



**Health and Community Services**

*Personal Health Information Act*  
Long Form Privacy Impact Assessment  
for [Organization Name] [Project Name]

---

Version []

Date: [date]

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Background	2
1.2	Purpose	2
1.3	Scope and Assumptions	2
1.3.1	Scope	3
1.3.2	Assumptions	3
1.4	Risk Acceptance	4
1.5	Methodology	5
1.6	Organization of Information	6
1.7	Information Gathering and Key Personnel	7
<b>2</b>	<b>Legislation and Policy Framework</b>	<b>8</b>
2.1	Privacy Legislation and Policy	8
2.1.1	Newfoundland and Labrador Personal Health Information Act	8
2.1.2	[Other Applicable] Privacy Act	8
2.1.3	Privacy Policies	9
2.2	[Organization Name] Description	9
2.2.1	Roles and Mandates	9
2.2.2	Accountability for Personal Health Information	10
2.2.3	Training and Awareness	10
<b>3</b>	<b>Operations and Environment</b>	<b>12</b>
3.1	Concept of Operations	12
3.2	Technology Description	13
3.3	Security	15
3.4	Users, Roles and Privileges	15
3.5	Physical Environment and Security	17
<b>4</b>	<b>Data Analysis</b>	<b>19</b>
4.1	Business Process	20
4.2	Personal Health Information	22
4.3	Data Flows	23
<b>5</b>	<b>Privacy Risk Assessment</b>	<b>26</b>
5.1	Principle 1 – Accountability	27
5.2	Principle 2 – Identifying Purposes	32
5.3	Principle 3 – Consent	33

---

5.4 Principle 4 – Limiting Collection	35
5.5 Principle 5 – Limiting Use, Disclosure, and Retention	36
5.6 Principle 6 – Accuracy	42
5.7 Principle 7 – Safeguards	44
5.8 Principle 8 – Openness	48
5.9 Principle 9 – Individual Access	50
5.10 Principle 10 – Challenging Compliance	55
5.11 Identification of Risk	56
<b>6 Privacy Risks and Recommendations</b>	<b>59</b>
6.1 Summary of Target Risk Achieved	60
6.2 Risk Assessment	60
6.3 Recommendations	65
<b>7 Action Plan</b>	<b>67</b>

**Annex A:** References

**Annex B:** Legislation and Policy

**Annex C:** Privacy Safeguards

---

## INTRODUCTION

### **The *Personal Health Information Act* Privacy Impact Assessment Template**

The Newfoundland and Labrador House of Assembly passed the *Personal Health Information Act (PHIA)* in the spring of 2008. PHIA applies to both public- and private-sector custodians of personal health information, and establishes rules relating to the collection, use and disclosure of such information; PHIA also provides individuals with the right to access and to request correction of their own personal health information.

A copy of PHIA is available on the Government of Newfoundland and Labrador's web site at <http://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm>. The *Personal Health Information Act* Policy Development Manual also contains a copy of PHIA.

#### ***Purposes of PHIA***

The purposes of the *Personal Health Information Act* as defined in PHIA are:

- To establish rules for the collection, use and disclosure of personal health information that protects the confidentiality of that information and the privacy of individuals with respect to that information;
- To provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in this Act;
- To provide individuals with a right to require the correction or amendment of personal health information about themselves, subject to limited and specific exceptions set out in this Act;
- To establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control;
- To provide for an independent review of decisions and resolution of complaints with respect to personal health information in the custody or control of custodians; and
- To establish measures to promote the compliance with this Act by persons having the custody or control of personal health information.

#### ***Purpose of this Long Form Privacy Impact Assessment Template***

The Department of Health and Community Services has prepared a Toolkit to help custodians understand and assess their ability to meet the Act's requirements as an organization and for specific systems or applications. The Toolkit consists of a series of checklists, documents and tools that custodians of personal health information, as identified in PHIA, can use in the implementation and interpretation of PHIA.

---

***How do you determine if a Short Form or a Long Form Privacy Impact Assessment is required?***

The Short Form Privacy Impact Assessment (PIA) is a short, straightforward and easy-to-use risk assessment tool that will help custodians identify the potential effects a process or system might have on their ability to safeguard an individual's privacy rights. The Short Form PIA is a question-and-answer assessment in table form, which sets out the requirements of PHIA.

A Short Form PIA allows a custodian to reflect on whether the collection, use and disclosure of personal health information for the activity are legally authorized. The Short Form PIA will help custodians determine when they are collecting personal health information, when they are using it and when they are disclosing it. Custodians will also identify why they are collecting, using and disclosing the information and the people who will have access to the personal health information.

Conducting a Short Form PIA is, as its name implies, a short, form of a Privacy Impact Assessment. Conducting a Short Form PIA may be appropriate in circumstances where the process, system or operation to be assessed is limited or narrow in scope and / or scale; the operation of a private, group medical practice, for example. For larger, more complex processes or systems, such as provincial information systems or multi-site operations, the Long Form Privacy Impact Assessment (see item 4 in the PHIA Risk Management Toolkit) might be a more appropriate risk management tool to employ, as the Long Form Privacy Impact Assessment provides custodians with the means to separate complex business and / or technical processes into small, manageable segments for further and easier consideration.

All Privacy Impact Assessments, regardless of their form, should be kept current, and should be updated whenever there is a significant change made to an assessed process or system, to reflect and assess any changes made.

Please see the warning and disclaimer in the introduction to the PHIA Risk Management Toolkit.

## **WHAT IS A PRIVACY IMPACT ASSESSMENT?**

A PIA is a formal risk management tool that identifies actual or potential risks to personal information posed by a proposed or existing activity or information system. A PIA also prioritizes measures that will address risks. The PIA process ensures that measures intended to protect privacy and ensure the confidentiality and security of personal health information are considered at the outset of a new program or service delivery initiative. A

---

PIA communicates how privacy is protected and personal health information kept confidential and secure from unauthorized access.

A PIA should not be considered as a record of compliance: the assessment of impact on privacy should be an open, collaborative process for arriving at privacy enhancing solutions. Risks that may not have emerged during planning can be discussed and solutions identified before they become problems.

### ***When Should a Custodian Conduct a PIA?***

A PIA is desirable when addressing risk to personal health information, including the when there are potential risks from one of the following:

- A new technology or the convergence of existing technologies;
- The use of known privacy-intrusive technology in new circumstances;
- The use of information technology that the custodian is using but which may not support privacy and security best practices; and
- A new project or from changed information handling practices that may affect privacy.

In addition, custodians can assess the impact of changes to collection, use or disclosure by conducting a PIA. Custodians trying to decide whether or not to conduct a PIA should complete the Preliminary Privacy Impact Assessment (PPIA) questionnaire, which is also part of the PHIA Risk Management Toolkit.

### ***How does a Custodian benefit from a PIA?***

PHIA does not require that custodians prepare a PIA but a PIA helps custodians to meet the requirements of PHIA:

- A PIA organizes information and analysis logically, which supports informed discussions about risk and how to address it.
- Decision makers will understand the risks that may be associated with a proposed system or program and will be able to make supportable decisions about personal health information.
- Custodians can address risk to personal health information once they have identified and quantified risks.
- A PIA represents the custodian's due diligence with regard to appropriate safeguarding of personal health information.
- A PIA provides the starting point for assessing the impact of change to operations, systems and programs already assessed; it can also be used for reviewing or auditing safeguards throughout the life cycle of operations, systems and programs.

- Engaging managers and employees during the conduct of the PIA and communicating its results promote understanding risk and how to safeguard personal health information.

### ***Organization of this PIA Template***

The PIA template provides a methodology and instructions for conducting a PIA. Instructions in the template itself are embedded in text boxes, which the custodian deletes when the PIA is complete.

Each set of embedded instructions in the PIA template starts with this symbol:



### **CONCEPTS**

Custodians should understand the concepts used in this template prior to conducting a PIA. The concepts are defined in the table below:

Concept	Description
Risk	<p>For the purposes of the PIA, risk is defined as the combination of <b>likelihood</b> that an adverse event will happen and the magnitude of the <b>impact</b> of the event. The impact can be on the custodian, the owner of the personal health information or both. Note that there is no zero rating for risk: risk cannot be completely eliminated.</p> <p>The PIA template <b>quantifies</b> risk as follows:</p> <p><b>Low</b> – There is a possibility that a risk will materialize but there are mitigating factors;</p> <p><b>Moderate</b> – There is a strong possibility that a risk will materialize if no corrective measures are taken; and</p> <p><b>High</b> – There is a near certainty that the risk will materialize if no corrective measures are taken.</p> <p>Examples of risk to personal health information include the following:</p>

	<ul style="list-style-type: none"> <li>○ Disclosure without consent;</li> <li>○ Unauthorized access;</li> <li>○ Errors and data corruption;</li> <li>○ Failure to provide information about uses on collection of personal health information;</li> <li>○ Unavailability of personal health information when needed;</li> <li>○ Failure to obtain knowledgeable consent;</li> <li>○ Use of personal health information for purposes other than those for which the information was collected;</li> <li>○ Disclosure outside of the circle of care;</li> <li>○ Failure to notify persons whose personal health information has been compromised;</li> <li>○ Failure to provide access to personal health information as required under PHIA;</li> <li>○ Failure to ensure that custodial employees understand all aspects of organizational privacy practices; or</li> <li>○ Failure to correct personal health information in a timely manner.</li> </ul>
Risk management	<p>Once risks are identified, managing risk involves choice. Risk decision choices include the following:</p> <ul style="list-style-type: none"> <li>○ <b>Avoid</b> - The level of risk may be reduced by removing the specific risk cause;</li> <li>○ <b>Transfer</b> – The level of risk may be reduced by moving the accountability for the risk to another entity, e.g. potentially some risk items could be borne by other stakeholders;</li> <li>○ <b>Reduce</b> – The level of risk may be reduced by choosing to implement additional privacy safeguards; and</li> <li>○ <b>Accept</b> – The level of risk may be accepted by reviewing and understanding the risk without implementing recommendations; this choice is unlikely for personal health information.</li> </ul>
Residual risk	The risk that remains after the implementation of all privacy safeguards, including recommended safeguards.
Target risk	The overall level of residual risk to personal health information that the custodian aims to achieve.



Threat and risk assessment	The systematic assessment of security threats, vulnerabilities and risk to operations, systems or programs and recommendations for addressing risk. Normally, threat and risk assessments address personnel, physical, information technology and administrative security. The PHIA Policy Development Manual includes guidance about security best practices.
Privacy safeguard	Any measure that the custodian uses to make sure that personal health information is protected throughout its life cycle, as required by the <i>Personal Health Information Act</i> . A privacy safeguard may be a policy, procedure, process, agreement, training or any other measure or combination of measures that can effectively reduce risk that the custodian's operations, system or program will inappropriately collect, use, disclose, retain or otherwise mismanage personal health information.
Personal health information	<p>As defined in the Personal Health Information Act:</p> <p>Personal health information means "identifying information in oral or recorded form about an individual that relates to:</p> <ul style="list-style-type: none"> <li>(a) the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family;</li> <li>(b) the provision of health care to the individual, including information respecting the person providing the health care; the name, business title, address and telephone number; licence number; and profession, job classification and employment status.</li> <li>(c) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;</li> <li>(d) registration information;</li> <li>(e) payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;</li> <li>(f) an individual's entitlement to benefits under or participation in a health care program or service;</li> <li>(g) information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;</li> <li>(h) a drug as defined in the <i>Pharmacy Act</i>, a health care aid, device,</li> </ul>

	<p>product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or</p> <p>(i) the identity of a person referred to in Section 7 of the <i>Personal Health Information Act</i>.</p>
Custodian	<p>As defined in the Personal Health Information Act:</p> <p>“...a person described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with the performance of the person's powers or duties or the work described in that paragraph:</p> <p>(a) an authority;</p> <p>(b) a board, council, committee, commission, corporation or agency established by an authority;</p> <p>(c) a department created under the Executive Council Act , or a branch of the executive government of the province, when engaged in a function related to the delivery or administration of health care in the province;</p> <p>(d) the minister, where the context so requires;</p> <p>(e) a health care professional, when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;</p> <p>(f) a health care provider;</p> <p>(g) a person who operates</p> <ul style="list-style-type: none"> <li>(i) a health care facility,</li> <li>(ii) a licensed pharmacy as defined in the <i>Pharmacy Act</i> ,</li> <li>(iii) an ambulance service, or</li> <li>(iv) a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider;</li> </ul> <p>(h) the Provincial Public Health Laboratory;</p> <p>(i) the Centre for Health Information;</p> <p>(j) with respect to Memorial University of Newfoundland, the Faculty of Medicine, the School of Nursing, the School of Pharmacy and the School of Human Kinetics and Recreation;</p> <p>(k) the Centre for Nursing Studies;</p> <p>(l) the Western Regional School of Nursing;</p> <p>(m) a person who, as a result of the bankruptcy or insolvency of the custodian, obtains complete custody or control of a record of personal health information, held by the custodian;</p> <p>(n) a rights advisor under the Mental Health Care and Treatment Act ;</p>

	(o) the Workplace Health, Safety and Compensation Commission; and (p) a person designated as the custodian in the regulations.
--	---

## PIA METHODOLOGY

The Methodology used in this PIA template is a risk management methodology. It consists of five steps, starting with contextual information and drilling down to the details of the personal health information and analysis of every action, process or procedure that affects it.

**Step One** is to establish the requirements that the custodian must meet as set out in legislation and policy – the context for undertaking the PIA. It includes a description of how the custodian has established internal controls and oversight for meeting those requirements throughout the personal health information’s life cycle. Section 2 of this template, Legislation and Policy Framework, describes this step more fully.

**Step Two** is to describe operations and the environment, including technology, the individuals that have access to personal health information, and the physical environment. Security safeguards implementation should be included in the descriptions; if there is a threat and risk assessment, its results and recommendations are summarized here. Section 4, Operations and Environment, describes this step more fully.

**Step Three** is to account for personal health information in detail. This includes a description of all personal health information and its life cycle from a business process point of view, and a detailed description of each process that has an impact on the personal health information. Section 4 of this template, Data Analysis, describes this step more fully.

**Step Four** is the privacy risk assessment. It uses the list of privacy safeguards in Annex C, matches them to the requirements they address, to assess whether or not risk is reduced to the target risk. This Section identifies where the target risk is met as well as gaps. By completing this Section, the custodian will have identified potential and actual weaknesses in privacy safeguards. Section 5 of this template, the Privacy Assessment, describes this step more fully.

**At each step**, the custodian identifies processes, procedures, policies and standards, or technologies that are planned or in place for safeguarding personal health information; these are called privacy safeguards. Annex C, Privacy Safeguards, provides further information about privacy safeguards.

---

The fourth step completes the assessment of the impact of operations, a system or a program on personal health information.

**Step Five** is the custodian's response to the assessment. The response consists of two parts:

**Response Part One:** The custodian examines the gaps in privacy safeguards, rates the risk associated with each one and recommends additional privacy safeguards that will reduce risk to the target risk level. Section 6 of this template describes this part fully.

**Response Part Two:** The custodian prepares an Action Plan that identifies how and when the custodian will implement the additional recommended privacy safeguards. Section 7 of this template describes this part fully.

## ORGANIZATION OF THE PRIVACY IMPACT ASSESSMENT

The organization of the PIA aligns with the PIA methodology. The PIA consists of an executive summary and seven sections, which are listed and described below. Annexes provide supporting details. The PIA report starts with introductory material to establish what the PIA will assess – organizational operations, an information technology system, a program – and the legislation and organizational policies that apply to the assessment. The PIA then uses detailed information and analyses to arrive at conclusions about risk. The last two sections – privacy risks and recommendations and an action plan – constitute the custodian's response to the risk assessment.

**Executive Summary:** The executive summary briefly describes the operations, system or program being assessed and highlights the risks identified and the recommendations for reducing risk and the action plan. It should be written for non-program and non-technical audiences. It is normally completed when the PIA is finished.

**Section 1:** The Introduction summarizes the background for the project; the purpose, scope and assumptions; the target risk, methodology and resources. **Annex A** lists resources consulted.

**Section 2:** The Legislation and Policy Framework captures information from step one in the methodology: it describes the legal and policy environment for safeguarding personal health information and organizational or project accountability. **Annex B** lists applicable legislation and policy.

**Section 3:** The Operations and Environment captures information from step two in the methodology: it contains an overview of the [Project Name] system, its technology and

---

architecture, and its operation. It may refer to the threat and risk assessment if one has been undertaken.

**Section 4:** The Data Analysis captures information from step three in the methodology: it is an overview of the business processes associated with the custodian's operations, system or program; a detailed inventory of the personal health information to which the [Project Name] system will potentially have access; and an analysis of the flow of personal health information for each process.

**Section 5:** The Privacy Risk Assessment captures information from step four in the methodology: it assesses the privacy safeguards and identifies gaps in privacy safeguards.

The analysis in Section 5 is supported by detailed information in **Annex C**, Privacy Safeguards, which lists existing and planned privacy safeguards.

**Section 6:** The Privacy Risks and Recommendations section identifies risk and recommends privacy safeguards that will address risk.

**Section 7:** The Action Plan contains a plan for the implementation of the recommendations listed in Section 7. This section includes a mechanism for the custodian to accept the recommendations.

#### PREPARATION TIPS

The tips listed below will help the custodian to prepare a thorough PIA:

**Assemble a team:** Even if an outside resource conducts the PIA, internal resources will need to contribute information. Internal resources can include planners, business managers, records managers, information technology experts, and partners and third party service providers.

**Assemble reference materials:** Examine documents that outline business plans, requirements and all other aspects of the operations, system or program being assessed; and conduct interviews and focus groups as required.

**Prepare a PIA plan:** Identify deliverables and milestones for measuring progress and reporting.

**Use a collaborative approach:** Soliciting the input of managers and employees will help them understand and buy into the PIA process. Use organizational communications tools to advertise the PIA process, its progress and the action plan.

**Brief executives:** Organizational executives should understand the PIA process and its potential outcomes.

---

**Identify resources and limitations** that may affect the implementation of recommendations. Doing this early will make an action plan realistic, which increases its acceptability.

### MAINTAINING THE PIA

The PIA is not a static document. The custodian should use it to confirm that organizational policy, practices and processes continue to protect personal health information: the PIA is the starting point for review and audit of personal health information risk management.

A privacy audit should be conducted to ensure that all recommendations set out in the action plan are implemented.

The PIA should be reviewed and its accuracy confirmed under the following circumstances:

- Change in concept of operation or business processes;
- Change in the collection, use or disclosure of personal health information;
- Change in legislation or regulation or in the legislated or regulator requirements of a partner;
- Information about new threats or threat capabilities that may require upgrades to security safeguards and practices;
- Acquisition of new software, hardware or other changes to technology infrastructure;
- Switch to a new service provider or change to a partnership arrangement; and
- Any change in the organization, system or technology infrastructure that could also affect privacy or security safeguards.

### *Other Uses of the PIA*

The custodian can use the PIA to communicate with provincial and public health authorities about how it safeguards personal health information. The custodian can also use the PIA or the executive summary of the PIA to communicate with the public or with persons receiving health care.

---

## GLOSSARY

Section 1 of the PHIA Policy Development Manual lists and defines the terms used in PHIA. PHIA is quoted extensively in Section 5 of this template. The glossary is therefore repeated here for convenience.

**Affirmation** is a solemn declaration made by those who object to taking an oath to avoid the religious implications of an oath. An affirmation has the same legal effect as an oath.

**Anonymized Information** is information which has been irrevocably stripped of identifiers, with no means to allow future linkages.

**Anonymous Information** is information that has never had identifiers associated with it (e.g., anonymous surveys).

**Circle of care** refers to the following individuals / entities when they are participating in activities related to the provision of care to the individual who is the subject of the personal health information:

- a health care professional, when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;
- a health care provider;
- a person who operates:
  - a health care facility,
  - a licensed pharmacy as defined in the *Pharmacy Act*,
  - an ambulance service, or
  - a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider

**Collection** in relation to personal health information means to gather, acquire, receive or obtain the information by any means from any source.

**Compliance**, for the purpose of this policy document, means conforming to a specification or policy, standard or law, such as the *Personal Health Information Act* that has been clearly defined.

**Commissioner** means the Information and Privacy Commissioner appointed under the *Access to Information and Protection of Privacy Act*.

**Complainant** means an individual requesting a review by the commissioner of a denial by the custodian of a request for access or correction; or

---

an alleged breach of a provision of this Act or the regulations.

**Confidentiality** means an obligation to keep an individual's personal health information private, ensuring that only those authorized have access to the information.

**Consent directive**, for the purpose of this document, is an instruction given by an individual or by their representative to the custodian or their representative as to how the individual's personal health information may be collected, used or disclosed.

**Contact Person(s)** are individuals appointed by the custodian to perform specific functions on behalf of the custodian.

**Custodian** means a person who has custody or control of personal health information as a result of or in connection with the performance of the person's powers or duties or work, as defined in greater detail in Section 4 of the *Personal Health Information Act*.

**Database** is an integrated collection of logically related records or files consolidated into a common pool that provides data for one or more uses.

**De-identified/coded Information** is information created when identifiers are removed and replaced with a code. Depending on access to the code, it may be possible to re-identify specific research participants (e.g., participant are assigned a code name and the principal researcher retains a list that links the code name with the particular individual's actual name so data can be re-linked if necessary.) Researchers who have access to the code and the data have identifiable information.

**Designate** is an individual that the custodian formally nominates as being the person responsible for making decisions required under the *Personal Health Information Act*.

**Disclosure**, in relation to personal health information in the custody or control of the custodian, means to make the information available or to release it, but does not include a use of the information.

**Express consent** is consent that is obtained as a result of an individual positively indicating, either verbally or in writing that they agree to a stated purpose.

**Good faith** means a sincere and reasonably-held belief that an action was proper and lawful, or a motive to act in a proper and lawful way, without malice or intent to defraud.

**Identifying Information** is information that identifies a specific research participant through direct identifiers (e.g., name, address, social insurance number or personal health number).



---

**Identifiable Information** is information that could be used to re-identify a subject through a combination of indirect identifiers (e.g., date of birth, place of residence or unique personal characteristics) using reasonably foreseeable means.

**Implied consent** is consent that may be reasonably inferred from signs, actions, or facts, or by inaction or silence of an individual.

**Information Manager** is a person or organization other than an employee of the custodian that processes, retrieves, stores or disposes of personal health information for the custodian, or provides information management or information technology services to the custodian

**Indirect collection** in relation to personal health information means to collect personal health information about an individual from a source other than the individual to whom the information pertains.

**Limited consent** describes a situation wherein an individual places a condition or restriction on their consent to the collection, use or disclosure of their personal health information by the custodian. Such limitations may include:

- Controlling the collection, use or disclosure of a particular item of information;
- Controlling the use or disclosure of their personal health information to a particular health professional or class of health professionals;
- Controlling the use or disclosure of their entire personal health information record that is in the control of the custodian.

**Oath** is either a promise or a statement of fact calling upon something or someone that the oath maker considers sacred, usually God, as a witness to the binding nature of the promise or the statement.

**Person** means any natural person (i.e., an individual) and also includes a board, commission, tribunal, partnership, association, organization or other entity.

**Privacy** means the right of an individual to control the collection, use, and disclosure of personal information about themselves.

**Registry**, in the context of health care, is a population-specific listing of persons having a condition that has significance to the overall health and well-being of a particular population.

**Relative** is a person connected with another by blood or affinity. For this purpose, the definition of relative is consistent with the *Advance Health Care Directives Act* and is a

---

person's spouse, children, parents, siblings, grandchildren, grandparents, uncles and aunts, nephews or nieces or other related individual.

**Successor** for the purpose of this document is defined as the entity that will assume the responsibilities of the custodian upon the incumbent custodian's resignation of responsibilities under the *Personal Health Information Act*.

**Use**, in relation to personal health information in the custody or control of the custodian, means to handle or deal with the information or to apply the information for a purpose and includes reproducing the information, but does not include a disclosure of the information.

**Wilful** means deliberate.

## Executive Summary



*The **Executive Summary** is for non-program and non-technical audiences. The custodian uses it to summarize briefly the operations, system or program being assessed for its impact on personal health information, the identified risk to personal health information, the recommendations for reducing risk and the action plan.*

*The custodian writes the Executive Summary when the privacy impact assessment is complete.*

This report assesses privacy safeguards for personal health information by using the Government of Newfoundland and Labrador Health Privacy Impact Assessment methodology to examine the effectiveness of health information protection practices and risk management for [Organization Name] [Project Name].

The privacy analysis concludes that <Insert list of principles fully addressed from Section 6.1 and a summary of risk identification from Section 5.11.>

The recommended privacy safeguards are intended to strengthen existing and planned privacy safeguards as follows:



*The custodian can insert Table 7, Summary of Privacy Safeguards Recommendations from Section 6.3.*

[Organization Name] can mitigate privacy risks to the target acceptable risk level of **Low** by strengthening existing and planned privacy safeguards with the recommended privacy safeguards, which are described in detail in Annex C to this report. The recommended safeguards will be implemented in accordance with the action plan by <Insert Date>.



A **Privacy Impact Assessment (PIA)** is a formal risk management tool that identifies actual or potential effects of an activity, a proposal, a system or an organization's operations on personal information. The PIA also identifies how the custodian plans to mitigate risks to personal information.

This **PIA template** focuses on the personal health information that the custodian collects, uses, discloses, or retains in the course of providing health or health-related services, as defined in the Personal Health Information Act. **It is intended as a guide: the custodian should adjust and tailor contents as necessary.**

Using this PIA template helps the custodian and responsible managers to analyze health privacy issues thoroughly and to understand and address risks associated with proposed or existing operations, information systems, or programs. The PIA documents an organization's guardianship of personal health information and is a credible information source regarding how obligations under the Personal Health Information Act (PHIA) are met.

This template is organized into seven chapters, each of which includes essential information and analysis. Embedded text is designed to guide custodians regarding the steps to take when conducting a PIA, and includes content suggestions and examples. **Custodians should delete the embedded text when they have completed the PIA.**

## 1 INTRODUCTION



The **Introduction** sets the stage for the PIA by identifying the organizational operations, system or program being assessed and by briefly describing the PIA's purpose and scope. The information in the introduction helps internal and external stakeholders to understand what the PIA applies to and helps to focus the PIA team. The introduction can state assumptions, describe the methodology and organization, identify resources, and define the terms used in the PIA.

The organization of the Introduction is suggested below, including sample text and additional explanations.

This document describes the health Privacy Impact Assessment (PIA) conducted for the [Organization Name] [Project Name].

## 1.1 BACKGROUND



*The **Background** highlights the operations, system or program and its business purpose in a few short sentences. This is the first opportunity for the custodian to identify what is being assessed for its impact on personal health information.*

The business purpose of [Project Name] is to...<Insert Background Information>.

## 1.2 PURPOSE



*The **Purpose** describes why the PIA is being undertaken. Custodians use the PIA to identify risks and to decide how to address risks. This means that custodians can make decisions regarding risk and risk mitigation with complete information about the personal health information affected by a system or program.*

*The **privacy safeguards** referred to below include measures that the custodian uses to make sure that personal health information is protected throughout its life cycle, as required by the Personal Health Information Act. The privacy safeguards may consist of policies, procedures, processes, agreements, training or any other measure or combination of measures that can effectively reduce risk that the custodian's operations, system or program will inappropriately collect, use, disclose, retain or otherwise mismanage personal health information.*

The purpose of this PIA is to provide business and technology managers with information that supports informed risk management decisions relating to personal health information in the [Project Name] system. The PIA identifies how personal health information is safeguarded and recommends privacy safeguards that strengthen existing and planned privacy safeguards.

## 1.3 SCOPE AND ASSUMPTIONS



*The **Scope and Assumptions** text describes what is included in the PIA, what is excluded from the PIA and the assumptions that govern the PIA. It is a way to ensure that managers and other users of the PIA report understand what the PIA is assessing and what is excluded from the assessment.*

### 1.3.1 SCOPE



The **Scope** identifies the boundaries of the PIA. The description of what is excluded can name specific systems, programs or organizations that may be connected to the custodian's operations, system or program. It is important to be clear about what is "in scope" and what is "out of scope" so that anyone who reads or uses the PIA is focussed accurately. This will help them to understand not only what the PIA encompasses, but the limits of the analysis and recommendations later in the PIA.

The focus of the PIA is the personal health information of <patients, etc> that will reside in [Project Name].

It describes the following:

- The personal health information in [Organization Name] [Project Name] applications: <Insert Application Names>; and
- The assessment will be limited to <Insert boundary description>.

Analysis of personal health information contained in <Insert System Names> systems is not in scope.

### 1.3.2 ASSUMPTIONS



**Assumptions** include anything that, if changed, can affect the outcome of the analysis, such as changes to system architecture or to partnership agreements. The assumptions should be stated as early as possible so that those who consult the PIA report understand any limitations or qualifications on the accuracy or completeness of data.

The PIA is based on...<Insert where assumptions came from, e.g. interviews, documentation, etc>. The following assumptions have been made for this PIA:

- <Insert assumptions>
- 
- 
-

## 1.4 RISK ACCEPTANCE



*This Section identifies the custodian's **overall target risk** as defined below. The custodian's risk tolerance level provides the PIA team with direction regarding the level of risk that is acceptable to the custodian. The identification of risk acceptance is an executive decision as it establishes the organization's tolerance for risk. Definitions from the introduction to this PIA template are repeated below for convenience. Custodians can insert this text if desired.*

***Target Risk** is the overall level of residual risk to personal health information that the custodian aims to achieve. Qualitative risk levels are useful to describe the level of risk that is acceptable to the custodian and to the owners of personal health information. This Section defines **Low, Moderate or High** risk.*

***Risk** is the combination of the likelihood that an adverse event will happen and the seriousness of the impact of the event. The impact can be on the custodian, the owner of the personal health information or both.*

***Residual Risk** is defined as the risk that remains following the application of privacy safeguards.*

*The Target Risk is normally Low, although there may be circumstances when a higher level of risk is acceptable in some areas. Executive level management should determine the target level of risk.*

***Examples of risk to personal health information** include the following:*

- Disclosure without consent;
  - Unauthorized access;
  - Errors and data corruption;
  - Failure to provide information about uses on collection of personal health information;
  - Unavailability of personal health information when needed;
  - Failure to obtain knowledgeable consent;
  - Unauthorized use;
  - Disclosure outside of the circle of care;
  - Failure to notify persons whose personal health information has been compromised;
- or*
- Failure to provide access to personal health information as required under PHIA.

The overall target risk is **Low**. This PIA uses the following risk ratings:

- **Low** – There is a possibility that a risk will materialize but there are mitigating factors;
- **Moderate** – There is a strong possibility that a risk will materialize if no corrective measures are taken; and
- **High** – There is a near certainty that the risk will materialize if no corrective measures are taken.

Setting the target risk level at **Low** indicates that to the extent that it is feasible, the exposure of personal health information to risk will be kept to a minimum.

## 1.5 METHODOLOGY



The **Methodology** explains the risk management approach used for safeguarding personal health information. It is included to promote reader comprehension of the concepts and the steps taken to assess and address risk to personal health information.

The methodology description from the introduction to this PIA template is repeated below for convenience. Custodians can tailor it as required:

The **Methodology** used in this PIA consists of five steps. Each step builds on its predecessor, starting with context and drilling down to the details of the personal health information and every element that affects it.

**Step One** establishes the requirements that <Name of Organization, System or Program> must meet as set out in legislation and policy – the context for undertaking the PIA. It includes a description of how <Name of Organization, System or Program> has established internal controls and oversight for meeting those requirements throughout the personal health information's life cycle.

**Step Two** describes operations and the environment, including the technology architecture, the individuals that have access to personal health information, and the physical environment. Security safeguards implementation should be included in the descriptions; if there is a threat and risk assessment, its results and recommendations are summarized here.

**Step Three** accounts for personal health information in detail. This includes a description of all personal health information and its life cycle from a business process point of view, and a detailed description of each process that has an impact on the personal health information.

**Step Four** assesses risk to personal health information. The custodian uses the list of privacy safeguards in Annex C, matches them to the requirements they address, and assesses whether or not risk is reduced to the target risk. This Section identifies where the



target risk is met as well as gaps in privacy safeguards. By completing this Section, the custodian will have identified potential and actual weaknesses in privacy safeguards. Section 5 of this template, the Privacy Assessment, describes this step more fully.

At each step <Name of Organization, System or Program> can identify the processes, procedures, policies and standards, or technologies that are planned or in place for safeguarding personal health information; these are called privacy safeguards. Annex C, Privacy Safeguards, provides further information about privacy safeguards.

The fourth step completes the assessment of the impact of operations, a system or a program on personal health information.

**Step Five** is the <Name of Organization, System or Program> response to the assessment. The response consists of two parts:

**Response Part One:** <Name of Organization, System or Program> examines the gaps in privacy safeguards, rates the risk associated with each one and recommends additional privacy safeguards or other methods that will reduce risk to the target risk level.

**Response Part Two:** <Name of Organization, System or Program> prepares an Action Plan that identifies how and when the custodian will implement the additional recommended privacy safeguards.

## 1.6 ORGANIZATION OF INFORMATION



The custodian can describe how information is organized to help guide readers or users of the PIA through the document. It includes more than just the table of contents: it should describe, briefly, each Section and how it supports the methodology.

The description of PIA organization from the introduction to this PIA is repeated below for convenience. It can be tailored to fit the information in the PIA.

**Executive Summary:** The executive summary briefly describes the operations, system or program being assessed and highlights the risks identified and the recommendations for reducing risk and the action plan. It should be written for non-program and non-technical audiences. It is normally completed when the PIA is finished.

**Section 1:** The Introduction summarizes the background for the [Project Name] project; the purpose, scope and assumptions; the target risk; methodology; and resources. **Annex A** lists resources consulted.

**Section 2:** The *Legislation and Policy Framework* documents information from step one in the methodology: it describes the legal and policy environment for safeguarding personal health information and organizational or project accountability. **Annex B** lists applicable legislation and policy.

**Section 3:** The *Operations and Environment* documents step two in the methodology: it contains an overview of the [Project Name] system, its technology and architecture, and its operation. It may refer to the threat and risk assessment if one has been undertaken.

**Section 4:** The *Data Analysis* documents step three in the methodology: it is an overview of the business processes associated with the custodian's operations, system or program; a detailed inventory of the personal health information to which the [Project Name] system will potentially have access; and an analysis of the flow of personal health information for each process.

**Section 5:** The *Privacy Risk Assessment* documents step four in the methodology: it assesses the privacy safeguards and identifies gaps in privacy safeguards. The analysis in Section 5 is supported by detailed information in **Annex C, Privacy Safeguards**, which lists existing and planned privacy safeguards.

**Section 6:** The *Privacy Risks and Recommendations* section identifies risk and recommends privacy safeguards that will address risk.

**Section 7:** The *Action Plan* is a plan for the implementation of the recommendations listed in Section 7. This section includes a mechanism for the custodian to accept the recommendations.

## 1.7 INFORMATION GATHERING AND KEY PERSONNEL



**Information Gathering and Key Personnel** provides an overview of the resources that contributed to the PIA through interviews, group sessions and documentation. Account for both internal and external resources so that the completeness of information and consultations is clearly documented. List details of resources and documentation in Annex A.

Annex A lists documents and individuals consulted in the preparation of this PIA.

## 2 LEGISLATION AND POLICY FRAMEWORK



*The **Legislation and Policy Framework Section** is the foundation for the analysis and assessments in Sections 3 to 6 inclusive: it is the first step in assessing risks to personal health information. First, it describes the personal health information legislation and privacy policy requirements that apply to the custodian and then it describes the custodian's internal policy and reporting arrangements for measuring how well it meets those requirements.*

*By the end of this step, the custodian will have summarized the requirements for protecting personal health information and organizational policy and accountability for safeguarding personal health information.*

Annex B lists relevant legislation, regulation and policy.

### 2.1 PRIVACY LEGISLATION AND POLICY



***Privacy Legislation and Policy** sub-section establishes the starting point for the requirements that the custodian's operations, system or program must meet. This Section lists and briefly describes applicable privacy legislation and policy, including PHIA. The PHIA Policy Development Manual contains guidance for custodians as they develop policies and procedures.*

#### 2.1.1 NEWFOUNDLAND AND LABRADOR PERSONAL HEALTH INFORMATION ACT

The provincial *Personal Health Information Act* (PHIA) governs the collection, use and disclosure of personal health information by custodians identified under the Act, irrespective of whether the information is dealt with in the public or private sectors or for commercial or non-commercial activities.

#### 2.1.2 [OTHER APPLICABLE] PRIVACY LEGISLATION



*The custodian can describe **applicable privacy legislation** of other provinces or countries. If jurisdictions other than Newfoundland and Labrador will participate in the custodian's operations, system or program, this section can describe the legislation from that jurisdiction, if it applies. It is important to document any requirements arising from multiple jurisdictions so that the PIA is complete, including those arising from formal agreements.*

*The custodian may wish to consult with the Department of Health and Community Services or with corporate legal counsel if organizations in other provinces or countries are involved.*

### 2.1.3 PRIVACY POLICIES



*The custodian can refer to the **PHIA Policy Development Manual**, which contains sample policy and procedure language that custodians may wish to make use of in developing or updating their own policies.*

## 2.2 [ORGANIZATION NAME] DESCRIPTION



***The Organization Description** focuses on the custodian. This sub-section describes the custodian's role(s) and mandate(s) and its oversight and accountability for personal health information. It includes brief descriptions of codes of ethics, professional codes and the custodial policies and reporting arrangements that govern its employees or partners. It identifies formal arrangements or contracts that extend its accountability for personal health information to third parties, including service providers and organizations to which the custodian discloses personal health information.*

*This sub-section includes a high level description of the custodian's business and its connection to personal health information as well as how the custodian has established internal accountability for personal health information. In the case of a project, it establishes the business objectives of the project and oversight for personal health information for all phases of the project.*

The [Organization Name] was established in [insert date] to provide [insert type of services] services to clients across the province.

### 2.2.1 ROLES AND MANDATES




***Roles and Mandates** describe the custodian's roles and mandates with regard to personal health information. It establishes the custodian's authority for collecting, using, disclosing, storing or disposing of personal health information. For this reason, the*

*description here will be important to the Data Analysis in Section 4. The custodian should ensure, therefore, that its authority for any aspect of personal health information is clear.*

The primary business of [Organization Name] is [Insert general description of business]. The [Insert source of mandate] provides [Organization Name] with its mandate, which is to provide services to clients who require [Insert as applicable]. In fulfilling its mandate, [Organization Name] has undertaken the following roles:

[List as applicable]

#### 2.2.2 ACCOUNTABILITY FOR PERSONAL HEALTH INFORMATION


 *The **Accountability for Personal Health Information** sub-section describes the custodian's roles and responsibilities in respect of personal health information and verifies the performance of those roles and responsibilities, whether it is for its operations, a system or a program. This sub-Section will make an important contribution to the assessment of how well the custodian exercises oversight for personal health information, including reporting relationships, review and audit, and the establishment and application of policy.*

*It should include the following information:*

- (1) The custodian's privacy policy and directives, review and audit procedures regarding policy, reporting relationships and accountability for personal health information, and*
- (2) Formal arrangements and contracts that address how partners and service providers safeguard personal health information in accordance with the custodian's requirements. These are important because they establish how the custodian extends its accountability to partners and service providers.*

*The custodian can use organization charts to clarify descriptions; the custodian can also append copies of agreements or contracts to the PIA.*

#### 2.2.3 TRAINING AND AWARENESS

 ***Training and Awareness** describes the custodian's training plans and awareness sessions related to procedures, policies or other measures related to safeguarding personal health information. It shows how the custodian ensures that employees and*

*contractors are made aware of their obligations and responsibilities with regard to personal health information.*



*This first step in the methodology can include listing and briefly describing all of the **internal policy, procedures, agreements or oversight** reported in this section in Annex C, Privacy Safeguards, if they act as safeguards for personal health information.*

### 3 OPERATIONS AND ENVIRONMENT



*The previous Section has provided the legislation and policy framework in which the custodian operates and describes the custodian's framework for oversight and compliance.*

*Documenting the **Operations and Environment** is the second step in the methodology. It focuses on the custodian's business or operation. It starts with the custodian's concept of the interaction between individuals and between individuals and technology – the operations – and it describes the technology, the individuals and the environment in which people and technology operate. This Section is the foundation for the Data Analysis in Section 4; the level of detail should be enough to support the Data Analysis.*

*In non-technical environments, this Section may be brief and will focus on the individuals that have access to personal health information and on the physical environment. If information technology is used for collecting, processing or storing personal health information, preparing this Section may require information technology expertise.*

*The description should include the security safeguards designed to protect personal health information from loss or theft, as well as from unauthorized access, disclosure, copying, use or modification throughout its life cycle. If a threat and risk assessment has been performed, this Section can refer to it and summarize relevant contents.*

*The headings below are suggestions: the description should be as complete as possible and organized logically. Detailed information can be included in an attachment.*

*At the end of this step, the custodian will have described the operations and information technology that affect personal health information and the environment in which the personal health information is collected, used, disclosed, stored, or disposed of. It is necessary to describe operations and environment before describing the personal health information itself and the data flows in Section 4.*

#### 3.1 CONCEPT OF OPERATIONS



*The **Concept of Operations** highlights the major characteristics of a system or program and how it will achieve its objectives. It introduces the technology and the environment discussed in the remainder of Section 3. It is normally written from the point of view of a user, but it could be described from a client's point of view.*



*The text below is an example of a concept of operations, in this case for a central database.*

The [Name of System] is a central database established to manage the approval of [Insert as applicable]. [Name of System] will be used to record and maintain [List as applicable] data. It will also track [List as applicable]. [Name of System] will not store the [List as applicable]. The initial roll out has no interface or connection with other systems or applications.

### 3.2 TECHNOLOGY DESCRIPTION



*The **Technology Description** should include an overview of the technical architecture, services, functionality, and connectivity. For some custodians, this Section will be brief or need not be undertaken if there is little or no technical infrastructure.*

*Custodians that use information technology to support their operations or programs should ensure that this Section is accurate and clear. Graphics can be used to support explanations and descriptions. The amount of information needed will be a function of the complexity and scope of the technology. If a third party is providing services of any kind or is involved in collection, management or use of personal health information, they should be accounted for here. The technology description will help clarify the business process and data flows in Section 4, Data Analysis.*

*The system architecture below is an example of how a graphic can help describe a system; the sample text shows how a graphic can be introduced. The custodian should identify structural elements, user interfaces and interactions, connectivity, portals and other information technology.*

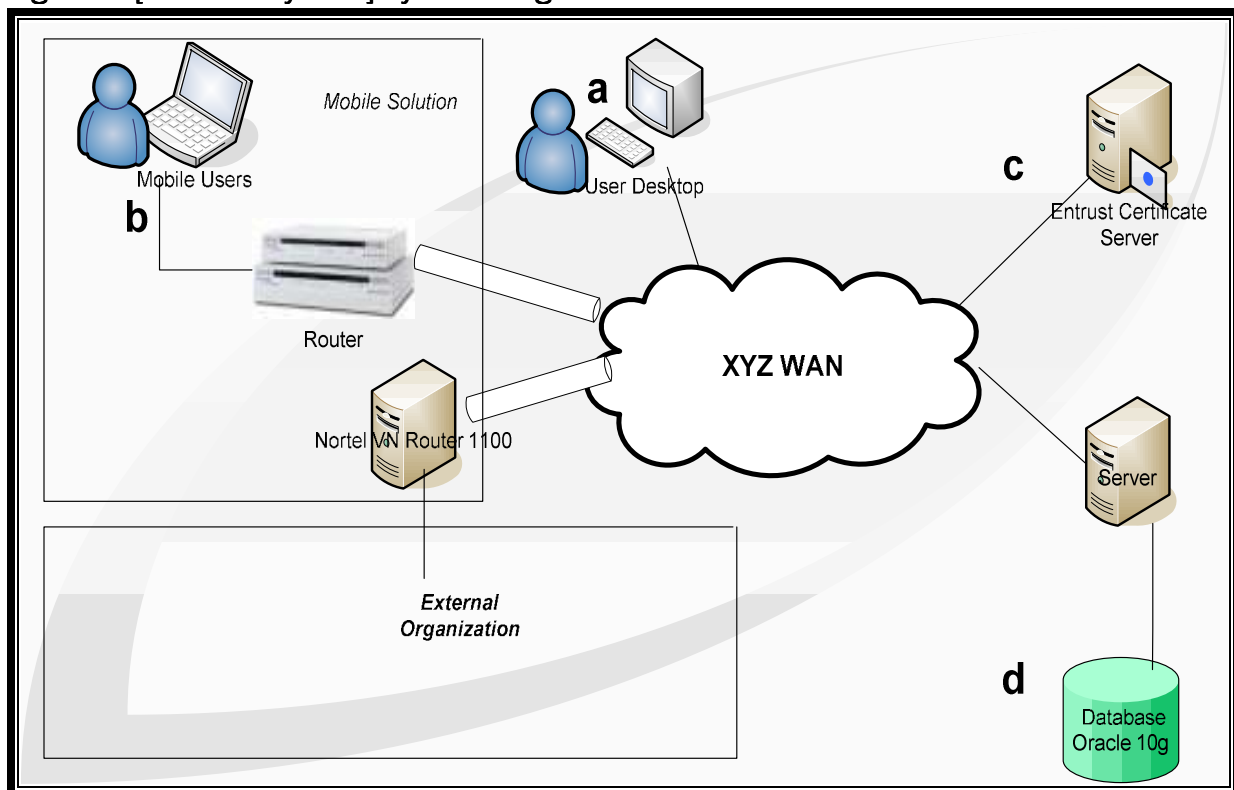
*The explanation should **describe each major element** of the system, user locations, data collection points, ownership and lines of demarcation between the organization and its partners if any, and security appliances such as firewalls and secure routers. Depending on the size and complexity of the information technology associated with the personal health information, the custodian may need to describe the functions of architectural elements using separate headings, e.g. point of service system.*

*Normally, architectural drawings are available from organizational information technology staff.*



The [Name of system] is a central database established to manage the approval of [List as applicable] and the issuance of [List as applicable]. [Name of system] will be used by [List as applicable] to record and maintain [List as applicable] data and photographs of [List as applicable]. The [Name of system] consists of the following major elements, which are shown in Figure 1[Name of System] System Diagram, and described in the text below Figure 1.

**Figure 1: [Name of System] System Diagram**



- a. Registered users access [Name of system] by launching the [Name of system] application;
- b. Registered [Name of system] mobile users launch the [Name of system] application from their laptop;
- c. The [Name of system] verifies the user in order for the user to access [Name of system]; and
- d. The [Name of system] Database provides security for data in transit and at rest.

### 3.3 SECURITY



Depending on the complexity of the operations, system or program being assessed, the custodian can include a separate sub-Section that describes information technology security, e.g. firewalls, intrusion detection, encryption, etc. This Section can incorporate information from a threat and risk assessment, if one has been undertaken. Appendix C to the PHIA Policy Development Manual contains information about security best practices. Note that custodians may require the input of a security expert for complex operations, systems or programs.

The text below is an extract from PHIA Policy Development Manual; the custodian can use it as a checklist for what to cover in this sub-section.

#### **Communications and Operations Management:**

Establish procedures and responsibilities  
Control third party service delivery  
Carry out future system planning activities  
Protect against malicious and mobile code  
Establish backup procedures  
Protect computer networks  
Control how media are handled  
Protect exchange of information  
Protect electronic commerce services  
Monitor information processing facilities

### 3.4 USERS, ROLES AND PRIVILEGES



The description of the **Users, Roles and Privileges** includes each individual's function and role with regard to personal health information. Any individual with access to personal health information, including system administrators and third party service providers of information technology, should be included in the community. Access to personal health information and what individuals are permitted to do – their privileges – also need to be accounted for. If there is a threat and risk assessment, the custodian can use information about personnel security and access controls for Community and Roles.

In complex technical systems, the custodian can organize this information using separate headings. The information can also be set out in table form, as suggested in the sample table below, or the custodian can list and describe roles.

*The list below is taken from Appendix C to the PHIA Policy Development Manual. The custodian can use it as a checklist for the security aspects of the description in this Section:*

***Information Access Control Management:***

*Control access to information*

*Manage user access rights*

*Encourage good access practices*

*Control access to network services*

*Control access to operating systems*

*Control access to applications and systems*

*Protect mobile and tele-working facilities*





***Human Resource Security Management::***

*Emphasize security prior to employment*


*Emphasize security during employment*

*Emphasize security at termination of employment*

**Table 1: Roles**

Role	Definition	Access to	Authorized Activities
 <i>List the individual roles</i>	 <i>Define the role</i>	 <i>List the technology, database, system to which the role has access.</i>	 <i>List what the role is authorized to do e.g. read, write, delete data. If privileges are stipulated in an agreement or contract, identify it.</i>
Receptionist	The person that greets patients, makes appointments and records patient name and contact information. The receptionist is normally the first point of contact for patients.	Patient Data Enrolment	Enter Data Read Data Amend Data
Caregiver	Nurse, Physician attending a patient who record health care actions.	Patient Record	Enter Data Read Data Amend Data
System Administrator	Maintains system	System	Configure system, patch management

### 3.5 PHYSICAL ENVIRONMENT AND SECURITY

 **The Physical Environment and Security** describes any aspect of the physical environment that can affect the protection of personal health information. It is normally described from a security or safety point of view and can summarize information from an existing threat and risk assessment. Risk to personal health information in the physical environment can include fire, flood, power outages, or pandemics. Safeguards include physical barriers to unauthorized access, such as locked doors and filing cabinets, as well as alarm systems.

*Other sections can be added if there is additional information about the custodian's environment that can affect personal health information.*

*The list below is from Appendix C to PHIA the Policy Development Manual and suggests coverage for this Section:*

***Physical and Environmental Security Management:***

*Use secure areas to protect facilities; and  
Protect your organization's equipment.*

The [Name of system] will be housed in a secure server room inside a security zone in the [Insert location]. Access to the server room is controlled by keypad entry and alarms; employees wear ID and visitors are escorted. There are few employees in the area and it is therefore easy to identify a visitor.

[Organization Name] mobile enrolment stations, which are ruggedized laptop computers issued to employees whose duties require them, are limited exclusively to [Organization Name] facilities and therefore access and use is within a restricted zone at minimum.

[Name of system] will only be accessible from [Organization Name] desktops and [Organization Name] -approved laptops in [Organization Name] facilities.

The [Organization Name] TRA addresses wireless and the use of laptops.



*The custodian can complete **this step** by listing and briefly describing each personal health information protective measure identified in this section in **Annex C, Privacy Safeguards**.*

## 4 DATA ANALYSIS



The **Data Analysis** focuses on the personal health information and all of the processes associated with it: the data analysis tracks the life cycle of personal health information, provides an inventory of personal health information, and accounts for all flows of personal health information. It is the third step in assessing impact on personal health information and builds on the information provided in the previous steps.

*The Data Analysis will normally include the following elements:*

**The Business Process** description provides a high level overview of the business process, to help external readers to understand the detailed information in the remainder of the data flows; the business process accounts for any information technology and external partners. The business process does not describe data flows: it describes the overall process that the system, operation or program supports.

**The Personal Health Information** is an inventory of all personal health information associated with the operations, system or program being assessed.

**The Data Flows** account for all flows of personal health information and depict every actor that participates in the collection, use, disclosure, storage and disposal or destruction of personal health information, starting with an overview of the personal health information and its life cycle. This Section can be organized according to activities or by technology if the principal focus of the assessment is how information technology affects personal health information. Completing this section may require input from managers.


**The Personal Health Information Summary** summarizes the collection, formats, user, purpose of collection, disclosure, storage or retention, retention period, disposal as described in the data flows.

**By the end of this step**, the custodian will have a complete accounting of all personal health information associated with the operations, system or program being assessed, and of all of the processes, individuals and information technology that collect, use, disclose, store or dispose of personal health information.

**The custodian is ready to identify risk to personal health information only when this section is complete and accurate.**

This Section describes the personal health information that will be collected for [Name of system]; and the data flows for each activity associated with personal health information.

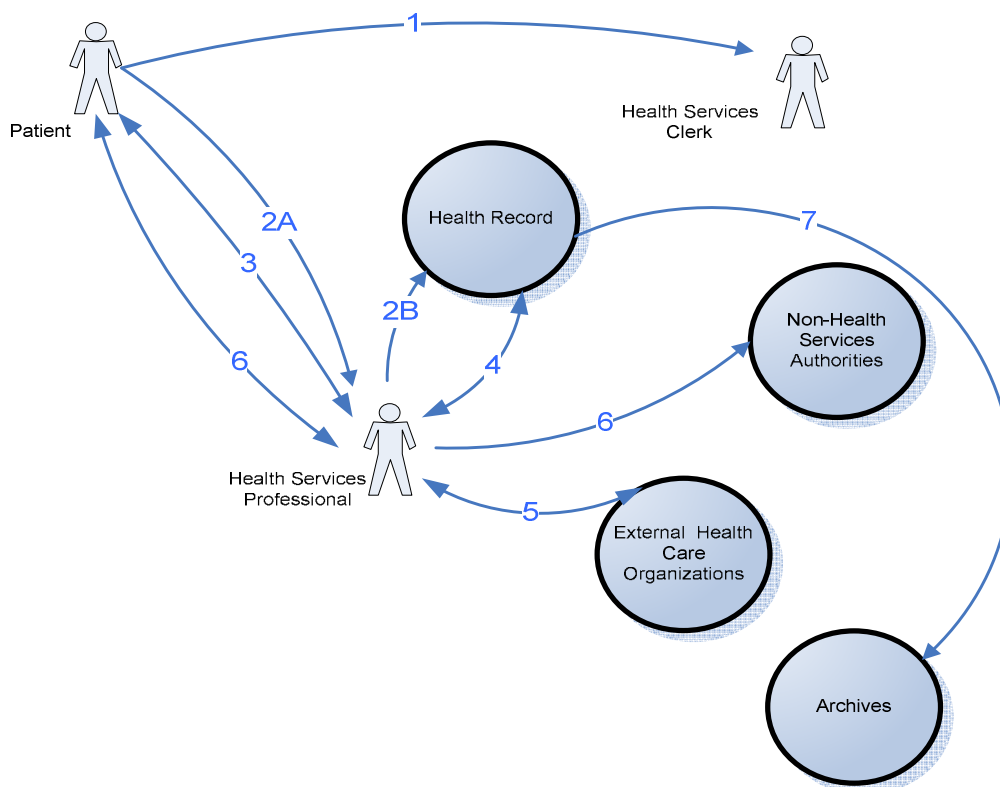
## 4.1 BUSINESS PROCESS

 The **Business Process** describes the activities that affect the personal health information listed in the preceding sub-Section. It should account for collection of personal health information, transactions and disclosures, and decisions.

Custodians can use a business flow diagram to provide a high level graphical description of the major components of the business process and show how personal health information circulates from the point of collection to the point where all copies are destroyed or permanently archived, i.e. the life cycle of the personal health information. Each numbered arrow corresponds to an action that the table below describes.

Once the custodian describes the business process, the data flows can follow.

Figure 2: Sample Business Flow Diagram





*The table below should describe each action shown in the business flow diagram. Step numbers and descriptions correspond to the sequence numbers in the Business Process Diagram. A table format can help to organize and present information clearly. If desired, the personal information affected can be listed in a separate column, but this table should focus on the life cycle of personal health information at a high level rather than specific details.*

**Table 2: Sample Business Flow Description**

Step #	Data Set	Description
1	Request for Treatment	The patient requests an appointment for health services. The appointment would normally be made through the health services clerk.
2A	Obtain consent	Consent is obtained from the patient by the health services professional.
2B	Record consent	Consent is recorded by the health services professional.
3	Patient information provided during a health encounter e.g. description of symptoms, tests, diagnosis, observations	The encounter could be an examination, a treatment, an assessment, administering diagnostic tests or medication, emergency care or any other health services encounter between a patient and a health services professional.
4	Patient health record	The health services professional views the patient's personal health information in the electronic health record. Following the health encounter, the health services professional enters notes relevant to the patient's health record into the patient's health record. The health services professional may also enter test results or other health information obtained from external health care organizations.
5	Test data e.g. blood test results, TB test results.	The health services provider sends test data, samples, and other material necessary for testing to a laboratory or other external health services organization and receives the test results.



Step #	Data Set	Description
6	Patient health assessment	Under limited circumstances, the health services professional may provide a patient assessment that includes health information to the approved external organizations.
7	Health record	Health records are archived in accordance with policy.

## 4.2 PERSONAL HEALTH INFORMATION



**Personal Health Information** is an **inventory** of all personal health information associated with the operations, system or program being assessed. The inventory is essential as it records all impacts on personal health information, which establishes the basis for the data flow analysis that follows.

For each information element there should be a clear statement regarding why the information is being collected, how it is being used or disclosed, who collected it, what format it is collected in, who is using it, who it is being disclosed to, where it is being stored and for how long. It should account for access by service providers or third parties. It is critical that the information in this sub-Section is complete and accurate.

The table below is an example of how this information can be organized and presented.

**Table 3: Data Description Table**

Description of Personal Health Information	Collect ed By	Type of Format	Used By	Purpose of Collection	Disclosed to	Storage or Retention Site	Retention Period	Disposal
Set Name e.g. Patient Record								
1. Elements e.g. Full name								
2. Elements e.g. Health #								
Set Name								
1. Elements								
2. Elements								

### 4.3 DATA FLOWS

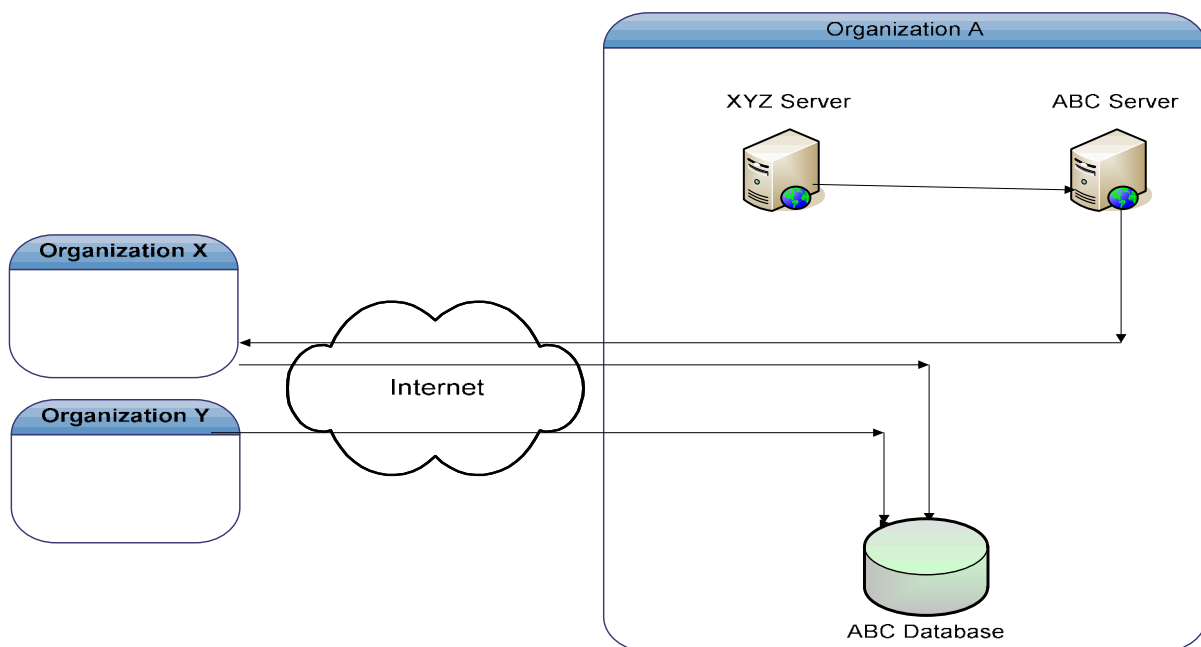



*The **Data Flows** sub-Section documents the flow of data for each process associated with personal health information. The custodian should account for every data set of personal health information, as described in Section 4.1, so that the privacy analysis in Section 5 can examine all activities that affect personal health information.*

*Graphics can help make actions and actors clearer. The example below shows one way to depict data flows. Following the graphic are descriptions of each data flow.*

This sub-Section describes the flow of personal information for each process. [Name of system] functionality is fully described in the “[Name of system] Specification Document”, which is the principal source of information for this Section. All of the data flows depicted in Figure 3 below assume that users have already logged onto [Name of system] using their secure credential.

Figure 3: Sample Data Flows



 The custodian should insert as many tables as there are flows of data: for complex systems, there will be many. Complex systems may require several sets of graphics, arranged logically according to systems, services or applications illustrated in the business flows figure. The PIA team may require input from information technology and business managers to ensure completeness and accuracy.

The headings used in the example are suggestions.

Once the custodian has described all of the data flows, the custodian has all of the information necessary to complete the privacy analysis in the next Section.

Name and Description	[Name of system] <b>data flow #1</b> – [Organization Y to ABC Database ]
Data Elements	[Data Set] information contained within the [ABC Database]
Origin	Organization Y

Destination	ABC Database
Format and Protocol	ABC database table(s); SQL database calls
Safeguards	All data is encrypted using Secure Sockets Layer. Access to the database is limited to authorized persons using tokens as described in Section 3.6.



*When this section is complete, the custodian can list all of the privacy safeguards identified in the course of documenting the data flows. List these in **Annex C, Privacy Safeguards**, and describe each briefly.*

## 5 PRIVACY RISK ASSESSMENT



The **Privacy Risk Assessment** is the fourth step in the PIA methodology. This step identifies potential risk to personal health information by identifying gaps in privacy safeguards, which the custodian then addresses in Sections 6 and 7.

The assessment organizes the requirements from PHIA according to the ten principles in the CSA Model Code: these are accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

The ten principles are recognized throughout Canada and therefore provide a standard approach to organizing an assessment of privacy safeguards. The requirements for each principle are set out in the left hand column of each table, followed by a column for listing privacy safeguards and a column for identifying gaps in privacy safeguards. This approach helps the custodian to identify where additional effort is required. The custodian can add requirements from other jurisdictions to the requirements column; the custodian has identified those requirements in Section 2 of the PIA.

When the custodian finishes completing the ten privacy tables, the custodian lists all gaps identified in the ten tables in a summary table at the end.

This template includes explanatory notes regarding each of the ten privacy principles. The custodian can tailor the explanatory notes for each principle as required.

By completing this Section, the custodian will have identified weaknesses or gaps in privacy safeguards.

This section identifies gaps in existing and planned privacy safeguards for protecting personal health information in accordance with the requirements of PHIA <Insert other applicable requirements identified in Section 2>.

This section is organized according to the ten privacy principles of the Canadian Standards Association's "Model Code for the Protection of Personal Information" (CSA Model Code), with the principle set out in bold italics. The requirements that support each principle are listed in the left column of each table; the privacy safeguards that address the requirements are listed in the next column and the third column identifies gaps in privacy safeguards. The summaries that follow indicate whether or not existing and planned

privacy safeguards are adequate for addressing risk to personal health information. Annex C fully describes privacy safeguards.

## 5.1 PRINCIPLE 1 – ACCOUNTABILITY

***An organization is responsible for personal information<sup>1</sup> under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.***





***How PHIA Requires Custodians to Address Accountability:*** Section 3 of PHIA has as one of its stated purposes the establishment of mechanisms aimed at ensuring the accountability of persons having custody or control of personal health information. Section 13 of PHIA requires custodians of personal health information to establish and implement policies and procedures to facilitate the implementation of, and ensure compliance with PHIA and its regulations in relation to the manner of collection, storage, transfer, copying, modification, use and disposition of personal information whether within or outside Newfoundland and Labrador. Finally, Section 18 of PHIA requires any custodian that is not a “natural person” (i.e., an individual person) to designate one or more contact people to facilitate the custodian’s compliance with the Act.

*The **Requirements** column in the table below lists all of PHIA requirements for this principle.*

*The custodian can add other requirements that were identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.*

Requirement	How Custodian Addresses the Requirement	Gap
-------------	---	-----


<sup>1</sup> For the purposes of this privacy impact assessment, the term “personal information” in each of the privacy principles refers to personal health information.


Requirement	How Custodian Addresses the Requirement	Gap
Designate a person to make a decision required of the custodian under PHIA.	 <i>List the identifying number and name of each applicable privacy safeguard from Annex C.</i>	 <i>Identify weaknesses or gaps in safeguards; custodians can use PHIA Policy Development Manual to help identify weaknesses or gaps.</i>

Requirement	How Custodian Addresses the Requirement	Gap
<p>Designate one or more contact persons to perform the following functions:</p> <p>Facilitate the custodian's compliance with this Act and the regulations;</p> <ul style="list-style-type: none"> <li>▪ Ensure that employees, contractors, agents and volunteers of the custodian and those health care professionals who have the right to treat persons at a health care facility operated by the custodian are informed of their duties under this Act and the regulations;</li> <li>▪ Respond to inquiries from the public in respect of the custodian's information policies and procedures; and</li> <li>▪ Respond to requests by an individual for access to or correction of personal health information about the individual that is in the custody or under the control of the custodian.</li> </ul> <p>NOTE: When the custodian does not identify a contact person, the custodian, if an individual rather than an organization, is considered to be the contact person. The custodian makes his or her contact information available in accordance with Section 18 of PHIA.</p>	102 Privacy Contact	Privacy Officer appointed but no terms of reference that list functions or duties to be performed.



Requirement	How Custodian Addresses the Requirement	Gap
Establish and implement privacy policy and procedures to facilitate the implementation of, and ensure compliance with, PHIA and regulations respecting the manner of collection, storage, transfer, copying, modification, use and disposition of personal health information whether within or outside the province. The policy and procedures should include all elements identified in Part II, Section 13.		
Identify third parties involved in custody or control of the personal information and establish legal arrangements regarding privacy requirements.		
Require employees, agents, contractors, volunteers and, where applicable, health care professionals who may treat patients in the custodian's health care facility, to take an oath or affirmation of confidentiality.		

Requirement	How Custodian Addresses the Requirement	Gap
Ensure that employees, agents, contractors, volunteers and, where applicable, health care professionals who may treat patients in the custodian's health care facility, comply with the provisions of PHIA, any Regulations promulgated under PHIA, and with the custodian's information policies and procedures.		
 <i>Add requirements identified in Section 2 if necessary, e.g. federal privacy legislation, electronic health records requirements, privacy legislation of another province or country, etc.</i>		

 *The custodian can **add a summary paragraph** to highlight the custodian's privacy safeguards and how the safeguards generally address PHIA requirements or other requirement that fall under the accountability principle.*

*Following the summary, add a conclusion that describes how well the privacy safeguards meet requirements, e.g. "The **[Name of operations, system or program]** meets all PHIA requirements." If there any gaps are identified, the conclusion should indicate that there is potential risk to personal health information, e.g. "The **[Name of operations, system or program]** will require additional privacy safeguards to achieve the target risk level of Low by addressing the following gaps: **[List gaps]**."*

**Summary and Conclusions:** The XYZ program will require additional privacy safeguards to achieve the target risk level of Low; the following deficiency needs to be addressed:

- Privacy Officer appointed but no terms of reference that list functions or duties.
- [Etc.]

## 5.2 PRINCIPLE 2 – IDENTIFYING PURPOSES

*The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.*



**How PHIA Requires Custodians to Address Identifying Purposes:** Under PHIA, the custodian is required to take reasonable steps to inform individuals regarding the purpose of collection and to provide them with a contact name and appropriate contact information. Reasonable steps include notice on collection, signage, verbal notification or more formal means, such as having the individual sign a notice.

The **Requirements** column in the table below lists all of PHIA requirements for this principle.

The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.

Requirement	How Custodian Addresses the Requirement	Gap
<p>On collection of personal health information, take reasonable steps to inform the individual or his or her representative:</p> <ul style="list-style-type: none"> <li>▪ of the purpose for the collection, use and disclosure of the information;</li> <li>▪ of the identity of and other relevant information relating to the contact person referred to in Section 18; and</li> <li>▪ of other information prescribed in</li> </ul>		


the regulations as described in section 20 of PHIA.		
---	--	--

Summary and Conclusions:

[...]

### 5.3 PRINCIPLE 3 – CONSENT

*The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.*

 **How PHIA Requires Custodians to Address Consent:** Part III of PHIA addresses Consent and states the custodian may not collect, use or disclose personal health information unless (a) the subject of the personal health information consents to the collection, use or disclosure or (b), the collection, use or disclosure is otherwise specifically authorized under PHIA.

Consent to use or disclosure of personal health information may be express or implied when personal health information is collected directly from an individual, who consents to its use and disclosure, and when provided by another custodian as part of the circle of care. Consent must be express if use or disclosure is outside of the circle of care, as set out in Section 25.

Several provisions of PHIA authorize specific types of collection, use and disclosure of personal health information without the consent of the individual. Refer to Sections 37 to 46 of PHIA for the circumstances under which the consent of the data subject is specifically not required under PHIA for disclosure of personal health information.

Consent is also discussed under Principle 5, Limiting Use, Disclosure and Retention.

The **Requirements** column in the table below lists all of PHIA requirements for this principle.

The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.

Requirement	How Custodian Addresses the Requirement	Gap
Obtain consent directly from the individual who is the subject of the information or from their duly appointed authorized representative, except as collection, use and / or disclosure without consent is permitted in Part IV.		
Where consent is not obtained from the individual who is the subject of the information or from their duly appointed authorized representative, ensure that Part IV permits the collection, use and / or disclosure without consent.		
Consent shall be knowledgeable and not obtained through deception or coercion.		
Obtain express consent when personal health information is to be disclosed outside of the “circle of care”, whether to a non-custodian or to the custodian for purposes other than for health care.		
Inform custodians with whom personal health information is shared of any limitations placed on disclosure by the individual patient.		

Requirement	How Custodian Addresses the Requirement	Gap
Provide for individuals to withdraw consent to collection, use or disclosure.		

Summary and Conclusions:

[...]

## 5.4 PRINCIPLE 4 – LIMITING COLLECTION

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.*



**How PHIA Requires Custodians to Address Limiting Collection:** Part IV of PHIA addresses the collection, use and disclosure of personal health information by custodians under the Act. Section 32 of PHIA requires that the custodian not collect more personal health information from or about an individual than is reasonably necessary to meet the purpose of the collection, i.e., to achieve the objectives that underlie the reason for the collection.

The **Requirements** column in the table below lists all of PHIA requirements for this principle.

The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.

Requirement	How Custodian Addresses the Requirement	Gap
Limit collection of personal health information to that which is reasonably necessary to meet the purpose of the collection, except where the collection is required by law.		

Summary and Conclusions:

[...]

## 5.5 PRINCIPLE 5 – LIMITING USE, DISCLOSURE, AND RETENTION

***Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.***



***How PHIA Requires Custodians to Address Limiting Use, Disclosure and Retention:***  
Part IV of PHIA addresses the collection, use and disclosure of personal health information by custodians of personal health information.

*Regarding the limiting of custodians' use of personal health information, Section 33 requires either that custodians have the consent of individuals for the contemplated use, or that the use be authorized under PHIA. Section 33 also requires that custodians not use personal health information at all if other information will serve the purpose of the use. The uses to which the custodian may put personal health information in their custody are explicitly set out under Section 34 of PHIA, and Section 35 requires that the custodian limit their use of personal health information to those of its employees and agents that need to know the information in order to carry out the purpose for which the information was collected, or for a purpose authorized under the Act.*

*PHIA also places limitations on custodians' ability to disclose personal health information. Section 36 requires either that custodians have the consent of data subjects for the contemplated use, or that the use be authorized under PHIA. Section 33 also requires that custodians not use personal health information if other information will serve the purpose of the use. Sections 37 to 46 of PHIA explicitly set out the circumstances under which the custodian may disclose personal health information without the consent of individuals. Section 47 sets out the circumstances for disclosure outside of Newfoundland and Labrador, including notifying individuals to whom personal health information is disclosed about the data owner's limitations on disclosure, if any.*

*The **Requirements** column in the table below lists all of PHIA requirements for this principle.*

*The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.*

Requirement	How Custodian Addresses the Requirement	Gap
Limit the use of personal health information to the minimum amount of information necessary to achieve the purpose for which it is being used.		
Limit the disclosure of personal health information to the minimum amount of information necessary to accomplish the purpose for which it is used, unless disclosure is required by law.		
Personal health information is not to be used or disclosed if other information will serve the purpose and only if consent is obtained for its use or disclosure.		



Requirement	How Custodian Addresses the Requirement	Gap
Disclose personal information only with the consent of the individual or where specifically authorized under Part IV.		
Use personal health information for the purpose for which the information was collected.  NOTE: Part IV, Section 34 sets out permitted uses in detail.		
Limit the use of personal health information to employees or agents who require the information to carry out the purpose for which the information was collected or for a purpose authorized under PHIA.		
When transferring records of personal health information to a successor custodian, take reasonable measures to notify the individual who is the subject of the information prior to the transfer or as soon as possible after the transfer regarding the transfer of information, including identification of the successor custodian.		

Requirement	How Custodian Addresses the Requirement	Gap
Ensure consent is obtained prior to disclosure of personal health information outside the province, and that the disclosure is permitted under PHIA as set out in Part IV, Section 47. The disclosure should only be to a person whose functions are similar to those performed by the disclosing custodian.		
Log all disclosures of personal health information, including name, date and purpose, and description of information disclosed, including the use of automatic logging for electronic health records.		

Requirement	How Custodian Addresses the Requirement	Gap
<p>Where the custodian uses or discloses personal health information about an individual without the individual's consent in a manner that is inconsistent with the information policies and procedures referred to in Section 13, the custodian must:</p> <ul style="list-style-type: none"> <li>▪ Inform the individual who is the subject of the information of the use or disclosure at the first reasonable opportunity except where, under Section 58, the custodian would be required or permitted to refuse access to the record of personal health information;</li> <li>▪ Make a note of the use or disclosure; and</li> <li>▪ Retain the note as part of the record of personal health information about the individual that it has in its custody or under its control unless the custodian reasonably believes that the use or disclosure of personal health information will not have an adverse impact as described in Section 15.</li> </ul>		
<p>Ensure that for personal health information to be disclosed outside of Newfoundland and Labrador, the following circumstances exist:</p>		

Requirement	How Custodian Addresses the Requirement	Gap
<p>(a) the individual who is the subject of the information consents to the disclosure;</p> <p>(b) the disclosure is permitted by this Act or the regulations;</p> <p>(c) the person receiving the information performs functions similar to the functions performed by a person to whom this Act would permit the custodian to disclose the information in the province under subsection 40(2);</p> <p>(d) the following conditions are met:</p> <p>(i) the disclosure is for the purpose of health planning or health administration,</p> <p>(ii) the information relates to health care provided in the province to a person who is a resident of another province or territory of Canada , and</p> <p>(iii) the disclosure is made to the government of that other province or territory of Canada ;</p> <p>(e) the disclosure is reasonably necessary for the provision of health care to the individual and the individual has not expressly instructed the custodian not to make the disclosure in its entirety; or</p> <p>(f) the disclosure is reasonably necessary for the administration of payments in connection with the provision of health care to the individual or for</p>		

Requirement	How Custodian Addresses the Requirement	Gap
contractual or legal requirements in that connection.		
When personal health information disclosure has been limited at the request of the individual, inform the individual to whom the information is disclosed of the limitation.		

Summary and Conclusions:

[...]

## 5.6 PRINCIPLE 6 – ACCURACY

*Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.*



### **How PHIA Requires Custodians to Address Accuracy:**

Section 16 of PHIA requires that custodians:

- (a) take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purpose for which the information is used or disclosed;
- (b) clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, completeness or up-to-date character of the information; and
- (c) make a reasonable effort to ensure that the person to whom a disclosure is made is the person intended and authorized to receive the information.

The **Requirements** column in the table below lists all of PHIA requirements for this principle.

The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.

Requirement	How Custodian Addresses the Requirement	Gap
Take reasonable steps to ensure that the personal information is accurate, complete and up-to-date.		
When information is shared or disclosed, establish procedures to provide notices of correction, either automatically or at the request of an individual.		
Record and retain requests for a review of errors or omissions and corrections or decisions not to correct.  NOTE: This requirement is also dealt with under Principle 9, Individual Access, below.		

Requirement	How Custodian Addresses the Requirement	Gap
<p>Establish a clearly defined process by which an individual may request access to, assess and discuss or dispute the accuracy of his or her personal health information or record.</p> <p>NOTE: This requirement also dealt with under Principle 9, Individual Access, below.</p>		

Summary and Conclusion:

[...]

## 5.7 PRINCIPLE 7 – SAFEGUARDS

***Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.***



***How PHIA Requires Custodians to Address Safeguards:*** Section 13 of PHIA requires custodians to establish information policies and procedures to facilitate the implementation of and ensure compliance with PHIA and its regulations, in relation to the manner of collection, storage, transfer, copy, modification, use and disposition of personal information, whether within or outside the province. These must include policies and procedures to:

- (a) protect the confidentiality of personal health information that is in custody or under its control and the privacy of the individual who is the subject of that information;*
- (b) restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that*

information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the information was collected or will be used;

(c) protect the confidentiality of personal health information that will be stored or used in a jurisdiction outside the province or that is to be disclosed to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and

provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information.

These information policies and procedures have to include appropriate measures to address the risks associated with the storage of personal health information, taking into account the manner and form in which the personal health information is recorded, the location of storage and the degree of sensitivity of the personal health information to be protected.

Section 15 of PHIA specifically addresses security measures that custodians will have to adopt. This Section requires custodians to take steps that are reasonable under the circumstances of their operations to ensure that:

(a) Personal health information in its custody or control is protected against theft, loss and unauthorized access, use or disclosure;

(b) Records containing personal health information in its custody or control are protected against unauthorized copying or modification; and

(c) Records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner.

The **Requirements** column in the table below lists all of PHIA requirements for this principle.

The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.

Requirement	How Addresses Requirement	Custodian the	Gap



Requirement	How Addresses Requirement	Custodian the	Gap
<p>Ensure that there are practices, policies and procedures in place to, at a minimum:</p> <ul style="list-style-type: none"> <li>▪ Protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information;</li> <li>▪ Restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the information was collected or will be used;</li> <li>▪ Protect the confidentiality of personal health information that will be stored or used in a jurisdiction outside the province or that is to be disclosed by the custodian to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information.</li> </ul>			
Version [ ]			46

Requirement	How Addresses Requirement	Custodian the	Gap
<ul style="list-style-type: none"> <li>Take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized access, use or disclosure;</li> <li>Records containing personal health information in the custodian's custody or control are protected against unauthorized copying or modification; and</li> <li>Records containing personal health information in the custodian's custody or control are retained, transferred and disposed of in a secure manner.</li> </ul> <p>NOTE: "Disposed of in a secure manner" means that the record cannot be re-identified or reconstructed.</p>			
<p>Ensure that employees, agents, contractors and volunteers, and those health care professionals who have the right to treat persons at a health care facility operated by the custodian, are aware of the duties imposed by PHIA and the regulations and by the custodian's information policies and procedures referred to in Part II, Section 13.</p>			

Requirement	How Addresses Requirement	Custodian the	Gap
Establish processes for notifying the Commissioner of a material breach involving the unauthorized collection, use, or disclosure of personal health information.			
Establish processes for notifying the individual(s) affected of a material breach involving the unauthorized collection, use, or disclosure of personal health information; or if the personal health information is stolen, lost, disposed of in a manner other than those permitted under PHIA or disclosed to or access by an unauthorized person.  NOTE: Part II, Section 15/(6) addresses researchers that receive information from another custodian and their obligation to notify; II/15/(7) notes circumstances when custodians do not need to notify individuals.			

Summary and Conclusion:

[...]

## 5.8 PRINCIPLE 8 – OPENNESS

*An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.*



**How PHIA Requires Custodians to Address Openness:** Openness, as addressed under PHIA, relates closely to the way that accountability is addressed.

Section 13 of PHIA requires custodians of personal health information to establish and implement policies and procedures to facilitate the implementation of, and ensure compliance with PHIA and its regulations in relation to the manner of collection, storage, transfer, copying, modification, use and disposition of personal information whether within or outside Newfoundland and Labrador. Finally, Section 18 of PHIA requires that any custodian that is not a “natural person” to designate one or more contact people to facilitate the custodian’s compliance with the Act.

Part V of PHIA sets out in significant detail the rights that data subjects have and responsibilities that custodians will be under with respect to personal health information. The **Requirements** column in the table below lists all of PHIA requirements for this principle.

The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian’s operations, system or program.

Requirement	How Addresses Requirement	Custodian the	Gap
Make available to those who are or who are likely to be affected by the custodian's activities a written statement that provides a general description of the custodian's information policies and procedures.			
Establish procedures for notifying individuals whose personal health information is stolen, lost, disposed of in a manner other than permitted by PHIA or the regulations, or disclosed to or accessed by an unauthorized person.			

Requirement	How Addresses Requirement	Custodian the	Gap
Inform the Commissioner in the event of a material breach.			

Summary and Conclusion:

[...]

## 5.9 PRINCIPLE 9 – INDIVIDUAL ACCESS

*Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.*



**How PHIA Requires Custodians to Address Individual Access:** Part V of PHIA sets out in significant detail the rights that individuals have and responsibilities that custodians will be under with respect to personal health information. An individual's right of access and correction are provided for under Sections 52, 53, 54 and 60, and the custodian's obligations in relation to the timeframes within which it must respond to a request for access, the content of the response, the grounds for refusing to grant access and the obligations of the custodian when amending an individual's personal health information are set out under Sections 55 through 64.

Under PHIA, with certain exceptions set out under Section 58 of the Act, individuals have a blanket right of access to any record that contains their personal health information, and either the individual themselves or their designate can exercise this right. Following the receipt of a request for access, the custodian will have 60 days within which to respond. In its response, the custodian will have to make the record available and, where requested to do so, provide a copy to the individual for a reasonable fee, advise the individual that the record is not in its possession or deny the request for access on the grounds set out under Section 58. Where the individual has been granted access to their personal health

information, they may request an amendment under Section 60, and the custodian will have 30 days within which to respond; the custodian may either make the requested amendment or deny the request based on any of the grounds set out under Section 62.

The **Requirements** column in the table below lists all of PHIA requirements for this principle.

The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.

Requirement	How Custodian Addresses the Requirement	Gap
<p>Establish procedures and ways that allow the individual who is the subject of the information to request access to his or her personal information.</p> <p>NOTE: The exceptions to an individual's right of access are set out in Part II, Section 58.</p>		

Requirement	How Custodian Addresses the Requirement	Gap
<p>Formal procedures for access must include the following elements:</p> <ul style="list-style-type: none"> <li>▪ Assistance to individuals whose requests that do not contain enough detail (Section 54);</li> <li>▪ Quick response time to requests; time is not to exceed 60 days (Section 55);</li> <li>▪ Record availability and copies of records (Section 56);</li> <li>▪ Fees (Section 57);</li> <li>▪ Ensuring the retention of information subject to a request until access is provided or denied (Part II, Section 15); and</li> <li>▪ Refusal of access (Section 58).</li> </ul> <p>NOTE: Informal procedures are permitted under Section 59.</p>		

Requirement	How Custodian Addresses the Requirement	Gap
<p>Establish a process for correcting information on request that includes the following elements:</p> <ul style="list-style-type: none"> <li>▪ Examination of the request to ensure that the record is demonstrably incorrect or incomplete and supplies the necessary information for correction (Section 62);</li> <li>▪ Written notification to an individual requesting correction that a correction to his/her information has been made (Sections 60 and 63);</li> <li>▪ Notification of correction to other parties to which the original information was disclosed within the past 12 months (Section 63);</li> <li>▪ Corrections are made no later than 30 days following a request (Section 61).</li> </ul> <p>NOTE: The exceptions to an individual's right of correction are set out in Part V, Section 62.</p>		



Requirement	How Custodian Addresses the Requirement	Gap
<p>Make corrections as follows:</p> <p>Record correct information in the record, and either strike out incorrect information without obliterating the record or label information as incorrect and sever it if striking out the information is not possible.</p> <p>Where it is not possible to record the correct information in the record, establish a practical system to inform a person accessing the record that the information in the record is incorrect and to direct the person to the correct information.</p>		
<p>Annotate records regarding refusals to correct personal health information, including details of the request, and notify the individual requesting the change regarding the annotation.</p>		
<p>Ensure that access to records for purposes of correction is provided only following confirmation of an individual's identity.</p>		

Requirement	How Custodian Addresses the Requirement	Gap
Establish processes for retaining personal health information that is the subject of a request for access under subsection 53(1) or for correction under subsection 60(1) for as long as necessary to allow the individual to exhaust any recourse under PHIA that he or she may have with respect to the request.		

Summary and Conclusion:

[...]

## 5.10 PRINCIPLE 10 – CHALLENGING COMPLIANCE

*An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.*



**How PHIA Requires Custodians to Address Challenging Compliance:** An explicitly stated purpose of PHIA, as set out under Section 3, is to establish measures to promote compliance with the Act. Under Section 18, the designation of a contact person to act as a point of accountability within the custodian's organization is intended to facilitate compliance with the Act.


The **Requirements** column in the table below lists all of PHIA requirements for this principle.

The custodian can add other requirements identified in Section 2 and can comment on how the requirements apply to the custodian's operations, system or program.

Requirement	How Addresses Requirement	Custodian the	Gap
<p>Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.</p> <p>NOTE: Part VI of PHIA provides for review of complaints by the Commissioner and Part VII addresses appeals.</p>			

Summary and Conclusion:





### 5.11 IDENTIFICATION OF RISK

 The gaps identified in the ten preceding tables represent **risk** to personal health information. **This summary identifies risk associated with each gap;** it does not attempt to measure the likelihood or impact of the risks. The table below is an example of how the custodian can list the risks identified in the preceding ten tables. If there are no gaps, then the summary can state that there are none, and therefore no identified risk to personal health information.

**Section 6, Privacy Risks and Recommendations,** is the first part of custodian's response to identification of risk.

The assessment of privacy safeguards shows that <Insert whether or not there gaps, and if applicable, refer to the summary table >.

**Table 4: Risk Identification**

Privacy Principle	Requirement	Gap	Risk ID	Risk
 List each principle that has a deficiency.	 List the requirement that is not adequately addressed. Listing the requirement helps to focus the custodian on risk.	 List each deficiency that falls into the privacy principle listed on the left.	 Identify the risk to personal health information that the deficiency creates. The row below contains an example. The custodian can number each risk for cross reference. In the example below, the risk has the ID of A-1 to reflect that it is an accountability issue (A) and 1 to show it is the first risk identified under that category. The custodian can use any cross referencing scheme.	
Accountability	Designate one or more contact persons to perform the following functions:  Facilitate the custodian's compliance with this Act and the regulations; Ensure that employees, contractors,	Privacy Officer appointed but no terms of reference that list functions or duties.	A-1	With no terms of reference, the Privacy Officer may neglect some important duties such as ensuring that employees, contractors and others are informed of

	agents and volunteers of the custodian and those health care professionals who have the right to treat persons at a health care facility operated by the custodian are informed of their duties under this Act and the regulations; Respond to inquires from the public in respect of the custodian's information policies and procedures; and Respond to requests by an individual for access to or correction of personal health information about the individual that is in the custody or under the control of the custodian.			their duties under PHIA, or responding to public inquiries. Ignorant employees, contractors or others may violate any aspect of PHIA.

## 6 PRIVACY RISKS AND RECOMMENDATIONS



*The **Privacy Risks and Recommendations** Section documents the first part of the custodian's response to the assessment of existing and planned privacy safeguards in Section 5. This Section highlights where privacy safeguards address requirements adequately and recommends how to address risk. It takes the risks from Section 5.11 and rates each one according to its likelihood and impact and then recommends how to address the risk. Section 6.2 below describes how to rate risk as **Low, Moderate or High**.*

*Once the custodian identifies gaps in safeguards, i.e. in addressing risk, managing risk involves choice. Risk decision choices include the following:*

***Avoid** - The level of risk may be reduced by removing the specific risk cause;*

***Transfer** – The level of risk may be reduced by moving the accountability for the risk to another entity, e.g. potentially some risk items could be borne by other stakeholders;*

***Reduce** – The level of risk may be reduced by choosing to implement additional privacy safeguards; and*

***Accept** – The level of risk may be accepted by reviewing and understanding the risk without implementing recommendations; this choice is unlikely for personal health information.*


*If the custodian recommends additional safeguards, the recommended safeguards should be added to Annex C.*

***The recommended privacy safeguards** will normally aim to reduce or to avoid risk.*


This section identifies where risk is adequately reduced, assesses risk associated with gaps in privacy safeguards, and makes recommendations for addressing risk.

## 6.1 SUMMARY OF TARGET RISK ACHIEVED

The following privacy principles are fully addressed by existing and planned privacy safeguards:

 *List the privacy principles for which the custodian has addressed PHIA requirements. This list reports what the custodian has accomplished in safeguarding personal health information.*

## 6.2 RISK ASSESSMENT




 *The Risk Assessment examines the risks that were identified Section 5.11, assesses risk, and recommends how to address each risk. By completing this step, the custodian will know how much risk each gap poses and what needs to be done to address risk.*

The risk rating table below shows how likelihood and impact are combined to arrive at risk ratings. It uses the risk ratings of Low, Moderate and High identified in Section 1 of this PIA to measure likelihood and impact for each risk identified in Section 5.11 and arrives at a risk rating for each. The Recommendation column identifies recommended actions for addressing the risk.

The Risk Assessment table applies the Low, Moderate and High values described in Section 1 of this PIA to the risks identified in Section 5.11.

**Table 5: Risk Rating Table**

Likelihood	Impact		
	Low	Moderate	High

	 Low likelihood + Low Impact = <b>Low</b> Risk Rating	 Low likelihood + Moderate Impact = <b>Low to Moderate</b> Risk Rating	 Low likelihood + High Impact = <b>Moderate</b> Risk Rating
Low	Low	Low to Moderate	Moderate
Moderate	Low to Moderate	Moderate	Moderate to High
High	Moderate	Moderate to High	High

 The Risk Ratings can be colour coded if desired for more impact.

The recommendations for responding to risk can be any of the following:

Avoid – The level of risk may be reduced by removing the specific risk cause;

Transfer – The level of risk may be reduced by moving the accountability for the risk to another entity, e.g. potentially some risk items could be borne by other stakeholders;

Reduce – The level of risk may be reduced by choosing to implement additional privacy safeguards; and

Accept – The level of risk may be accepted by reviewing and understanding the risk without implementing recommendations; this choice is unlikely for personal health information.





The custodian completes Table 6 Risk Assessment below, starting with the list of risks from the final column in Section 5.11. The custodian then assesses the likelihood and the impact of the risk according to the rating scheme described below. The custodian can use the risk rating scheme in Table 5 to rate likelihood, impact and risk rating or the custodian can use a more detailed rating scheme. The custodian can attach number values to ratings if preferred.

Note: The definitions for risk used below are the same as the definitions in Section 1, the Introduction; if the custodian uses a different rating scheme, the definitions in Section 1 should be changed.

**Likelihood** means the likelihood that an event will occur. The following definitions apply to rating the likelihood of an event:

- **Low:** There is little history of such an event inside the organization and the threat is considered unlikely to occur.
- **Moderate:** There is some history inside the organization or elsewhere and the threat could occur.
- **High:** There is significant history inside the organization or elsewhere and the threat is likely to occur.

**Impact** means the magnitude of damage should the event occur. Impact can be on the custodian, on the owner of the personal health information or on both. Impact can include loss of reputation, embarrassment, financial loss, loss of livelihood, or other negative consequences. The magnitude of the impact may be difficult to measure: something that has a low impact on a large custodial organization may be significant to a small organization. **Defining impact** will help the custodian's employees and third party partners and stakeholders to understand the consequences of failing to apply privacy safeguards and demonstrates to other organizations how the custodian has arrived at conclusions about risk. Impact can be described as Low, Moderate or High:

- **Low:** Little or no damage could result if the event occurs.
- **Moderate:** Serious damage could result if the event occurs.
- **High:** Extremely serious damage could result if the event occurs.






Once likelihood and impact have been rated, the custodian can arrive at a **Risk Rating** of Low, Moderate or High:

**Low:** *There is a possibility that a risk will materialize but there are mitigating factors; exposure is Low.*

**Moderate:** *There is a strong possibility that a risk will materialize if no corrective measures are taken and/or the consequences will be serious; exposure is Moderate.*

**High:** *There is a near certainty that the risk will materialize if no corrective measures are taken and/or the consequences will be extremely serious.*


Table 6: Risk Assessment

Risk		Likelihood	Impact	Risk Rating	Recommendation
Risk ID	Description				
 Copy the risk ID and the description of the risk identified in Section 5.11 into this column. The text in the next row is an example.		 Based on an analysis of similar organizations and experience, gauge the likelihood of the event occurring; enter its rating and a brief description of what the rating is based on. The rating and text below are examples.	 Assess the impact of the event; enter its rating and a description of what the rating is based on. The rating and text below are examples.	 Combine likelihood and impact and enter the risk rating. The rating and text below are examples.	 Recommend how to address the risk: avoid, transfer, reduce, or accept. The recommendation should aim to address likelihood, impact or both. More than one recommendation may be required. The recommendation and text below are examples.
A-1	With no terms of reference, the Privacy Officer may neglect some important duties such as ensuring that employees,	Moderate  Over time or with a new appointee,	High  The potential is for widespread	Moderate to High  Exposure is	<b>Reduce:</b> Prepare detailed terms of reference for the Privacy Officer and use them to review performance annually. This will



Risk		Likelihood	Impact	Risk Rating	Recommendation
Risk ID	Description				
	contractors and others are informed of their duties under PHIA, or responding to public inquiries. Ignorant employees, contractors or others may violate any aspect of PHIA.	it is reasonable to expect some duties to be neglected.	harm to patient privacy and to the organization's reputation that would arise from failure to execute the requirements of PHIA from a highly visible position in the organization.	rated at this level, given the likelihood and impact of this event occurring.	reduce the likelihood of the event.

### 6.3 RECOMMENDATIONS

The recommended safeguards aim to reduce residual privacy risk to <Insert target risk level> by strengthening existing and planned privacy safeguards. Annex C fully describes each recommended privacy safeguard listed in Table 4 below.

 *The custodian can list each recommendation with the privacy principle that it applies to. The list of recommendations will form **the starting point** for the action plan in Section ; the custodian can also use Table 7 in the Executive Summary.*

**Table 7: Summary of Recommendations**

Privacy Principle Addressed	Recommendations
 <i>Insert the privacy principle and the specific requirement addressed by the recommendation. This helps to focus the analysis on the requirement.</i>	 <i>List the recommendation(s) that address(es) the principle.</i>
Accountability:	Detailed Terms of Reference for Privacy Officer

---

## 7 ACTION PLAN









The **Action Plan** is the second element of the custodian's response. It is a prioritized list of activities and target dates for implementing the recommendations listed in Section 6. Each element of the plan can be set out in separate tables, in order of priority, as in the sample table below. Note that each table provides an "Accept" column.

*This Section can include a Gantt chart or similar graphic to depict the activities, dependencies and relationships.*

*The custodian can use the Action Plan to review or audit the implementation of privacy safeguards. The custodian can also use the Action Plan to report its compliance with PHIA or other requirements to partners, stakeholders or oversight bodies.*

<Insert introductory description of the action plan that will implement the recommendations from Section 6>

No: <Sequential #>		Requirement Addressed: <Insert Privacy Principle and specific requirement>		Privacy Safeguards Category: <Insert Category, e.g. Management, Business, Operations, Technical, Security>	
Activity Name: <Name of Activity that will implement specific recommendations from Section 6>					
Activity Description: <Description of the activity that will implement specific recommendations from Section 6>					
Resource Requirements: <Insert estimated total of days effort and/or estimated total cost for completing this activity>					
Recommendation Number	Recommendation Title	Costs and Resources Required	Target Date	Accept (Yes/No)	Organization
 Enter the cross reference number from Annex C	 Enter the name of the recommended privacy safeguard from Annex C	 Enter costs and list resources	 Enter target date of completion	 Enter Yes or No	 Enter name of organization that is responsible for completing the activity.

No: <Sequential #>		Requirement Addressed: <Insert Privacy Principle and specific requirement>		Privacy Safeguards Category: <Insert Category, e.g. Management, Business, Operations, Technical, Security>	
--------------------	--	--	--	--	--

Activity Name: <Name of Activity that will implement specific recommendations from Section 6>					
Activity Description: <Description of the activity that will implement specific recommendations from Section 6>					
Resource Requirements: <Insert estimated total of days effort and/or estimated total cost for completing this activity>					
Recommendation Number	Recommendation Title	Costs and Resources Required	Target Date	Accept (Yes/No)	Organization

No: <Sequential #>	<b>Requirement Addressed:</b> <Insert Privacy Principle and specific requirement>		<b>Privacy Safeguards Category:</b> <Insert Category, e.g. Management, Business, Operations, Technical, Security>		
Activity Name: <Name of Activity that will implement specific recommendations from Section 6>					
Activity Description: <Description of the activity that will implement specific recommendations from Section 6>					
Resource Requirements: <Insert estimated total of days effort and/or estimated total cost for completing this activity>					
Recommendation Number	Recommendation Title	Costs and Resources Required	Target Date	Accept (Yes/No)	Organization



## Annex A – Information Resources



*The custodian can list the information sources used to prepare the PIA. The tables below are suggested formats. Listing information resources contributes to the credibility of the PIA and demonstrates the custodian's thoroughness.*

The table below lists the persons who contributed directly to this PIA.

Personnel	
Name	Area of Responsibility

The table below lists the documents used in preparing this PIA.

Documentation

## Annex B – Legislation and Policy



*The custodian can list the legislation, policy, codes of conduct, professional ethics or contracts that apply to the organization, system or project and its protection of personal health information. Providing links to web sites can make it easier for readers to find legislation and policy. The custodian can use this annex as a checklist when conducting reviews or audits of privacy safeguards.*

## Annex C – Privacy Safeguards

The table below list privacy safeguards, and organizes them into categories. Privacy safeguards are listed as existing, planned or recommended. Together, they reduce risk to personal health information for the [Project Name] system to the target risk level of **Low**.



*The **Privacy Safeguards** table below is an example of how the custodian can organize privacy safeguards, which the custodian enters during the development of Sections 2 to 4 of the PIA or during the completion of Section 5. It is an example only.*





*The custodian can consider the list as an inventory of the measures that the custodian uses to make sure that personal health information is protected throughout its life cycle, as required by the Personal Health Information Act. The privacy safeguards may consist of policies, procedures, processes, agreements, training or any other measure or combination of measures that can effectively reduce risk that the custodian's operations, system or program will inappropriately collect, use, disclose, retain or otherwise mismanage personal health information*

*The custodian can assign a privacy ID number to each privacy safeguard for quick cross reference; the description can consist of a title and a full description of the privacy safeguard. The status will be one of existing, planned or recommended.*

*The custodian consults the list of privacy safeguards when completing the Privacy Risk Assessment in Section 5.*

*The custodian can use the privacy safeguards list as a **checklist** for future privacy reviews and audits.*

Privacy ID Number	Description	Status
-------------------	-------------	--------

Privacy ID Number	Description	Status
Policy and Accountability		
100	[Organization Name] Personal Health Information Policy The privacy policy sets out responsibilities for collecting, using, disclosing and disposing of personal health information. The policy is reviewed annually.	<div>  <i>Labelling the status as "Existing" indicates that it is in place.</i> </div> <div>Existing</div>
101	[Project Name] Reporting Relationships The project has provided for privacy input from the [Organization Name] access to information and privacy officer, including review of processes and procedures.	<div>  <i>Labelling the status as "Planned" indicates that it is not yet in place but will be implemented.</i> </div> <div>Planned</div>
102	Privacy Officer The privacy contact for personal health information is xxxx.	Existing
103	<div>  <i>This privacy safeguard has been added to address a deficiency under the Accountability principle.</i> </div> <div>Detailed Terms of Reference for Privacy Officer</div>	<div>  <i>Labelling the status as "Recommended" indicates that it was</i> </div>

Privacy ID Number	Description	Status
	The Privacy Officer for personal health information is xxxx. The privacy officer's duties and responsibilities are described in [Name of document] and comply with PHIA; a copy is available at <a href="http://www.xyz123.org">www.xyz123.org</a> . The terms of reference are used to review the Privacy Officer's performance annually.	<i>added to address a deficiency.</i>
		Recommended
Directives and Standards		
200	Directive for secure disposal of media Secure disposal of media is required to ensure that personal health information does not reside on hard drives or removable media when they are no longer required.	Recommended
201		
Business Operations		
300	Secure shredders Employees have convenient access to cross-cut shredders, which are used to destroy paper documents when they are no longer required. The shredders meet RCMP standards for shredding sensitive information.	Existing
Technical Security Safeguards		

Privacy ID Number	Description	Status
400	Data Encryption All data in transit will be encrypted using 256 bit encryption. Stored data will not be encrypted.	Planned
Training and Awareness		
500	Health Privacy Awareness All employees are required to participate in health privacy awareness sessions or to use on-line awareness packages. Supervisors monitor employee participation.	Existing
Review and Audit		
600	PIA Audits The Privacy Officer will audit privacy impact assessments following implementation of recommended safeguards to verify that all recommended privacy safeguards are in place and to assess their effectiveness.	Planned