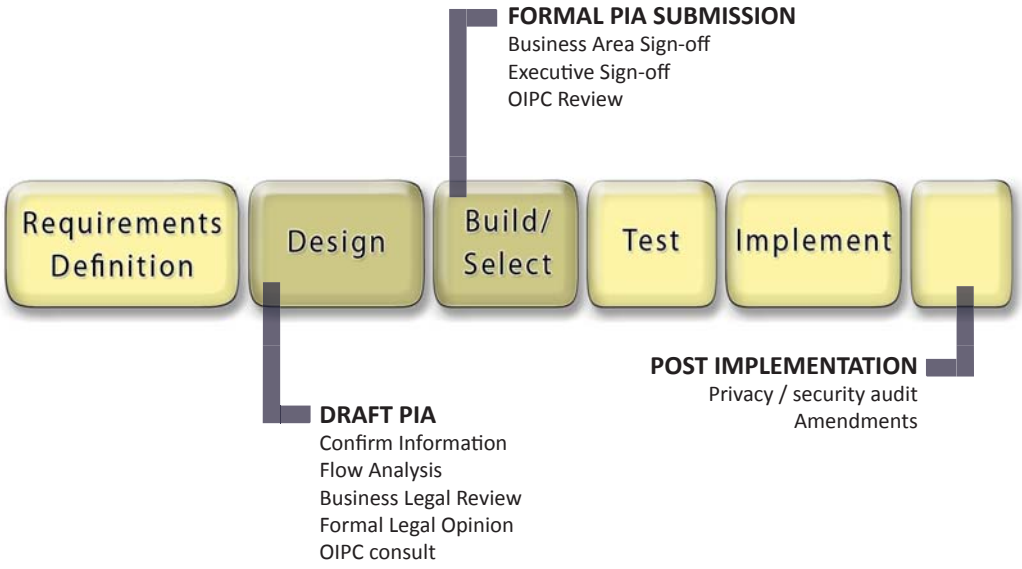
- Access controls to enforce the need to know principle
- System logging controls that meet reporting and retention requirements of the HIA
- Ability to limit access to health information at a patient's request
- Encrypting health information transmitted over public networks or stored on mobile devices

There is no point in attempting to do a PIA until you know how health information fits into your project. Therefore, you should review the health information elements needed for your project and understand how they will be collected, used and disclosed before writing your PIA.

Your PIA must include details on your information security and privacy policies and procedures. You should at least have draft versions of these project components before you begin the PIA.

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.

BUILD PIA INTO EXISTING BUSINESS PROCESSES



PIA SUBMISSION

PIA FORMAT

The format described in the PIA Requirements is mandatory for HIA PIAs. PIA submissions must include the following sections. Each section is described in more detail in the PIA Requirements.

- **COVER LETTER**
  The cover letter is a brief letter, addressed to the Information and Privacy Commissioner that introduces the PIA. It is signed by the custodian or their authorized representative.

- **COVER PAGE**
  The cover page provides basic information about the PIA and contact information for people involved in the PIA process.

- **SECTION A**
  Project Overview describes the project to be assessed.

- **SECTION B**
  Privacy Management addresses your overall management of privacy functions, including organizational structure and policies.

- **SECTION C**
  Project Privacy Analysis addresses privacy topics related to the specific project that is the subject of the PIA.

- **SECTION D**
  Project Privacy Risks and Mitigation Plans describes the privacy risks and mitigation measures you have identified for the project in question. This is a critical component of the PIA and should be completed in as much detail as possible.

- **SECTION E**
  Policy and Procedures Attachments provides a list of privacy and information security policies you need to attach to your submission. Policies and procedures specific to the project are also included in this section.

GUIDANCE for WRITING YOUR RESPONSES

Organize your PIA using the section titles and questions in the order they appear in the Requirements. Do not skip any section. If an item is not applicable or unavailable, say so in your response and explain why. If you leave sections of your PIA blank with no explanation, it will be considered incomplete and returned to you un-reviewed.

Please provide sufficient detail in your responses to demonstrate that you have made a reasonable effort to consider privacy impacts in your project. If you do not provide enough detail, the OIPC Portfolio Officer assigned to review your PIA will likely ask for clarification, increasing your overall PIA review time and possibly delaying your project.

POLICY & PROCEDURE ATTACHMENTS

The attachments listed in Section E are required for effective privacy management and compliance. Your PIA will be considered incomplete if it does not include organizational and project-specific policies and procedures.

REFERENCES

To get the fastest review possible, attach policies and procedures listed in **Section E** of the Requirements with page references. If you do not provide clear references, the OIPC may return your PIA without review.

PREVIOUS SUBMISSIONS

It may be possible to re-use your privacy management description or policies you included in a previously accepted PIA submission. First, you should consider whether you need to make any revisions to accommodate your current project or any recent changes to legislation. If you don't need to make any revisions, please confirm this in your current PIA and provide a reference to the previously accepted PIA, using the file number assigned by the OIPC. If you do make changes to accommodate the current project, please submit a revised version.

COVER LETTER

Organize your PIA using the titles and headings in this section, in the same order that they appear here.

Submit your PIA with a cover letter signed by someone with executive authority to do so. In most cases, this is the custodian or someone who has been formally authorized to act on the custodian's behalf.

COVER PAGE

Please include the following information on your cover page:

- Official Project Name, including any other names or acronyms commonly used to refer to the project.
- Legal Name of the custodian that prepared the PIA.
- Name, Title and Full Contact Information of the person with primary responsibility for completing the PIA. This person will be the OIPC's primary point of contact for any questions about the PIA. It will normally be whoever wrote the PIA or performs the role of privacy officer or HIA Coordinator.

this could be the same person in a smaller organization

- Name, Title and Full Contact Information of the person with primary responsibility for HIA compliance. This is the "responsible affiliate" under HIA section 62.
- PIA submission date.
- Expected Project Implementation Date (for information technology projects, this is the date when your production system goes into use with live data).
- OIPC File References for any previously accepted PIAs that are related to the current PIA (for example, ABC Clinic Electronic Medical Record Project, H9999).

SECTION A
PROJECT SUMMARY

Describe the proposed project, including its objectives. State why the project must collect, use or disclose health information.

Your overview should answer some basic questions about the project that triggered the PIA (for a discussion of what kinds of projects trigger PIAs, see page 10).

1. What does the system or administrative practice do?

2. What is the business rationale for the project (i.e. what problem are you trying to solve)?

3. Who are the key players?

4. Where will health information be stored/accessed?

5. Why does the project need to collect, use or disclose health information to achieve its objectives?

The OIPC publishes summaries of all accepted PIAs in an online PIA Registry. The information you provide in this section is posted in the PIA Registry, which is available to the public at **www.OIPC.ab.ca.**

SECTION B ORGANIZATIONAL PRIVACY MANAGEMENT

If you have already provided a description of your privacy management in a previous PIA and no changes are needed, you may reference the previous PIA using the OIPC file number.
(see page 17 for more details on re-using parts of previously accepted PIAs).

You do not need to list your privacy and security policies here; you will have an opportunity to do that in Section E of your PIA.

1. **MANAGEMENT STRUCTURE**
   How is your senior management involved in decision-making related to privacy?
   Describe your senior management's engagement in setting privacy policy and resolving privacy issues. For example, who does your privacy officer or HIA Coordinator report to? Is there a privacy committee? You may include an organization chart showing how the privacy function is positioned in your management structure.

2. **POLICY MANAGEMENT**
   How do you develop, approve and implement privacy policies?
   Describe how policies are developed, who approves them, how they are communicated, how often they are reviewed, and any other relevant information concerning the privacy policy environment.

3. **TRAINING AND AWARENESS**
   How are your employees and contractors trained in privacy?
   Identify privacy training you give your employees and contractors, such as new employee orientations and on-going privacy awareness programs. You should note who receives training, how often you offer training, whether your training program is periodically updated to reflect legislative and technology changes, and how you document that someone has received privacy training.

4. INCIDENT RESPONSE

How do you identify, investigate and manage privacy incidents?

The OIPC defines a privacy incident as an event that adversely affects the confidentiality, integrity or availability of health information. A privacy incident may result in the collection, use or disclosure of health information in contravention of the HIA.

Describe your approach to privacy incident response. Your description should state what triggers your incident response plan, who is involved in incident response, how you decide to notify affected parties and how you learn from incidents to improve your privacy practices.

5. ACCESS AND CORRECTION REQUESTS

How do you manage requests from individuals to access their own health information and to make corrections?

Under the HIA, individuals have a right to access their own health information and a right to ask you to make corrections. These rights help to protect individuals' privacy by giving them the ability to see exactly what health information an organization holds about them, which helps them to make decisions about how much information to share and may alert them to potential privacy concerns.

State who is responsible for responding to access and correction requests, how you inform people about your decisions to grant or refuse access/corrections and whether you have an informal process for routine requests.

SECTION C PROJECT PRIVACY ANALYSIS

1. HEALTH INFORMATION LISTING

List the health information that is collected, used or disclosed in the project.

Provide a list of all information you are collecting, using or disclosing that falls within the definition of "health information" in HIA.

As you compile your list, make sure you have a defensible reason to collect, use or disclose each piece of health information in your project. When reviewing your PIA, the OIPC may ask you how the listed health information contributes to the objectives of your project.

For some projects, complete listings of every data element are often too lengthy to be useful. In such cases, you may summarize by providing a description of health information types with some examples in each category.

In all cases, you must list unique identifiers. Unique identifiers are data elements that uniquely identify a single individual, such as name, hospital identification number, personal health number, or account number.

2. INFORMATION FLOW ANALYSIS

Provide a description of the flow of health information for this project. Support your description with a diagram and table that describe the purposes and legal authority for each collection, use and disclosure of health information.

This part of the PIA has two components: an information flow diagram and a table showing the purposes and legal authority for each information flow.

COMPONENT #1 - Information Flow Diagram

An information flow diagram illustrates how health information is collected, how it is used, and how it is disclosed beyond your project or organization.

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 examples given provide two approaches to health information flow diagrams; you may use another method if it makes sense for your project.

Information Flow Diagram Examples

The following are two examples of information flow diagrams for a project proposed by Custodian ABC. This project will:

- collect health information from three different sources:
  the patient, a specialist, and an insurer
- use this information to make health care decisions
- give results and feedback to the patient for on-going care
- send health information to a data storage company

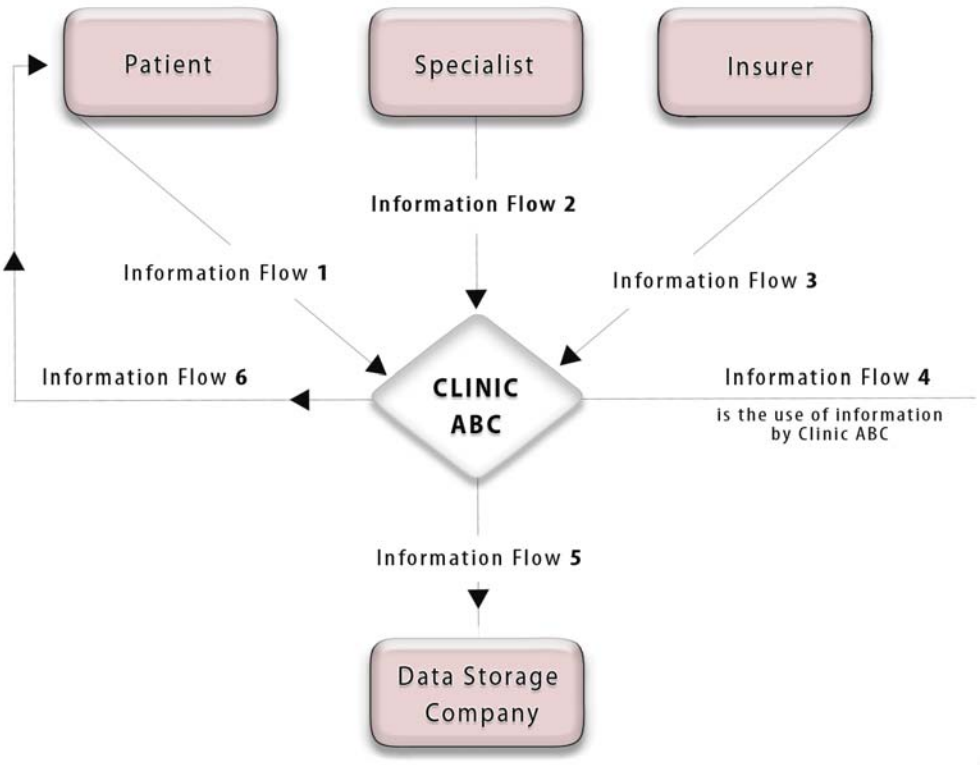
Be sure to number each information flow (i.e. each collection, use and disclosure) for easy reference.

You will need to refer to each flow in a table that describes its purpose and legal authority.

SAMPLE INFORMATION FLOW

Diagram # 1

This type of diagram is best for less complex PIAs that involve small numbers of organizations.



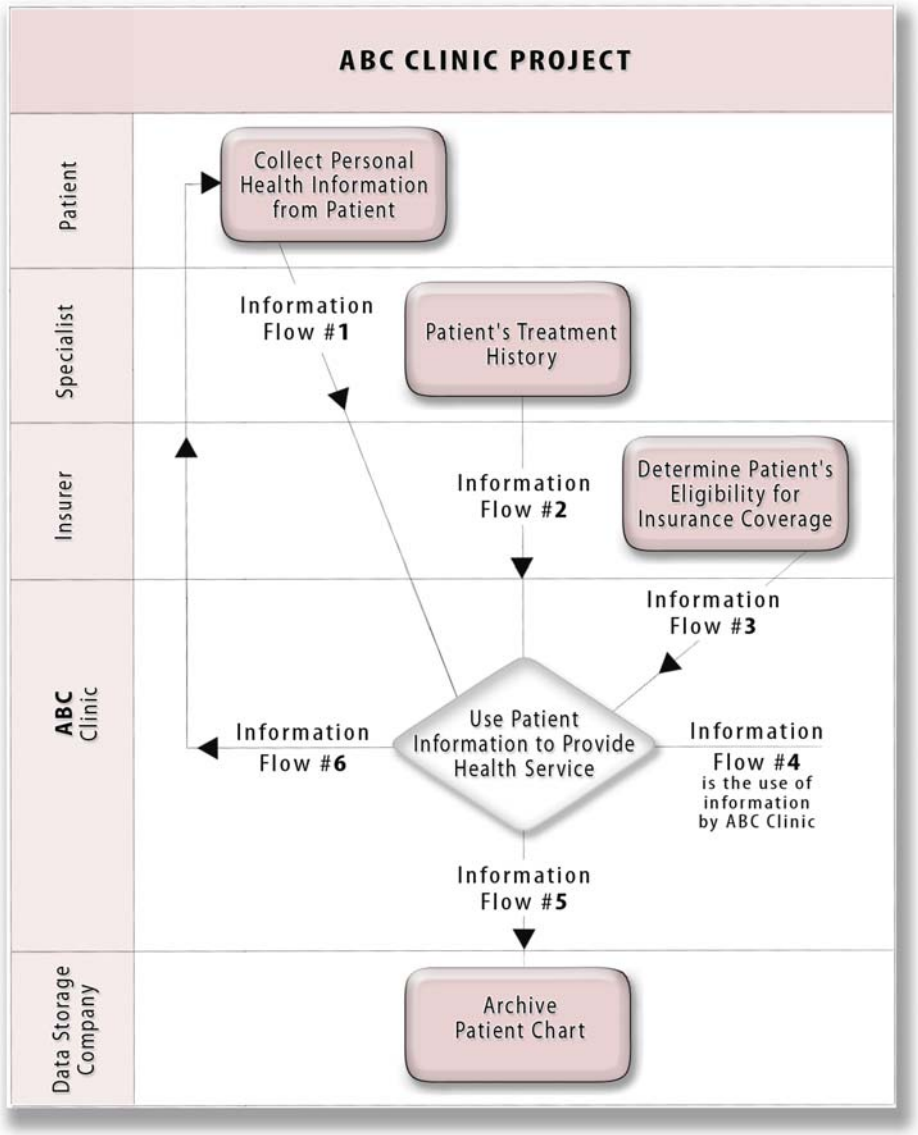
SAMPLE INFORMATION FLOW

Diagram # 2

This type of diagram is best for complex PIA's that involve several organizations.

Be sure to number each information flow (i.e. each collection, use and disclosure) for easy reference.

You will need to refer to each flow in a table that describes its purpose and legal authority.



COMPONENT #2 - Legal Authority and Purposes Table

The HIA sets out specific and limited purposes for the collection, use and disclosure of health information.

Legal authority may come directly from the HIA, or other legislation applicable in Alberta or Canada.

The table below documents that each category of health information is collected, used or disclosed for a clearly defined purpose. Each purpose must be supported by your legal authority to collect, use or disclose health information.

INFOR-MATION FLOW	DESCRIPTION	TYPE OF INFORMATION	PURPOSE	LEGAL AUTHORITY (cite specific sections of appropriate legislation)
1	Collection of health information directly from the patient	Name, address, provincial health number	Information collected to process payment for health services	Collection - (see HIA **Sections 18-24** for legal authority to collect health information)
2	Health information collected from a specialist	Patient's name, provincial health number, history	Information collected to review previous treatment and care	Collection - Indirect Collection - (see HIA **Section 22** for authority to collect health information indirectly)
3	Health information is collected from a 3rd party	Individual's name, account number and details of requested service	Information collected to evaluate individual's eligibility for coverage under insurance plan	Collection - Indirect Collection - (see HIA **Section 22** for authority to collect health information indirectly)
4	Health information is used by ABC clinic	Name, address, provincial health information collected from three data sources	Health information is used to deliver health service	(see HIA **Sections 25-30** for legal authority to use health information)
5	Health information is provided to a data storage vendor	Patient chart	Health information is used to maintain back-ups of data and ensure that the information is retained	Use - Information manager agreement (See HIA **Section 66** and the *Health Information Regulation* for related legal authorities)
6	Health information is disclosed back to the patient	Diagnosis, care instructions	Health information is disclosed to provide ongoing treatment and care	(See HIA **Section 33** for legal authority to disclose health information to patient)

3. NOTICE

Describe how you will notify individuals of all purposes for which their health information is collected. Notifying individuals about why you are collecting health information and what you will do with it is a requirement of the HIA**.**

Identify measures you take to ensure individuals are informed about how you will use their health information (written notices, posters, web pages, etc.).

Consider any unique needs of individuals or groups in relation to this project. Depending on the scope of the project or unique privacy risks, a general notice may be appropriate in some situations, while other projects may need a specific privacy statement.

Your notice needs to include:

- A description of why the health information is collected
- The specific legal authority that authorizes the collection
- Contact information for someone in your organization who can answer questions about the collection

4. CONSENT AND EXPRESSED WISHES

Describe the role that individual consent plays in this project and how you will consider any wishes expressed by individuals about how much information to share. Under the HIA, consent is not required to collect or use health information to provide health services. Rather, custodians rely on legal authority to collect and use health information. Custodians do not normally need individual consent to disclose health information either, as long as they are making the disclosure to provide health services. However, consent may provide authorization to disclose health information in certain circumstances.

If you do rely on consent to disclose health information, consider what form of consent is required under law, how you will keep a record of consent and how individuals can withdraw their consent. Consent must be recorded on paper or electronically and meet the requirements set out in HIA section 34.

You must have the means to consider and accommodate wishes individuals express about how much of their health information to share through your project. While you may decide it is in the best interests of a particular patient to share their health information despite their wishes, you still need to implement some way of accommodating their expressed wishes, when appropriate.

5. DATA MATCHING

State whether the health information from this project will be linked, matched or otherwise combined with health information from other sources. If so, describe how the linkage or matching will occur and its purpose.

Data matching is the creation of new information by combining two or more sets of health information. Data matching can pose privacy risks, for example, unintended inferences may be made about individuals whose data is matched, or previously anonymous data may become identifiable.

Sections 70 and 71 of the HIA require that custodians prepare a privacy impact assessment before performing data matching involving health information. The custodian that carries out the data matching is responsible for preparing the PIA.

6. CONTRACTS AND AGREEMENTS

Describe contracts or agreements with third-parties involved in your project. Describe the privacy provisions that bind third parties to your own requirements for privacy protection.

You are responsible for ensuring that your contractors comply with the HIA in relation to the services they provide on your behalf. Your agreements with third parties, such as service contracts for IT support or other services, should include provisions binding providers to a standard of privacy protection equivalent to your own.

Information Managers are a special class of service provider identified in the HIA. Information Managers provide information management or information technology services and may process, store, retrieve, de-identify, or dispose of health information. There are specific requirements for information manager agreements in HIA **Section 66** and in the *Alberta Electronic Health Record Regulation*.

Consider providing copies of your third-party agreements. At a minimum, you should provide the privacy provisions from these agreements.

7. USE OF HEALTH INFORMATION OUTSIDE ALBERTA

Describe how and why health information from your project is used in jurisdictions outside Alberta.

Custodians are directly responsible for the actions of their service providers, including those located outside of Alberta.

You may need to engage a service provider from outside of Alberta who will have access to health information in your custody or control. Transferring or storing health information outside Alberta is permitted under the HIA, but requires careful consideration to assess and mitigate risk. This is particularly important as the laws that protect privacy in other provinces or countries may not be equivalent to those in Alberta. Therefore, you must review agreements with out-of-province service providers to ensure they contain contractual language that meets the specific requirements of the HIA and the *Health Information Regulation*.

Extra-provincial disclosures may occur in ways you have not considered. For example, if your computer help desk is outside Alberta, health information may flow outside the province during help desk calls. Also, your data backup or archiving facility may be located out of province. If you are part of an international organization, your data may be accessible from beyond Canada. Be sure you have considered all possible disclosures or uses of health information outside Alberta.

The *Health Information Regulation* specifies extra measures to be followed if you use or disclose health information outside of Alberta. Be sure you review these provisions if you disclose health information to another jurisdiction.

SECTION D
PROJECT PRIVACY RISK MITIGATION

1. ACCESS CONTROLS

Describe how persons, positions, employee categories or third parties are given access to specific health information data elements or categories. This describes your application of the "need-to-know" principle. 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 who has access to the information, the nature of the information, the circumstances under which they have access, the type of access and the purpose or reason for the access.

For projects involving access to electronic systems, provide a description of the processes used to authenticate user identity and authorize user access to system screens, reports and features. You should also describe how user authorization is terminated when someone leaves or changes position. Include clear descriptions of the access controls themselves and how they are implemented and maintained for the project.

Use an access table based on the following example to answer this question. The table below is for illustration only; you may need to adjust it to provide room for your responses.

Example Table: Access to Health Information by Role

Position & Job Title	User Role	Number of Staff in this Role	Type of Access (Read, Write, Edit)	Description of Information this User Can Access (include examples)
Administrative Support				
Physician				
Pharmacist				
Nurse				
Contractors				

2. PRIVACY RISK ASSESSMENT AND MITIGATION PLANS

Describe the specific privacy risks you have identified for this project and how you plan to mitigate them.

Every project that collects, uses or discloses health information has some privacy risk. The HIA does not require that you completely eliminate all risk. Rather, you need to identify risks and apply reasonable privacy protection measures. Your response to this question should describe the measures you are taking to address specific privacy risks associated with this project.

Project Privacy Risks

Based on the experience of the OIPC, most projects face the five risks listed below. Your mitigation plans must address each of these risks.

If any of these risks do not apply to your project, please explain why.

1. Unauthorized use of health information by internal or authorized parties.

2. Unauthorized collection/use/disclosure of health information by external parties.

3. Loss of integrity of health information.

4. Loss, destruction, or loss of use of health information.

5. Your contractor or business partner collects, uses or discloses health information in contravention of the HIA or your policies.

The above risks are broad. You should describe the circumstances that lead to the risks within your project. For example, you may face the risk of unauthorized use of health information by external parties because your computer terminals are located in public areas, or because the information includes financial details, making it a valuable target to hackers.

Your mitigation plans must include a combination of administrative, technical or physical measures you have taken to mitigate or reduce privacy risk.

You will likely have more than one measure to address each risk. For example, you may have a policy combined with a training program and an audit to reduce a particular risk.

Please provide a specific reference to a page number and heading or section number if you refer to attached polices and procedures as part of your mitigation plans.

Other Privacy Risks

You will likely identify risks beyond the five listed above. For example, re-identification of anonymised data through data matching, theft or loss of mobile devices, or unauthorized disclosure via a wireless network may be risks that are unique to your project.

This is a sample risk mitigation table:

Privacy Risk	Description	Mitigation Measures for Project	Policy Reference
Unauthorized use of information by authorized users			
Unauthorized collection/use or disclosure of information by external parties			
Loss, destruction or loss of use of information			
Loss of integrity of information			
Unauthorized or inappropriate collection/use or disclosure by a contractor or business partner			
Other project specific privacy risks			

3. MONITORING

Describe your plans to monitor compliance with your privacy protection measures. Include a description of the monitoring processes you will use, how frequently you will apply them, and how you will review results to improve the privacy and security of health information.

Monitoring is essential to test and improve your ongoing privacy compliance. Provide a project-specific monitoring/audit plan, describing who will conduct reviews, the frequency of monitoring, what kind of anomalies will be flagged for review, and when your incident response plan will be triggered.

System logs are a feature of information technology applications, not paper records. However, there are monitoring processes that can identify anomalous records, loss of records, or other triggers that may reflect gaps or deficiencies in your privacy protection measures, even for paper-based projects.

Review PIA Amendments on page 12 to guide you in submitting a revised PIA to the OIPC.

Your plans to monitor access and disclosure should reflect the sensitivity of the health information involved. Very sensitive information, such as diagnostic, treatment and care records or patient financial information, demands more rigorous monitoring than less sensitive information, such as contact information (however, some circumstances may even require strict monitoring of contact information). Your plans may include internal system log reviews and audits, or independent third party audits.

4. PIA COMPLIANCE

Describe how you will periodically review your PIA and provide updates or revisions to the OIPC as necessary. Also describe how you will monitor your compliance with the statements made in the PIA and make any necessary changes.

Your privacy impact assessment describes your project, usually just before implementation. Over time, business processes and practices will change and your implemented project may no longer be accurately reflected in your PIA. Similarly, risks and the measures available to mitigate those risks will also change, as a result of new knowledge, new technologies, or other changes to the environment.

It is important to plan for periodic reviews of your project post-implementation to ensure it still conforms to your PIA. If there are gaps between what you described in your PIA and current reality, consider writing a PIA amendment. Periodic review of privacy protection measures, which include your PIAs, is mandatory under the HIA.

SECTION E
POLICY & PROCEDURES ATTACHMENTS

Attach copies of policy documents to demonstrate you have addressed the topics listed in the appendices. Use the following table to summarize all of the policy and procedure documents you provide with your PIA.

PRIVACY POLICY TABLE

For each topic in the table, indicate whether you have an applicable policy or procedure and, if so, the title of the document and relevant page reference(s). Your policies and procedures may respond to more than one of the topics in the table below. If so, please cross reference those policies or procedures to avoid duplication in your responses. However, make sure that you provide page numbers for any cross references to allow easy identification of the relevant material.

GENERAL PRIVACY POLICIES

The table starts with general privacy policies. These are your organizational privacy policies that should be in place whether or not you ever need to write a PIA. If you are a custodian under the HIA, policies that facilitate implementation of the HIA are mandatory.

PROJECT SPECIFIC POLICIES

The second part of the table allows you to enter project-specific policies. These are privacy and information security policies that only apply to the project covered in this PIA.

PREVIOUS PIA SUBMISSIONS

If there are no changes, you may refer to general privacy policies submitted in a previously accepted PIA. See page 17 for a description of how to re-use policies.

GENERAL PRIVACY POLICIES

TOPIC	POLICY DESCRIPTION	ATTACHMENT TITLE(S)	PAGE REFERENCE(S)
PRIVACY ACCOUNTABILITY	This is a broad policy that enables privacy roles and accountability within your organization. Sometimes called a privacy charter, this policy does not provide detailed work instructions, but rather sets out responsibilities and commitments in relation to privacy. This policy should include: • Where privacy fits into your organizational structure • Who is responsible for privacy, including who is responsible for responding to privacy complaints • Who is responsible for information security • Commitment to protect confidentiality and to collect, use and disclose health information in a limited manner • Commitment to maintain accuracy of health information • Commitment to provide privacy training and awareness to employees • Commitment to maintain technical and administrative safeguards to protect health information • Right of access to health information and right to request corrections • Schedule for periodic review of privacy policies		
ACCESS TO HEALTH INFORMATION	Your process and timeframes for responding to formal requests from individuals for access to their own health information. Include references to appropriate fee schedules or other policies for charging fees to process access requests. If you require that individuals fill out a form to make access requests, include it here. You should also consider a process for responding to informal requests or making routine disclosures.		

GENERAL PRIVACY POLICIES

TOPIC	POLICY DESCRIPTION	ATTACHMENT TITLE(S)	PAGE REFERENCE(S)
CORRECTION REQUESTS	Your process and timeframes for responding to individuals who ask you to correct their health information. Include your process for responding to these requests and describe how you inform individuals of your decisions to grant or refuse corrections.		
TRAINING, AWARENESS & SANCTIONS	Your privacy training program for employees and others that will have access to health information in your custody. This policy should include sanctions for not complying with your privacy policies.		
COLLECTION OF HEALTH INFORMATION & NOTICE	Acceptable reasons for collecting health information, which should include statutory authority, under the HIA or other relevant legislation. Include examples or descriptions of how you notify individuals about why you are collecting their information.		
USE OF HEALTH INFORMATION	Acceptable uses of health information in your organization.		
DISCLOSURE OF HEALTH INFORMATION	Reasons why your organization discloses health information to other organizations or persons. This policy should cover: • disclosure with consent • disclosure without consent • disclosure of non-identifying information • keeping a record of disclosure • disclosure notice		

GENERAL PRIVACY POLICIES

TOPIC	POLICY DESCRIPTION	ATTACHMENT TITLE(S)	PAGE REFERENCE(S)
RESEARCH	How your organization handles research, requests from researchers under Sections 48-56 of the HIA. This should cover: • approval process for research requests • agreements with researchers		
THIRD-PARTIES	How you ensure that third parties, which include contractors and information managers, protect your organization's health information. This policy should include: • privacy requirements for third-parties • review of third-party compliance • requirements for out-of province information managers		
PRIVACY IMPACT ASSESSMENTS	Circumstances that trigger your organization to conduct a privacy impact assessment. This policy should describe who is responsible for conducting PIAs and how often they are reviewed.		
RECORDS RETENTION & DISPOSITION	How long you keep records containing health information and what you do with them once they are no longer needed. Include references to any statutory or professional records retention and disposition schedules you follow. This policy should also include a process to securely dispose of health information when no longer needed. The HIA requires that disclosure records and certain system log information be kept for 10 years.		

GENERAL PRIVACY POLICIES

TOPIC	POLICY DESCRIPTION	ATTACHMENT TITLE(S)	PAGE REFERENCE(S)
INFORMATION CLASSIFICATION	Information should be protected at a level commensurate with its sensitivity and the risks it faces. Describe how you classify health information in order to determine the most appropriate level of security.		
RISK ASSESSMENT	New risks to the confidentiality, integrity and availability of health information may arise over time as technology and business processes evolve. This is your policy for conducting periodic risk assessments to assess the effectiveness of your privacy policies.		
PHYSICAL SECURITY OF DATA & EQUIPMENT	The physical and administrative measures you take to secure health information in paper and electronic form. This policy should describe how you secure your workspaces, computers, fax machines, copiers, and other office equipment. Pay special attention to securing mobile equipment, such as notebook computers and mobile data storage devices.		
NETWORK & COMMUNI-CATIONS SECURITY	Measures you take to secure your network and communications infrastructure. This could include such controls as malware (anti-virus) protection, firewalls, intrusion detection systems and encryption.		
ACCESS CONTROLS	Identifying and verifying users of your health information, deciding what information they need to use, and making changes when users change positions or leave. Identification and verification includes assigning usernames, passwords and tokens.		
MONITORING & AUDIT	How you ensure that users of health information comply with your policies. This policy should describe what you monitor to ensure compliance, frequency of review and triggers for a formal audit/review or activation of your incident response plan.		

GENERAL PRIVACY POLICIES

TOPIC	POLICY DESCRIPTION	ATTACHMENT TITLE(S)	PAGE REFERENCE(S)
INCIDENT RESPONSE	Your plan to deal with contraventions of the HIA or your own privacy policies. Your plan should: • Define what constitutes a privacy incident (or levels of privacy incidents) • Identify members of an incident response team • Describe process to bring incidents to attention of senior management and engage them in response • Process to determine whether to notify individuals affected by incident • Process to determine whether to notify Office of the Information and Privacy Commissioner about incident		
BUSINESS CONTINUITY	How you ensure health information is available when needed. This includes your plans to back-up data and your plans for disaster recovery, based on business need.		
CHANGE CONTROL	Ensuring that changes to systems do not adversely affect the confidentiality, integrity or availability of health information.		

PROJECT SPECIFIC POLICIES

TOPIC	POLICY DESCRIPTION	ATTACHMENT TITLE(S)	PAGE REFERENCE(S)
PROJECT SPECIFIC POLICIES	Include project-specific policies here		

GLOSSARY

The following terms and definitions are used throughout these Requirements.

TERM	DEFINITION
Affiliate	Under the HIA an affiliate is an individual employed by a custodian, a person who performs a service for a custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian, an information manager, or a health services provider who has the right to admit and treat patients at a hospital as defined in the *Hospitals Act.*
Collection	Refers to the act of bringing health information into your organization from an external source, which may be the subject of the information (i.e. the patient) or a third party.
Custodian	A health services provider, individual, board, panel, agency, corporation or other entity designated as a custodian in the HIA or regulations, responsible for compliance with the HIA.
Disclosure	Refers to the act of providing health information to someone who is not an affiliate of your organization.
FOIP	*Freedom of Information and Protection of Privacy Act.*
Health Information	Information about an identifiable individual that meets the definition of health information under the HIA. This includes two kinds of health information: - Registration information, such as an individual's name, contact information, information about payment for health services, provincial health number and other unique numbers. - Diagnostic, treatment and care information,
HIA	*Health Information Act*.

TERM	DEFINITION
Information Manager	A service provider engaged by a custodian under the HIA to provide information management or information technology services involving health information. The HIA places specific requirements on the custodian and the information manager for such arrangements.
OIPC	Office of the Information and Privacy Commissioner.
PIA	Privacy impact assessment.
PIPA	*Personal Information Protection Act.*
Policy	A written statement that communicates management's intent, objectives, requirements, responsibilities, and/or standards in a particular area of operations or planning.
Project	A project, program, initiative, application, system, undertaking, or endeavour for which a PIA may be appropriate.
Use	Refers to the act of applying health information to a particular purpose within your organization.

NOTES

Office of the
Information and Privacy
Commissioner of Alberta

410, 9925 - 109 Sreet
Edmonton, Alberta T5K 2J8
Phone: 780.422.6860
Fax: 780.422.5682

www.OIPC.ab.ca