Completing a Privacy Impact Assessment

Annotated Template

Alberta

Completing a Privacy Impact Assessment Annotated Template, Version 1.1

Alberta Health, Government of Alberta

April 2023

Contact

Information Management Branch
Health Information Systems
Alberta Health
21st Floor, ATB Place North
10025 Jasper Avenue NW
Edmonton, Alberta, T5J 1S6 Canada

Email: hiahelpdesk@gov.ab.ca

Statement of Availability

As part of the Government of Alberta's commitment to open government, this publication is posted to and permanently retained in the Open Government Portal at https://open.alberta.ca/publications/completing-a-privacy-impact-assessment-annotated-template

Table of Contents

Privacy Impact Assessments

Purpose and Template

The purpose of a privacy impact assessment (PIA) is to describe how proposed administrative practices or information systems may affect the privacy of the individuals who are the subjects of the information.

Under Section 64 of the *Health Information Act* (HIA), a custodian is required to prepare a PIA any time there are new, or if there are changes to, existing administrative practices or information systems relating to the collection, use or disclosure of individually identifying health information. For example, a PIA is required when a custodian gives access to health information to new parties such as an EMR vendor or when a custodian decides to share information with a Primary Care Network.

Under Section 60 of the HIA, custodians have a duty to protect health information and "must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards". Custodians must also ensure the accuracy of health information (section 61) and adopt policies and procedures to facilitate the implementation of the HIA (section 63). The PIA process is a due diligence exercise that helps mitigate risks and ensure compliance with these and other obligations under the HIA.

This PIA template is intended to assist community-based custodians in completing PIAs. Designated custodians are defined in Sections 1(1)(f) of the HIA and 2(1) of the *Health Information Regulations* (*HIR*). Following this template does not guarantee that the Office of the Information and Privacy Commissioner will accept your PIA.

Please keep in mind that not all the guiding questions provided in this template will be relevant to you and your practice, and that more information may be required depending on your circumstances.

All examples and samples provided are illustrative only and should not be viewed as authoritative statements of the law. This template is not to be used as a substitute for legal advice. In case of any doubts as to the proper application of the HIA, please consult with your privacy coordinator or legal counsel. Please note that this template also does not replace advice from information technology security professionals about the security of your information system.

Resources

Alberta Health

The *Health Information Act* Guidelines and Practices Manual, Chapter 5: Duties and Powers of Custodians Relating to Health Information, offers information about the PIA requirements and process.

Privacy & Security Resources

- Alberta Health
    - Health Information Act Forms
    - Responsibilities of Custodians and Health Information Act Administration Checklist
    - HIA Guidelines and Practices Manual, Chapter 14 – Duty to Notify (Mandatory breach reporting)
    - PIA Update Self Assessment Tool
- Office of the Information and Privacy Commissioner (OIPC)
    - PIA Requirements Guide
    - Guidance for Electronic Health Record Systems (assessment of system safeguards and sample practices)
    - Advisory for Communicating with Patients Electronically
- Contact your health professional college or association to inquire about member-specific PIA resources.

Office of the Information and Privacy Commissioner (OIPC)

- For more information about PIA requirements and the PIA process, please visit the OIPC website: Privacy Impact Assessments.
- Contact information:
- Monday – Friday 8:15 am to 4:30 pm
- Toll Free: 1-888-878-4044
- Email: generalinfo@oipc.ab.ca

Questions about the HIA?

For questions about PIAs or other topics related to the HIA, please contact the HIA Help Desk at:

780-427-8089 or hiahelpdesk@gov.ab.ca.

Preparing Your PIA

- Start the process early. You must submit your PIA to the OIPC for review and comment before implementing a new or updated administrative practice and/or information system. You may wish to contact the OIPC to ask about a time estimate for their review and comments.
- It is important to gather all relevant information about your proposed system or practice before starting to draft your PIA. Gather all relevant documentation, such as previous privacy and security assessments, privacy policies and training materials, agreements with services providers that have access to health information, and information about business processes, practice workflows, and information flows. Some of these documents (e.g., policies and procedures) will be attached to your completed PIA prior to submission.
- As required, use the information you gather to inform the explanations you provide in the PIA for your specific system or practice. The PIA's broad headings cannot be modified, but you may consider adding subheadings for clarity.
- 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 in your PIA blank with no explanation, the OIPC may consider your PIA incomplete and return it to you un-reviewed.
- It is important to remember your audience for your PIA. A PIA is not intended to be a technical assessment, but an assessment of privacy issues arising from a new, or changes to an existing, administrative practice or information system. Make an effort to keep information straightforward and understandable by a reader who does not have expertise in information system technology, law, or the background of the systems.
- Write clearly and concisely. Avoid jargon and acronyms unless they are explained. There is no minimum or maximum length required for a PIA. Use your professional judgement to determine what information is necessary to include. Information must be comprehensive, but you should make an effort to include only information that is necessary for the reader's understanding of the practice or system and its impacts.
- Explain any terms, positions, and organizations that are not commonly understood.
- Remember: A custodian may delegate their PIA-related work to a responsible affiliate (e.g., office manager, or a consultant), but ultimate accountability for a PIA remains with the custodian.

Cover Letter

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

DATE

Diane McLeod
Information and Privacy Commissioner
Suite 410, 9925-109 Street NW
Edmonton, AB T5K 2J8

Dear Ms. McLeod:

Re: Privacy Impact Assessment for [*insert Title*] – [*CUSTODIAN NAME*]

Please find attached my PIA regarding the implementation of [*insert name of system or type of practice*], a [*insert high-level description of the system or practice, e.g., billing submission service, electronic medical record (EMR), patient portal, dictation service, etc.*].

[*Use this section to briefly highlight any critical or relevant information regarding the PIA. This may include whether or not you have an existing or previously accepted PIA, or if you have reviewed your policies and procedures and found no need for updates as part of this new PIA/PIA amendment.]*

The attached PIA is submitted for review and acceptance by the OIPC. Should there be questions about any aspects of the submission, please contact [*primary contact name or role as listed in cover page below*] for clarification.

Yours truly,

[Custodian Name]

Note: The responsible custodian must sign the PIA. This responsibility cannot be delegated to another individual.

Cover Page

Fill out the following information:

Official Name *Of your practice or system*	
Legal Name of Custodian	
Person(s) responsible for drafting the PIA *Examples: Custodian, Office Manager, Privacy Officer, PIA contractor, HIA coordinator.*	Name: Title: Contact Information:
Person(s) with delegated responsibility for HIA compliance within the organization *In a community practice setting, one person might occupy more than one role. The same person may be responsible for both drafting the PIA and ensuring HIA compliance.*	Name: Title: Contact Information:
PIA Submission Date	
Expected Start Date *Remember – you must submit a PIA to the OIPC for review before you implement a new system or practice.*	
OIPC File Reference Numbers for previously accepted and related PIAs *Examples may include an electronic medical record (EMR) PIA or Alberta Netcare PIA that you have completed previously.*	

Section A: Project Summary

Use this section to describe the proposed system or practice, including its objectives. State why the system or practice requires the collection, use or disclosure of health information.

[Use this space to describe how you will meet the legislative requirements.]

HIA Requirements:

Under Section 60 of the HIA, you are required to safeguard the health information in your custody and control. One aspect of this requirement is completing this PIA (HIA Section 64). When implementing a new, or making changes to an existing, system or practice in your clinic that involves health information, it is important to explain what the system or practice is, what it does, and how you plan to meet your obligations under the HIA during and after its implementation.

Guiding Questions:

- *What does the information system or administrative practice do? What is its purpose?*

For example, if you are planning to implement a new electronic medical record (EMR), describe the system you will be using and how it operates. Explain why you would like to implement the EMR. Common reasons for implementing an EMR include improving communication between health care professionals and between health care providers and patients, improving clinical practice, storing health records, and supporting clinic productivity.

- *Why does the system or practice need to collect, use, or disclose health information to achieve its objectives?*
- *Who is involved with the system or practice and what is their role?*

For example, do you employ staff that will be involved in implementing the system or practice? Have you hired a vendor to deploy a new system, such as an EMR?

- *Where will the health information be accessed and stored?*

For example, will servers be physically located at your clinic/business, or will they be cloud-based?

- *Will you and your affiliates access health information from within your clinic/office, using only your devices? Will you and your affiliates access health information be using mobile devices? Will your affiliates be permitted to access health information using their own devices?*
- *Will a vendor be responsible for certain activities such as storing information in an off-site server? Does your vendor have direct access to health information? Will you and your affiliates manage the health information directly? Do you allow remote access? Will patients be provided with access to health information via a portal?*

Section B: Organizational Privacy Management

Use this section to describe how you will meet your legislative requirements under the HIA. Describe your overall approach to privacy management, including organizational structure, policy management, records management, affiliate training, and privacy incident/breach response and access/correction/expressed wish request processes. This section can also help you identify any gaps in your organization's current privacy-related policies, procedures, and practices.

If you have already provided a description of your privacy management in a previous PIA and no changes are needed, you may reference the past OIPC file number for the PIA.

Resources

The Alberta Health document Responsibilities of Custodians and Health Information Act Administration Checklist provides more information and guidance. Sample forms and model letters can be found in the Alberta Health document Health Information Act Forms. The OIPC's PIA Requirements Guide also provides a list of HIA-related policies for reference (pages 34-36).

If you are implementing a new electronic medical record system, the OIPC has developed Guidance for Electronic Health Record Systems containing an assessment of system safeguards and sample practices.

You may also wish to contact your college or association for member-specific resources.

Note: You do not need to list all your organizational policies and procedures here – they will be listed and attached in **Section E – Policy & Procedures Attachments**.

1. Management Structure

[Use this space to describe how you will meet the legislative requirements.]

HIA Requirements:

*As a custodian, you have specific duties and responsibilities under the HIA (Part 6) to appropriately protect and manage health information that is in your custody and control. When working through this section, keep in mind the overarching "NHL Principles": to collect, use and disclose health information on a **need**-to-know basis, and to the **highest** degree of anonymity and in the most **limited** manner possible.*

Under Section 62 of the HIA, you must identify any affiliates who are responsible for ensuring the HIA, its regulations, and your HIA-related policies and procedures are complied with. Examples of a responsible affiliate include a dedicated privacy officer or an office manager. For more information about this duty, see Chapter 5 in the HIA Guidelines and Practices Manual.

Guiding Questions:

Describe how decisions are made about health information privacy within your practice. Include an organizational chart if you have developed one.

- *Who is responsible for establishing and managing your privacy policies? Have you designated one or more responsible affiliates? If so, describe their role as well as how, and under what circumstances, they are required to report to you.*
- *How do you resolve privacy-related issues?*

For example, how will you respond to patient complaints about privacy? How will you resolve disputes between custodians regarding the management of health information? How will you decide whether to participate in information sharing with another custodian or body such as Alberta Health, Alberta Health Services, or the Health Quality Council of Alberta? How will you decide whether to participate in research?

2. Policy Management

[Use this space to describe how you will meet your legislative requirements.]

HIA Requirements:

Under Section 63 of the HIA, you have a duty to develop policies and procedures to support the implementation of, and compliance with, the HIA's rules. As affiliates, your staff, contractors, students, etc. are responsible for following your policies and procedures.

Guiding Questions:

- *How are privacy policies developed, approved, and implemented in your clinic?*
- *How and when are privacy policies reviewed for efficiency, effectiveness, relevance to your practice, and ongoing compliance with HIA? (Reminder: the HIR requires regular review of safeguards that protect health information, including policies).*
- *How are your privacy policies communicated to staff?*
- *What do you do to ensure your affiliates are following your privacy policies?*

***Tip:** Some regulatory colleges have developed PIA-related resources to support their members. Contact your professional college to see if they have resources that can help you develop appropriate policies.*

3. Training and Awareness

[Use this space to describe how you will meet the legislative requirements.]

HIA Requirements:

Ensuring your affiliates are appropriately trained and aware of the privacy policies and procedures you have established is not only your responsibility under the HIA; it is a key element and safeguard in the management of health information.

Note that under HIA Section 62(2), any collection, use or disclosure of health information by one of your affiliates is considered a collection, use or disclosure by you, the custodian.

Guiding Questions:

- *Will you develop your own training or will your affiliates complete training through another organization?*
- *How will your affiliates (e.g., employees, contractors, students, etc.) be trained in privacy (e.g., new employee orientations, ongoing training, or awareness programs)? How often do you plan to offer training?*
- *How often do you plan to review and update your training material?*
- *How do you plan to document that someone has received privacy training?*
- *Have you established remedies for situations where an affiliate does not follow your privacy policies and procedures?*
- *Will you enter enter into an oath of confidentiality, or other type of non-disclosure agreement, with your affiliates?*

4. Incident Response

[Use this space to describe how you will meet the legislative requirements.]

HIA Requirements:

Mandatory breach reporting under the HIA came into force on August 31, 2018. Custodians have a duty to notify the Minister of Health, the Information and Privacy Commissioner of Alberta, and the affected individual of health information breaches when there is risk of harm to an individual (HIA section 60.1 and HIR section 8.1).

For more information and guidance about mandatory breach reporting, see Chapter 14: Duty to Notify of the Health Information Act Guidelines and Practices Manual and Alberta Health's Health Information Act webpage. The OIPC also provides key resources, including the OIPC Breach Report Form and Key Steps in Responding to Privacy Breaches guidance document, on the OIPC website.

Guiding Questions:

- *How do you plan to identify and manage privacy incidents? Have you developed a policy on managing privacy incidents? Your description should describe what events trigger your response plan, who is involved in the process, how you will contain a breach, how you will evaluate the risks associated with a breach, how you will notify affected parties, and how you learn from incidents to improve your privacy practices and prevent future breaches. If you have engaged the services of a vendor, be sure to describe the vendor's responsibilities.*

5. Access and Correction Requests

[Use this space to describe how you meet the legislative requirements outlined below. Address each requirement and explain how you intend to meet it to manage requests from individuals to access or correct their own health information.]

HIA Requirements:

The HIA gives Albertans the right to access their own health information (Section 7) as well as to request corrections to inaccurate information in their health record (Section 13). You must make every reasonable effort to respond to an individual's access or correction request within 30 calendar days.

Access

As a custodian, you have a duty to assist applicants and must make every reasonable effort to respond openly, accurately, and completely (Section 10). Section 11 of the HIA also sets out certain circumstances where access to health information may or must be refused. Note that an individual may give written authorization to another person to act on his/her behalf (under Section 104(1)(i)) or by using an Authorization of Representative Form found in the Alberta Health document Health Information Act Forms.

For more information and guidance, see Chapters 2 and 3 of the Health Information Act Guidelines and Practices Manual.

Correction

Individuals have the right to make a written request asking that a correction or amendment be made to their own health information. You may refuse to make a requested correction or amendment if the information is a professional opinion or observation made by a custodian, or if the record was created by a custodian other than yourself. Note that, in your response to the individual, you must either make the correction or amendment, or notify the applicant in writing of the reason for the refusal.

For more information and guidance, see Chapter 4 of the Health Information Act Guidelines and Practices Manual.

Individuals may use the Request to Correct or Amend Health Information Form found in the Alberta Health document Health Information Act Forms.

Guiding Questions:

- *Who is responsible for responding to access and correction requests?*
- *Who makes final decisions on whether to apply exceptions to an access request or whether to make corrections?*
- *How will you inform people about your decision to grant or refuse access and correction requests? Will you provide the written notice in person, or by mail? See Model Letter I in the Alberta Health document Health Information Act Forms for an example notice.*
- *Will you have an informal process for routine requests? For example, what will your process be for responding to a client who asks for a copy of recent blood-work results or prescriptions?*
- *Have you developed a process to respond to your patients' requests for information available via provincial systems, such as Alberta Netcare?*

Section C: Project Privacy Analysis

Use this section to describe how you will meet your legislative requirements. It addresses privacy topics related to your system or practice, including a list of the health information that is collected, used, or disclosed, a description of how and where the health information flows, and the sections in the HIA that authorize those flows.

Also included in this section is your approach to collection notices, consent and expressed wishes, and contracts and agreements.

1. Health Information Listing

HIA Requirements:

Use the table below to provide a list and description of the types of health information you will collect, use, or disclose. Ensure you have a defensible reason under the HIA for doing so. See HIA Sections 20, 22, 27 and 35 for more information about some commonly used legal authorities for collection, use and disclosure, but note that there are other sections in the HIA to consider as well.

Generally, if there are many data elements, consider grouping similar data together and attaching an appendix.

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

Guiding Questions:

- *What health information will be collected, used, or disclosed? For what purposes? Think about the description you provided in **Section A: Project Summary.***
- *Keep in mind the HIA requires that custodians only collect, use, and disclose the amount of health information that is essential to meet the intended purpose.*

Example Table 1

Health Information Listing Table		
Data Element	**Description**	**Purpose**
Personal Health Number (PHN)	*Unique Identifier*	*Uniquely identify patient in jurisdiction. Used to track health services.*
Gender	*E.g., Male, Female, etc.*	*Identifies patient*
Name	*Unique Identifier*	*Identifies patient*
Date of Birth		*Identifies patient*

Phone Number		*Method of contact*
Prescriptions	*A listing of medications prescribed to a patient.*	*Ensures an accurate and historical record of medications prescribed to an individual.*
Allergies	*A listing of allergies a patient has.*	*Ensures health services provided to individual are safe and appropriate.*
Vaccinations		*Supports clinical decision making and health promotion activities*

Example Table 2

Health Information Listing Table		
Registration Information	**Diagnostic, Treatment, and Care Information**	**Scheduling/Billing Information**
*Patient name**	*Family and social history*	*Appointment dates*
Address	*Past medical history*	*Appointment time*
Phone number (home)	*Immunization history*	*Reason for visit*
Date of Birth	*Medications*	*Payer*
*Personal Health Number**	*Consults*	*Amount owing*

* Unique identifier

2. Information Flow Analysis

HIA Requirements:

This section of the PIA has two required components. First, use this space to provide a description of the flow of health information for this project. Next, use the spaces below to support your description with an information flow diagram and a table that describe the purposes and legal authority for each collection, use and disclosure of health information.

As a custodian, you are responsible for ensuring you and your affiliates are collecting, using, and disclosing information appropriately. You must be able to answer questions about your business/clinic's collection, use and disclosure of health information in the event that an Albertan or the Office of the Information and Privacy Commissioner (OIPC) asks for more information.

Mapping the flow of health information in your clinic and the legal authority for those flows is an obligation and will help you ensure compliance with the HIA.

a. Information Flow Diagram

[Use this space to develop your information flow diagram.]

There is no universally accepted format for information flow diagrams. Refer to the examples on pages 33 - 36 of this document for guidance.

***Note**: Remove the Tips and Examples pages before submitting your PIA to the OIPC.*

b. Legal Authority and Purposes Table

HIA Requirements:

The HIA sets out specific, limited purposes for the collection, use, and disclosure of health information. A Legal Authority and Purposes Table documents how each flow of information is supported by a clearly defined purpose and legal authority from the HIA and any other applicable legislation (e.g., Public Health Act; Child, Youth and Family Enhancement Act, etc.).

Refer to the Information Flow Diagram you created in the last section to create your Legal Authority and Purposes Table. Each flow of information in the previous diagram should be numbered. Use the table below to describe each numbered flow, including the type of information involved, the purpose, and the legal authority for the flow.

Refer to the examples on pages 32 - 36 of this document to complete your Legal Authorities and Purposes table.

Legal Authority and Purposes Table				
Flow #	***Description***	***Type of Information***	***Purpose***	***Legal Authority (Cite specific sections of appropriate legislation)***
1				
2				
3				
4				

3. Notice

[Use this space to describe how you will meet the legislative requirements.]

HIA Requirements:

Section 22(3) of the HIA requires a notice to be provided to individuals prior to collecting health information from them. Notice can be provided in several ways, but it should allow patients adequate opportunity to review and understand the notice before their information is collected. For example, on a poster in your waiting room, written on your practice's website or patient portal, and/or provided in writing on patient registration forms or brochures.

Per HIA Section 22(3), a collection notice must include three components:

- *Why the health information is being collected.*
- *The legal authority for the collection; and*
- *The title, business address and business phone number for an individual in your clinic who can answer questions about the collection (e.g., a designated Privacy Officer).*

A sample Collection Notice can be found in the Alberta Health document Health Information Act Forms.

See Chapter 6.6.3 of the Health Information Act Guidelines and Practices Manual for more information about collection notices.

4. Consent and Expressed Wishes

[Use this space to describe how you will meet the legislative requirements to obtain consent and consider an individual's expressed wishes.]

HIA Requirements:

Consent

Sections 33, 35 to 40, 46, 47 and 53 of the HIA outline circumstances where you can disclose your client's health information without their consent, such as for the purpose of providing health services. In situations where you do not have the legal authority to disclose without consent, a sample Consent to Disclosure form that meets the requirements set out in Section 34 of the HIA can be found in the Alberta Health document Health Information Act Forms.

See Chapter 8.4 of the Health Information Act Guidelines and Practices Manual for more information about consent.

Expressed Wishes

Section 58(2) of the HIA requires custodians to consider the expressed wishes of the individual who is the subject of information, together with any other relevant factors, when making a decision relating to the disclosure of the individual's health information.

Under Section 56.4, custodians have a duty consider an individual's expressed wish with regard to how readily available their information is made via the provincial electronic health record, Alberta Netcare. An individual may express this wish through presenting any authorized custodian, with whom they have a current care relationship with, an application for Global Level Person Masking, or Masking. For more information about masking, please see the Alberta Netcare website.

***Note:** If you are an authorized custodian, please see section 5.0 of the Alberta Netcare Information Exchange Protocol for more information about your role and responsibilities in the masking process.*

- *Do you have a process to consider, decide and respond to an individual's expressed wishes about the disclosure of their health information?*
- *Does your system have the functionality to allow you to limit disclosure based on a patient's expressed wish?*

See Chapter 5.2.2 of the Health Information Act Guidelines and Practices Manual for more information.

5. Data Matching

[Use this space to describe how you will meet the legislative requirements when using health information for data matching.]

HIA Requirements:

'Data matching' is defined in Section 1(1)(g) of the HIA. Data matching means combining identifying or non-identifying health information from two or more electronic data sets without consent of the individual to create individually identifying health information, often for purposes related to data analytics and/or research.

***Note:** Keep in mind that this definition of data matching refers only to situations where combining data sets creates a new body of individually identifying health information. Data matching does not include looking an individual up in a system and/or verifying an individual's identity by cross-referencing data if no new individually identifying health information is created.*

Sections 68 to 72 of the HIA establish the rules for when and how data matching may happen, such as with two or more data sets under your own custody and control, with another custodian or non-custodian, or for research purposes. For more information about data matching rules, see Chapter 5.4 of the Health Information Act Guidelines and Practices Manual.

Guiding Questions:

- *Will you be engaging in data matching as defined in the HIA?*

- *Will you be engaging in data matching with another custodian or a non-custodian?*

If yes, provide a description and purpose.

6. Contracts and Agreements

[Use this space to describe how you will meet your legislative requirements to enter into contracts and agreements. It is best practice to provide copies of your third-party agreements. At a minimum, you should include the privacy provisions from these agreements.]

HIA Requirements:

Contracts and agreements between you and your affiliates establish the roles and responsibilities your affiliates have in performing their duties on your behalf or in providing contracted services to you, and impose limits on the collection, use and disclosure of health information by your affiliates. They will also address how your affiliates are expected to respond in the event of a breach of health information.

Note: *Information Manager Agreements are a specific type of agreement under section 66 of the HIA. An 'information manager' is a person or body that: processes, stores, retrieves, or disposes of health information; transforms health information to make it non-identifiable; or provides information management or information technology services. Section 7.2 of the HIR lists specific requirements for Information Manager Agreements. Section 8(4) of the HIR lists additional provisions that must be included in agreements with Information Managers that store, use or disclose health information outside Alberta.*

See Chapter 5.3.2 of the Health Information Act Guidelines and Practices Manual for more information about Information Manager Agreements and Appendix 4 Components for Agreement with Information Manager .

Agreements with non-affiliate service providers:

You may wish to consider entering into a non-disclosure agreement with other types of service providers who may encounter health information, such as cleaners or landlords.

Information Sharing Agreements (ISAs):

An ISA is the legal contract that defines the data stewardship rules and processes that custodians have agreed to when working in a shared patient record environment. An ISA outlines access, transfer and return of patient records, and helps guide issues pertaining to the management, security requirements, and professional responsibilities relating to the sharing of patient records.

While ISAs are not mentioned in the HIA, you may have ISAs with other members of your clinical team or with other organizations with whom you exchange health information (e.g., if you are a member of a Primary Care Network or share data with the Health Quality Council of Alberta, etc.). Some regulatory colleges and associations have developed requirements and resources to support their members. Contact your professional college or association to see if they have resources to help you navigate ISAs.

Guiding Questions:

- *Have you entered into an agreement with all your information managers that meet the requirements of the HIA?*
- *Have you considered which of your service providers may encounter health information and have entered into an appropriate non-disclosure agreement?*

7. Health Information Used, Stored or Disclosed Outside of Alberta

[Use this space to describe how you will meet the legislative requirements if health information will be used or stored outside of Alberta.]

HIA Requirements:

The HIA does not prohibit transfers of health information outside of Alberta but requires you to take specific measures to ensure the privacy and confidentiality of the information, including entering into a written agreement with the person or organization prior to the storage, use, or disclosure of the information outside of Alberta (HIR Section 8(4)).

See Chapter 5 of the Health Information Act Guidelines and Practices Manual for more information.

***Note:** if health information is being disclosed to a person outside of Alberta for the sole purpose of providing continuing treatment and care to the individual, an agreement with the recipient is not required.*

Guiding Questions:

- *Will the health information be used, stored, or disclosed outside of Alberta?*

Examples of when this might occur is if your computer system's help desk is located out of province, or if you use cloud-based data storage whose servers are located out of province.

Section D: Project Privacy Risks and Mitigation Plans

Use this section to describe the privacy risks and mitigation measures you have identified for the project. Include information about how access to health information will be controlled, how you plan to monitor compliance, and how you will periodically review the PIA and notify the OIPC about any changes.

Depending on the type and level of threats and risks to the health information involved in your system or practice, you may decide to implement several administrative, physical, and technical safeguards. Common examples of each type of safeguard include:

Administrative

- Authorized access: Access to health information (including the place or system where health information is kept) must be restricted to individuals who are authorized to handle the information to perform their duties.
- Security checks: May need to be employed to ensure that individuals in key employee positions are screened (e.g., background/record checks and taking oaths of confidentiality).
- Procedures, policies, and practices: Should be current, in writing, and available to all staff. Policies, procedures, and penalties should also be outlined in contracts for service providers.
- Training: privacy, access to information, and information security training you provide to your affiliates, including general awareness training, plus training on how to use privacy and security features in your information systems.
- Monitoring and review: conducting regular monitoring to ensure your affiliates are following your policies and procedures and reviewing your policies and procedures for on-going effectiveness.
- Sanctions: establishing sanctions that may be imposed against affiliates who breach, or attempt to breach, your administrative, technical, and physical safeguards that protect health information.

Physical

- Access to your clinic/facility, computer operating system/software, file room, etc. must be controlled to ensure that access is granted only to authorized individuals. Controls can include locked desks, cabinets, and file rooms, security systems, and appropriate mechanisms to dispose of health information.
- Ensuring your information managers have established appropriate physical security safeguards for data centres and health information storage facilities.

Technical

- Role-based access to health information systems, passwords and two-factor authentication, unique authentication, anti-malware, firewalls, intrusion detection and prevention systems, maintaining up-to-date and patched software and operating systems, system logging and access to health information logging, storing health information in encrypted form, planning for disaster recovery (e.g., regular back ups, off-site storage), and implementing policies, procedures and practices to restore and replace health information that has been damaged, lost or destroyed either accidentally or deliberately.

1. Access Controls

[Use this space to describe how you will meet your legislative requirements.]

HIA Requirements:

As per Section 60 of the HIA, you have a duty to protect health information through the use of administrative, technical and physical safeguards.

***Note:** Under the HIA, you have a duty to abide by the 'NHL' principles (Sections 57 and 58). This means you and your affiliates have a duty to only collect, use or disclose health information based on your **need** to know the information, to the **highest** degree of anonymity possible, with the most **limited** amount of information essential to achieve the intended purpose (a list of purposes for which health information can be collected, used, and disclosed can be found in Section 27).*

For more information about your duties as a custodian, including more information about safeguards, see Chapter 5 of the Health Information Act Guidelines and Practices Manual.

Guiding Questions:

- *Who will have access to health information under your custody or control that is stored electronically (e.g., in an EMR)?*
- *Who will have will have access to health information under your custody or control that is stored physically (e.g., who will have keys to filing cabinets, file rooms, etc.)?*
- *Will access be based on job role?*
- *What information will each role be granted access to? Describe why certain roles require access to health information.*
- *What type of access will be provided?*
- *How will access be terminated when an employee leaves or changes position?*

Example Table

Access Controls Table				
Position & Job Title	**User Role**	**Number of Staff in this Role**	**Type of Access**	**Description of Information this User Can Access (include examples)**
Physician	*Provide medical care to patients*	*3*	*Read, write, edit.* *Keys to file room and filing cabinets*	*Demographic information (e.g., Full name, PHN, phone number, address).* *Diagnostic, treatment, and care information*
Medical Office Assistant	*Register patients*	*2*	*Read, write, edit; Keys to file room*	*Demographic information (e.g., Full name, PHN, phone number, address)*
Office Manager	*Supervise administrative duties and employees*	*1*	*Keys to file room; Keys and security code to building*	*Demographic information (e.g., Full name, PHN, phone number, address)*

2. Privacy Risk Assessment and Mitigation Plans

HIA Requirements:

New risks to the confidentiality, integrity and availability of health information often arise over time as technology and business processes evolve.

HIA section 60 and HIR Section 8 require you to maintain administrative, technical, and physical safeguards to protect the health information that is in your custody and control, and to conduct periodic reviews of the effectiveness of your safeguards.

Use the table below to describe the risks to privacy that may occur in your setting, and the policies and procedures that you have developed to mitigate these risks. Be sure to describe the measures you are actively taking to mitigate identified risks.

See Chapter 5 of the Health Information Act Guidelines and Practices Manual for examples of safeguards.

See the OIPC document Guidance for Electronic Health Record Systems for examples of practices you can adopt to meet some of your obligations under the HIA.

Risk Mitigation Table			
Privacy Risk *What is the risk?*	**Description** *How would you describe the risk?*	**Mitigation Measures** *What are the administrative, physical, or technical controls or measures you are taking to mitigate the risk?*	**Policy Reference** *Which of your policies and procedures will help mitigate this risk?* *(Section E of this PIA template contains a listing of common policies)*
Unauthorized use of information by authorized users	*Affiliates could access and disclose personal information without appropriate authority (e.g., looking at family or friends' health information)*	*Oath of confidentiality; Role based access controls, Privacy Policies, Privacy Training, regular review of access logs, sanctions for misuse*	*E.g., Use of Information Policy; Access Controls Policy; Monitoring and Auditing Policy*
Unauthorized collection/use or disclosure of information by external parties	*Hacker gains access to clinic network or database (e.g., through hacking or phishing)*	*Firewalls in place; Staff training in recognizing phishing scams.* *Incident response procedures in place*	*E.g., Training, Awareness and Sanctions Policy; Incident Response Policy*
Loss, destruction, or loss of use of health information			
Loss of integrity of information			
Unauthorized or inappropriate collection/use or disclosure by contractor or business partner			

Other relevant privacy risks (e.g., theft or loss of mobile devices, unauthorized disclosure via wireless network, etc.)			

3. Monitoring

[Use this space to describe your plans to monitor compliance with your privacy protection measures, including a description of the process, how frequently you will apply them, and how you will review the results.]

HIA Requirements:

As a custodian, you must protect the confidentiality of the health information in your custody and control against any reasonably anticipated threats to the security, integrity, or loss of the health information, as well as its unauthorized use, disclosure, or modification (HIA Section 60).

This means you must be able to identify if/when your affiliates are collecting, using, or disclosing health information inappropriately, if an unauthorized third-party gains access to health information that is in your custody and control (e.g., through hacking or phishing), if there is a loss of records, or any other triggers that may reflect gaps or deficiencies in your privacy protection measures. This also means you must have policies in place to respond to these situations.

Your plans to monitor access and disclosure should reflect the sensitivity of the health information involved.

***Note:** A custodian must create, maintain, and review audit logs for electronic health information systems. It is best practice to ensure your electronic health record information system logs the information listed below. If a custodian is authorized to use Netcare, the custodian's electronic medical record information system must be capable of logging the information as per Section 6(1) of the Alberta Electronic Health Record Regulation. If a custodian is not authorized to use Netcare, is it still best practice and expectation of the OIPC that the electronic medical record information systems log this information.*

- *User identification and application identification associated with an access*
- *Name of user and application that performs an access*
- *Role or job functions of user who performs an access*

- *Date of an access*
- *Time of an access*
- *Actions performed by a user during an access, including without limitation, creating, viewing, editing, and deleting information*
- *Name of facility or organization at which an access is performed*
- *Display screen number or reference*
- *Personal health number of the individual in respect of whom an access is performed*
- *Name of the individual in respect of whom an access is performed*
- *Any other information required by the Minister (Note: The Minister has not stipulated anything further at this time, but custodians should be alert to changes in the future).*

Guiding Questions:

- *Who will conduct audits? How often will audit logs be reviewed? What kind of anomalies will be flagged?*
- *Have you dedicated adequate resources, time, and training to those who will conduct reviews?*
- *What are your plans for responding to anomalous incidents?*

4. PIA Compliance

[Use this space to describe how you will meet the legislative requirements.]

HIA Requirements:

As a custodian, you are obligated to ensure adequate levels of privacy protection to the health information of the clients you serve. This means ensuring compliance with the practices, policies and procedures set out in your PIA.

This also means ensuring your PIA stays up to date with any internal or external changes that affect your practice. Schedule regular PIA reviews to ensure it continues to reflect your current environment (e.g., annually). Participation in provincial eHealth initiatives is often contingent on maintaining an up-to-date PIA and policies.

It is also important to notify the OIPC when any substantial changes are made to an existing system or practice. This may involve amending an existing PIA, or simply writing a letter to the OIPC, depending on the complexity and scope of the change.

Examples of significant changes: *new user roles and permissions, new flows of information to external users, new service providers, move to new EMR/physician practice management system (PPMS), adopting Wi-Fi, remote access, mobile access, ePrescribe functionality, text or email notifications, patient portal, moved infrastructure to data centre or cloud.*

Examples of less-significant changes: *Routine upgrades and patches to EMR/PPMS, routine updates and patches to operating system, server or network, interface improvements, security patches, new custodian(s) in environment, address change, and changes to service providers who do not handle health information (e.g., change in cleaning company).*

Refer to the OIPC PIA Requirements for more guidance on PIA amendments.

Guiding Questions:

- *How often will you review this PIA?*
- *Does your new, or changed, administrative practice or information system require an update or amendment to an existing PIA?*
- *How will you ensure identified gaps in your privacy protection measures are addressed?*

Section E: Policy & Procedures Attachments

Use this section to review and attach your practice's policy documents. Your PIA will be considered incomplete if it does not include your organizational privacy policies and procedures.

1. General Privacy Policies

[Use the table below to demonstrate how you meet the legislative requirements.]

HIA Requirements:

Section 63 of the HIA requires custodians to establish policies and procedures to facilitate the implementation of the HIA within their organization. This is a requirement regardless of whether or not a PIA is required.

Attach the policies and procedures you have developed that address your obligations under the HIA. See the Office of the Information and Privacy Commissioner's PIA Requirements Guide for a description of each of the topics listed below.

Topic	Policy Description	Attachment Title(s)	Page Reference(s)
Privacy Accountability			
Access to Health Information			
Correction Requests			
Training, Awareness & Sanctions			
Collection of Health Information			
Use of Health Information			
Disclosure of Health Information			
Research			
Third Parties			
Privacy Impact Assessments			
Records Retention & Disposition			

Information Classification			
Risk Assessment			
Physical Security of Data and Equipment			
Network & Communications Security			
Access Controls			
Monitoring and Audit			
Incident Response			
Business Continuity			
Change Control			
Mandatory Breach Reporting			

2. Other Policies

Use this space to attach any other privacy policies and procedures that are relevant to this PIA. For example, if you are implementing a new EMR, attach any policies you have created specifically for it. Policies such as who will have access to it and what kinds of safeguards are in place to protect the health information held within it.

Topic	Policy Description	Attachment Title(s)	Page Reference(s)

Before You Submit Your PIA: Checklist

- ☐ Have you provided all the essential information about the current plan for your system or practice?
- ☐ Have you included all relevant documents with your PIA? Have you attached your organizational policies and procedures?
- ☐ Have you completed every section? If an item was not applicable or unavailable, have you indicated and explained why? If you leave sections in your PIA blank with no explanation, the OIPC will consider your PIA incomplete and return it to you un-reviewed.
- ☐ Have you written your PIA as clearly and concisely as possible? Have you written your PIA with your audience in mind? Have you written it in a way that can be understood by those without technical knowledge of your system or administrative practice?
- ☐ Have you avoided jargon and acronyms unless they are explained?
- ☐ Have you explained any terms, positions, and organizations that are not commonly understood?
- ☐ Although information must be comprehensive, have you made an effort to include only information that is necessary for the reader's understanding of the practice or system and its impacts?
- ☐ Have you included a PIA cover page or cover letter that includes the elements listed in the OIPC PIA Requirements?
- ☐ Has your PIA been reviewed and signed-off by the custodian(s) responsible for the custody or control of the health information described in the PIA?

Effective Information Flow Diagrams

Tips and Examples

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

Focus should be on when/how you *collect*[1] information from someone/somewhere, when/how you *use*[2] the health information within your organization, and when/how you *disclose* information to someone/somewhere else.

In your information flow diagram, you should also describe when your project uses health information that you have already collected or is already in your possession.

Use any diagram format that makes sense for your project but be sure to number each flow for easy reference. You will need to refer to each numbered flow in the legal authorities table.

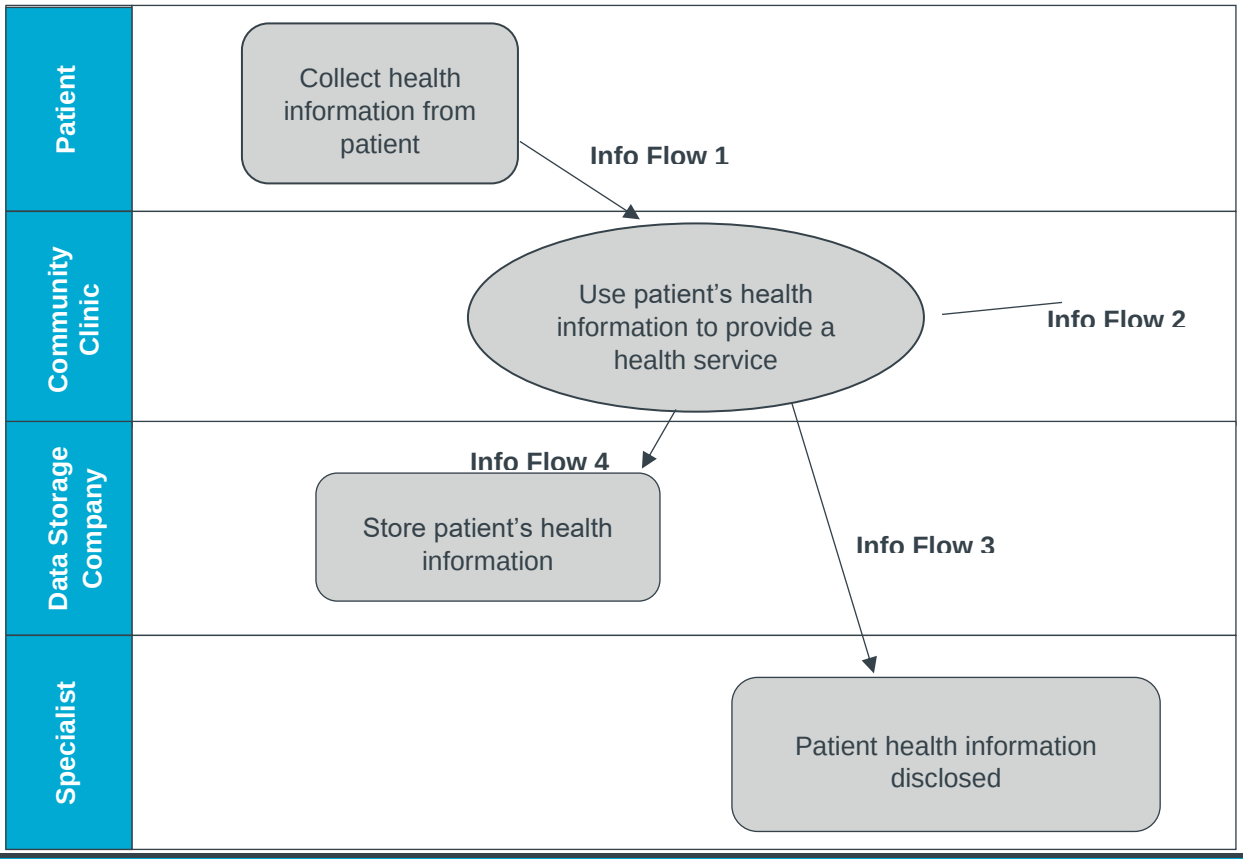
To prepare for this section, think about how health information is:

Collected	Used	Retained	Secured	Disclosed	Disposed of
by? from? how? when? where? why? authority?	by? from? when? where? why? authority?	by? how? how long? where? why?	by? how? when? where? why?	by? to? how? when? where? why? authority?	by? how? when? where? why? authority?

[1] The HIA defines 'collect' as to gather, acquire, receive, or maintain health information.

[2] The HIA defines 'use' as to apply health information for a purpose and includes reproducing the information but does not include disclosing the information.

Information Flow Diagram Example 1: Integrating a Specialist Referral Service



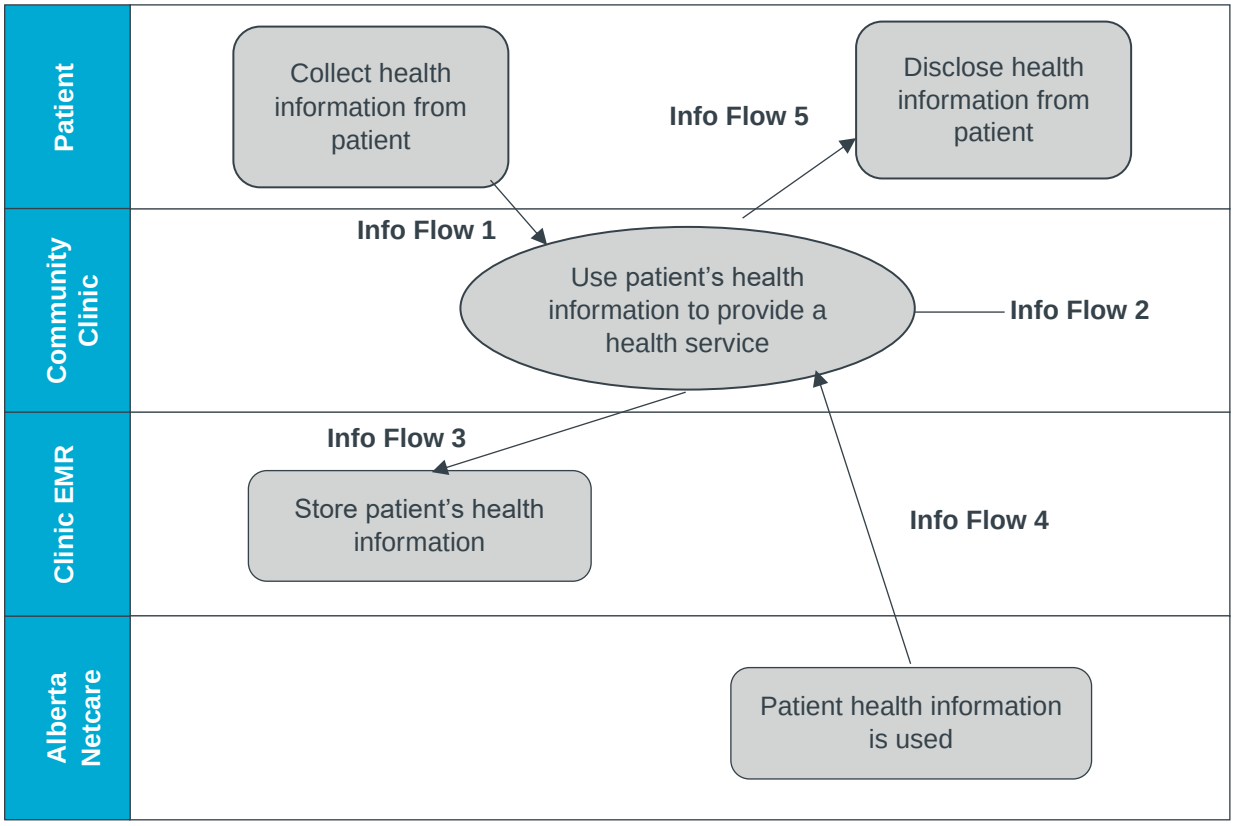
Legal Authority and Purposes Table

(To be used with Information Flow Diagram Example 1)

Flow #	Description	Type of Information	Purpose	Legal Authority
1	*Health information collected directly from patient*	*Name, personal health number, phone number, address*	*Information collected to provide health service*	*Collection - HIA 20(b); HIA 21(1)(a)*
2	*Health information used by Community Clinic*	*Name, personal health number, phone number, address*	*Information used to provide health services*	*Use - HIA 27(1)(a)*
3	*Health information is disclosed to Specialist*	*Name, personal health number, medical history*	*Referral for health services*	*Disclosure – HIA 35(1)(a), 36(a) and 27(1)(a)*
4	*Health information is provided to data storage company*	*Name, personal health number, phone number, address, diagnostic, treatment, and care information*	*Information stored for applicable retention period*	*Ss. 66(2) and (3) (see HIA section 66 and s. 7.2 of the HIR for related legal obligations when dealing with information managers)*

Information Flow Diagram Example 2:

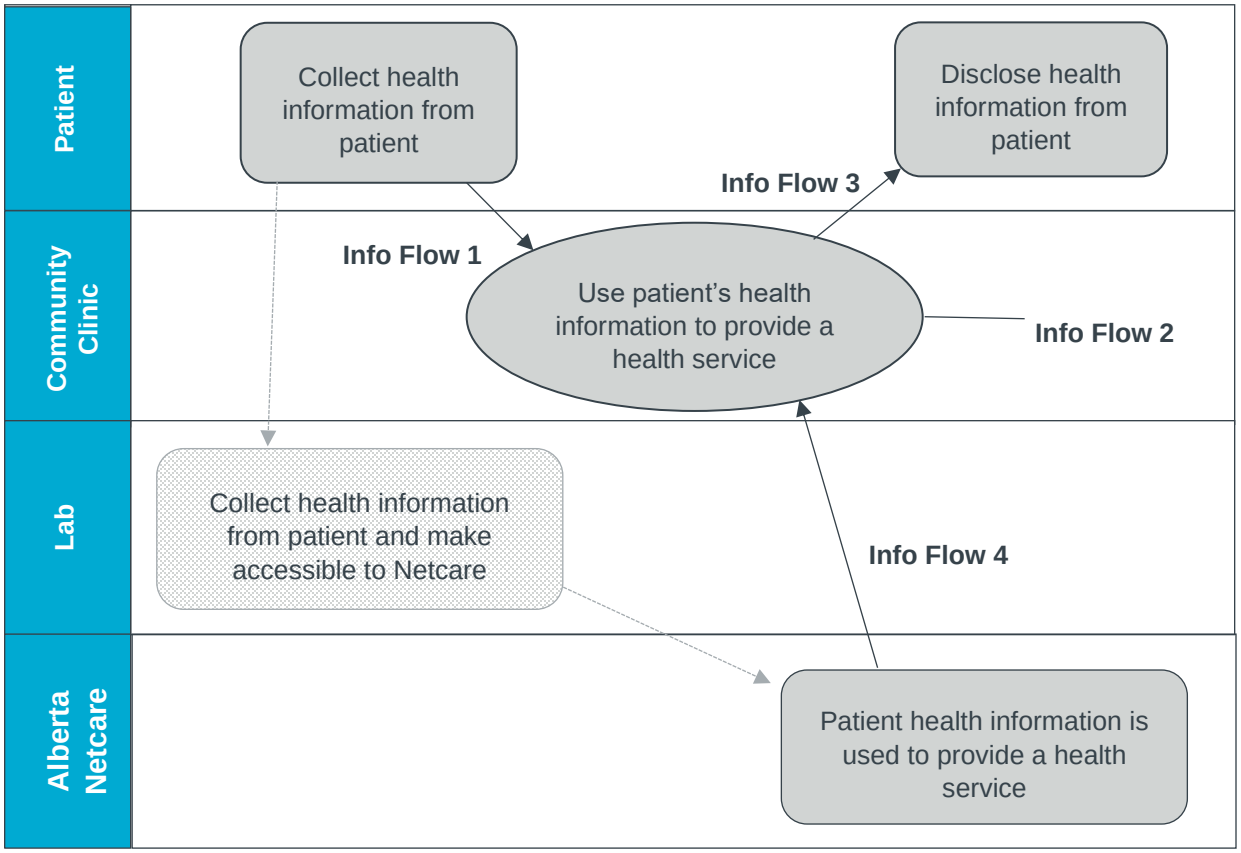
Integrating an eHealth Solution



Legal Authority and Purposes Table (To be used with Information Flow Diagram Example 2)				
Flow #	**Description**	**Type of Information**	**Purpose**	**Legal Authority**
1	*Health information collected directly from patient*	*Name, personal health number, phone number, address*	*Information collected to provide health service*	*Collection - HIA 20(b); HIA 21(1)(a)*
2	*Health information used by Community Clinic*	*Name, personal health number, phone number, address*	*Information used to provide health services*	*Use - HIA 27(1)(a)*
3	*Health information is stored in Clinic EMR*	*Name, personal health number, medical information*	*Information stored to provide health services and for internal management purposes*	*Ss. 27(1)(a) &(g) and 66(3) (see HIA section 66 and s. 7.2 of the HIR for related legal obligations when dealing with information managers)*
4	*Health information is accessed by Clinic from Alberta Netcare*	*Name, personal health number, lab results, pharmacy dispensations*	*Information used to provide health services*	*Use – HIA 56.5(1)(a) and 27(1)(a)*
5	*Health information is disclosed to patient*	*Name, personal health number, lab tests*	*Information is disclosed to the individual to provide a health service*	*Disclosure - HIA 33*

Information Flow Diagram Example 3:

Integrating a Laboratory Requisition Practice



Legal Authority and Purposes Table (To be used with Information Flow Diagram Example 3)				
Flow #	**Description**	**Type of Information**	**Purpose**	**Legal Authority**
1	*Health information collected directly from patient*	*Name, personal health number, phone number, address*	*Information collected to provide health service*	*Collection - HIA 20(b); HIA 21(1)(a)*
2	*Health information used by Community Clinic*	*Name, personal health number, phone number, address*	*Information used to provide health services*	*Use - HIA 27(1)(a)*
3	*Health information is provided to patient*	*Name, personal health number, lab tests*	*Information is disclosed to the individual to provide a health service*	*Disclosure - HIA 33*
4	*Health information is provided to Clinic from Alberta Netcare*	*Name, personal health number, lab results*	*Information used to provide health services*	*Use – HIA 56.5(1)(a) and 27(1)(a)*

Note: Information flows from the patient to the lab and from the lab to Alberta Netcare are included here to demonstrate the full lab requisition process. The clinic custodian is responsible for accounting for flows 1-4 as listed in the Legal Authority and Purposes Table.