Privacy Impact Assessment

Personal Health Information Act

What is a Privacy Impact Assessment?

The *Personal Health Information Act (PHIA)* sets out mandatory requirements relating to personal health information held by custodians. *PHIA* also requires that custodians protect the confidentiality of personal health information, and the privacy of the individual who is the subject of that information. This includes protecting the personal health information from theft, loss and unauthorized access to, use of, disclosure, copying, modification or disposal.

A privacy impact assessment is a tool to identify risks and mitigation strategies associated with the use of personal health information. It is an essential tool for ensuring compliance with the privacy requirements set out in *PHIA* and is a building block of a good privacy management program.[1]

When Should I Complete a Privacy Impact Assessment?

You should complete a privacy impact assessment (PIA) for all new systems, projects, programs or activities. PIAs should also be completed when any significant changes are being contemplated to projects, programs or systems. PIAs are "evergreen". This means that they should be completed at the conceptual, design and implementation phases of each project and should be periodically reviewed to ensure that no new risks have emerged and to confirm that all mitigation strategies have been properly implemented. This PIA template was created by the Office of the Information and Privacy Commissioner for Nova Scotia and it incorporates elements of a number of existing templates.

Notice to Users

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP, MGA* and *PHIA* the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any proposal from a public body or health custodian. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Information and Privacy Commissioner for Nova Scotia will keep an open mind. It remains the responsibility of each public body or health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca/

[1] For more information about privacy management programs visit the website of the Office of the Information and Privacy Commissioner website at: https://oipc.novascotia.ca/

Privacy Impact Assessment

Project Name: _____

Document Version, Review and Approval History

Version	Author	Nature of Change	Date

Document Owner

Name	Organization	Title

Document Sign-Off

Name	Organization	Title	Signature	Date

Table of Contents

A. General Information

1. **Name of Program or Service**

2. **Name of Department, Branch and Program Area**

3. **Name of Program or Service Representative**

4. **Contact Information**

5. **Key Program or Service Dates**

List key program and service dates including those listed in the table below:

Milestone	Due Date	Completion Date
Project initiation		
PIA Commencement		
PIA Completion		
PIA Review		
Threat & Risk Assessment		
Vendor Conformance testing		
Go Live Date		

B. Description

1. **Description of the Initiative:** Provide a summary of the program, project activity or system. Describe its purposes, goals and objectives. Explain the need for the new program, project or system and its benefits.

2. **Scope of this PIA:** Explain what part or phase of the initiative the PIA covers and what it does not cover.

3. **Conceptual Technical Architecture:**

   a. Logical Architecture - describe
   b. Technical Interfaces - describe

4. **Elements of Personal Health Information**: List the personal health information data elements involved in the initiative. This could include citizen's name, family member names, age, address, educational history, work status, health information, test results, clinical notes, financial information, photos, personal health card number.

5. **Description of Information Flow (include text and diagram)**:

   Describe the following information flows:

   (i) Intended information flow for the new project, program or system. Insert information flow diagram here (see sample at Appendix A). Describe the purposes for collection, use and disclosure of personal health information (PHI) as illustrated.

   (ii) If planned, describe how a pilot phase and/or limited roll out flow will occur.

   (iii) Describe:

   - How the system will implement a patient's requests for her own PHI.
   - How the system will implement consent directive to mask PHI.
   - How the system will process a record of user activity request.
   - How the system vendor will provide business/technical support.

   As noted above, attach an information flow diagram showing how information will be collected and disclosed as a result of the initiative. See **Appendix A** for a sample information flow diagram.

If your initiative will not involve the collection, use or disclosure of personal health information, you can stop here and submit this document to your privacy officer.

C. Collection, Use and Disclosure of Personal Health Information

1. **Limiting Collection, Use and Disclosure:** Privacy is a fundamental right of citizens and so any limitation on the privacy of citizens should be carefully analyzed to ensure such limitation is warranted. If your project involves highly sensitive personal information, a broad collection of personal information or a serious impingement on privacy, answer the following four questions before proceeding:

   a. **Is the measure demonstrably necessary to meet a specific need?** At a minimum, the objective must relate to societal concerns which are pressing and substantial in a free and democratic society. To be "demonstrably necessary" the custodian should explain the rational connection between the specific need and the project.

   b. **Is it likely to be effective in meeting that need?** Provide empirical evidence to support the initiative.

   c. **Is the loss of privacy proportional to the need?** Explain how the collection, use and/or disclosure of personal health information will be undertaken in the least privacy invasive manner possible. Minimizing the number of data elements collected, limiting access to the data and short retention periods are all examples of reducing the privacy invasive impact.

   d. **Is there a less privacy invasive way of achieving the same end?** Explain what other less privacy invasive methods have already been tried to meet the identified need.

Based on this analysis you may decide you do not need to collect, use or disclose personal health information for your project. You may decide to reduce the data elements (you need to go back and redo part B before proceeding) or you may determine that you can justify the scope of your collection, use and/or disclosure and so proceed to question C. 2.

2. **Legal Authority for the Collection, Use and Disclosure of Personal Health Information:** For each of the collection, use and disclosures identified, evaluate the health custodian's legal authority and complete the following table. Refer to **Appendix B** for a sample of the legal authority tables.

   For each type of personal health information collected, complete the following table. Group personal health information types in broad categories such as: client demographic information, medications, test results, allergies and intolerances information, patient observation information, immunization information, etc.

Data element	**Rationale for collection, use or disclosure**		**Method of collection**	
	Consent (identify lawful purpose)	Permitted or required by law (identify law)	Direct	Indirect (state authority)

3. Legal Authority for Storage or Disclosure Outside the Province

Section 44 provides that a custodian may disclose personal health information about an individual collected in the province to a person outside the province in limited circumstances.

- **a.** Will personal health information be disclosed or stored outside of the province?
- **b.** If so, describe the circumstances, reason and the legal authority for disclosure or storage outside of the province (refer to sections 44(1) (a) – (e)).

D. Access Rights for Individuals

1. Access to Information Requests (s. 71)

Using a diagram and narrative steps explain how the custodian will respond to requests by patients for access to their own personal health information.

2. Correction and Accuracy (ss. 85-99)

- **a.** How is an individual's information updated or corrected?
- **b.** If personal health information has been disclosed to others, how will the custodian notify them of the update or correction?

3. Consent Directives (s. 17)

Describe how the system will implement consent directives to limit (mask) or revoke an individual's consent to the collection, use or disclosure of personal health information?

4. Record of User Activity (s. 63)

Describe how the system will process a record of user activity request.

5. Retention (s. 50, Reg. s. 11(3))

- **a.** Confirm that the custodian has an approved written retention schedule that applies to the personal health information affected by this project (s. 50).
- **b.** How will the custodian ensure that the retention schedule is regularly applied to personal health information collected by virtue of this project?
- **c.** Confirm that the custodian has an approved written retention schedule that includes a requirement that information that was used to update a record of user activity related to an individual's personal health information is retained for at least one year after each date of access (Reg. s. 11(3)).

6. Access or Privacy Complaints (s. 91, s. 62)

- **a.** Describe how individuals will be informed of their rights to make an access or privacy complaint to the Information and Privacy Commissioner.
- **b.** Confirm that the custodian has an approved complaints policy (s. 62(2)).

E. Security of Personal Information (s. 62, s. 65, Regulation s. 10)

1. **Reasonable Security:** *PHIA* requires that custodians protect personal health information by making reasonable security arrangements against such risks as theft, loss, unauthorized access, use, disclosure, copying or modification of information. (s. 62).
    a. **Administrative Safeguards** – Describe administrative safeguards (such as policies, training, contract provisions, consent forms, etc.).
    b. **Technical Safeguards**
        i. Describe technical safeguards (such as passwords and user ID, authentication, encryption, firewalls and intrusion detection, secure transmission, disaster recovery).
        ii. Describe all additional technical safeguards implemented in compliance with Regulation s. 10 (network infrastructure, hardware, software).
    c. **Physical Safeguards** – Describe physical safeguards (such as secure access, laptops secured to desk, alarm systems).
    d. **Auditing** – Describe auditing capability and strategies (audit logs, records of user activity, proactive and focused audit capacity).

If your initiative involves the creation of a new system, complete and append a security threat and risk assessment. As part of that assessment, you may also need to complete vulnerability and penetration testing.

2. **Access Matrix (s. 25):** Personal health information should only be used and disclosed as permitted under *PHIA*. Access to personal health information must be limited to those employees whose job responsibilities require that they access the personal health information (need to know). Attach a copy of the user access matrix. A user access matrix lists all of the position types (e.g. clerical, head nurse, nursing assistant) across one axis and all of the personal health information types (or file types or data modules) across the other. The matrix will identify by position which individuals will have access to the identified data.

F. Risk Identification & Mitigation

Assess the impact on privacy, confidentiality and security of personal information as a result of the new program or service or change and make recommendations for mitigation of privacy risks. See **Appendix C** for examples of risks and mitigation strategies.

Risk Mitigation Table

	Risk	Mitigation Strategy	Likelihood	Impact
1				
2				
3				
4				

G. Action Plan

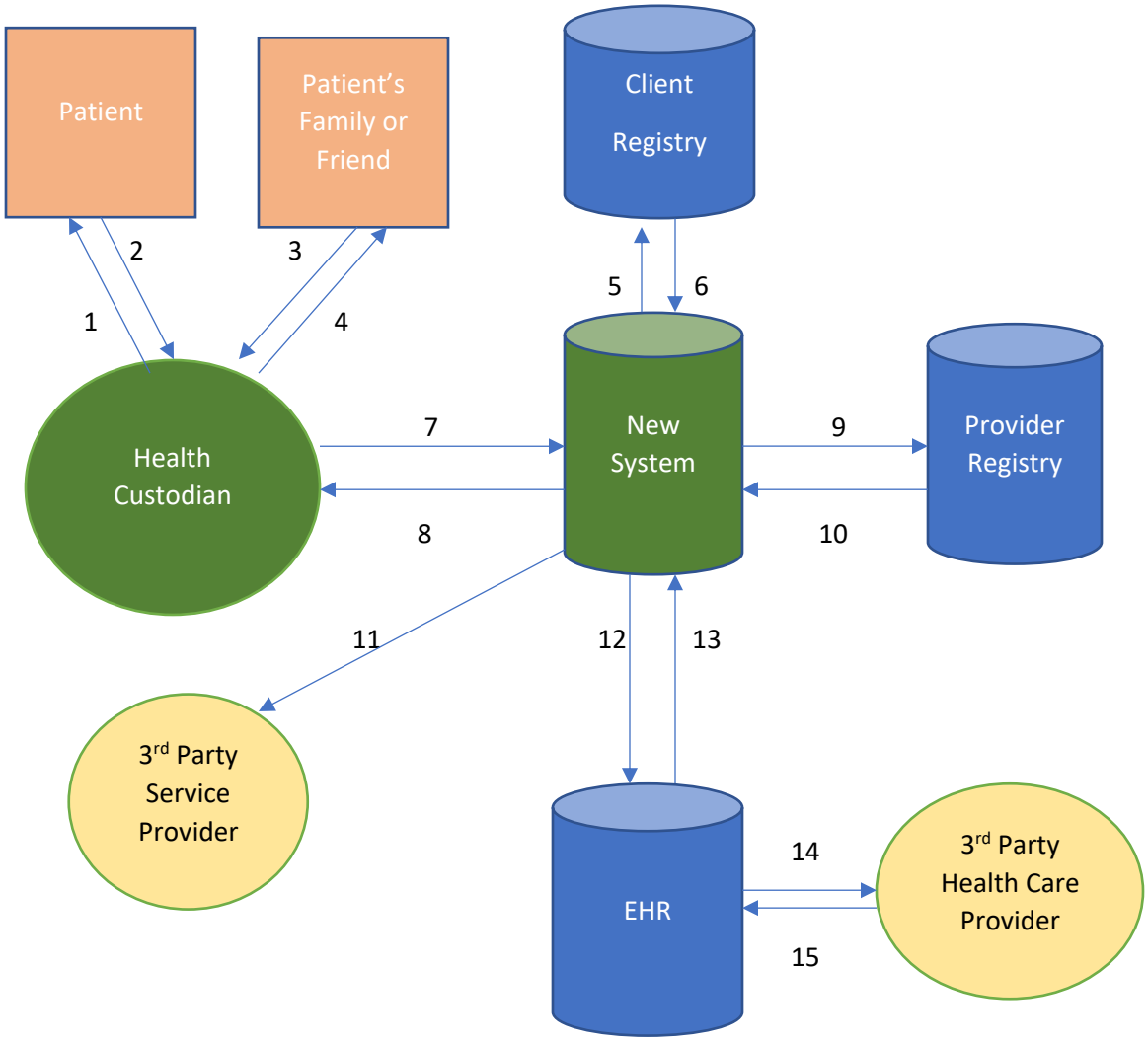
The purpose of this section is to provide an action plan to implement the recommendations listed in section F to reduce the privacy risks that have been identified. This section will provide a mechanism to track the recommendations, as well as describe responses to the recommendations of the PIA. Ensuring the recommended mitigations are implemented according to the action plan is the program area's responsibility and may be followed-up by the privacy officer at any point.

Privacy Risk Action Plan		
Risk	**Mitigation Strategy & Steps Required**	**Responsible Employee & Date to be Achieved**

PIA Review Date: _____

PIAs require regular review to ensure that the system, project or program has not substantially changed and to ensure that mitigation strategies have been properly implemented. In addition, changes in other areas (such as technology or the implementation of other related programs) may create new risks that should be identified and mitigated. Typically, the review date is selected based on the action plan – within six months of the final required completion dates is a good standard to use.

Appendix A: Sample Flow of PHI



In the narrative, explain each arrow into new system (collection) and each arrow out (disclosure).

Appendix B: Sample Summary of Authorities Under *PHIA*

Client Demographic Information

Data element	Rationale for collection, use or disclosure		Method of collection	
	Consent (identify lawful purpose)	Required by law (identify law)	Direct	Indirect (state authority)
Client name	Required to correctly identify the individual		√	
Client HCN	Same		√	√ Consent, if individual unable to recall get from Client Registry
Client date of birth	Same		√	

Immunization Information

Data element	Rationale for collection, use or disclosure		Method of collection	
	Consent (identify lawful purpose)	Required by law (identify law)	Direct	Indirect (state authority & source of data)
Adverse reaction indicator	Required to provide service			√ Consent – client authorized indirect collection from DIS
Immunization date	Required to provide service		√	√ Consent – when client unable to recall dates, from immunization data base (specify)
Immunization type	Required to provide service		√	√ Consent – when client unable to recall dates, from immunization data base (specify)

Audit Log Information

Data element	Rationale for collection, use or disclosure		Method of collection	
	Consent (identify lawful purpose)	Required by law (identify law)	Direct	Indirect (state authority & source of data)
Date/time of record access		63(1) *PHIA* To identify date & time the access to the patient record occurred		System generated (upload), s. 31(k) & s. 63(1) *PHIA*
Description of access (type of transaction)		63(1) *PHIA* Description of type of access to allow assessment of authorization to access		System generated, s. 31(k) & s. 63(1) *PHIA*
User ID		63(1) *PHIA* To identify user		System generated, s. 31(k) & s. 63(1) *PHIA*
User name		63(1) *PHIA* To identify user		System generated, s. 31(k) & s. 63(1) *PHIA*
User location ID		63(1) *PHIA* To identify user location – assists with assessing authorization		System generated, s. 31(k) & s. 63(1) *PHIA*
Patient ID		63(1) *PHIA* unique patient ID assigned in patient registry		User input or system generated, necessary to create audit log 31(k) & s. 63(1) *PHIA*
Patient name		63(1) *PHIA* first and last name of patient		User input, necessary to create audit log 31(k) & s. 63(1) *PHIA*

Appendix C: Sample Risk Identification & Mitigation Table

You will need to adopt a scale to measure likelihood and impact. High, medium and low will do or you can choose a numerical scale for greater subtlety in choice.

	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1	Authorized user views record for personal reasons	• Log all read only and change activity • Monitor logs regularly, conduct spot audits and ensure audit capacity in response to complaints • Oath of employment and confidentiality agreements • Training	Likelihood increases with more users	• More sensitive data results in higher impact • More data exposed by incident results in higher impact
2	Service provider fails to report privacy breach to custodian	Contractual terms: • Require reporting within 24 hours • Impose penalties for failure to report and late reporting • Require the service provider to log all read only and change activity and to monitor the logs regularly • Permit the custodian to conduct audits and to review service provider audit logs	• Experience with the service provider may help determine this • Severity of consequences for service provider may lower the likelihood	Same considerations as above
3	Client's personal health information is compromised when transferred to the service provider	Transmission is encrypted and over a secure line	Low – depending on the quality of the encryption	Same considerations as above