

The *Personal Health Information Act* Risk Management Toolkit

Short Form Privacy Impact Assessment

What is a Short Form Privacy Impact Assessment?

The Short Form Privacy Impact Assessment (“PIA”) helps custodians to identify the effects that a process or system might have on the privacy of an individual. Short Form PIAs also identify ways in which adverse privacy risks can be managed. A Short Form PIA is desirable when assessing the following types of risks in health care:

- Risks arising from a new technology or the convergence of existing technologies;
- Risks arising from the use of a known privacy-intrusive technology in new circumstances;
- Risks arising from a new project; and
- Risks arising from a significant change in information handling practices.

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, the people who will have access to the personal health information, and under what legal authority they intend to make a particular collection, use or disclosure. The Short Form PIA will help to document the “data flows” of the activity and will act as a record of the administrative, technical and physical protections of the personal health information that is collected, used and disclosed.

A completed Short Form PIA becomes a management tool for custodians as it helps to identify where new or updated policies are required and informing the decision to expand an activity to new users or collect more information.

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

The Short Form 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.

Short Form Privacy Impact Assessment questionnaire

If you have determined that your organization is a health information custodian and that the proposed or existing information system, technology or program with which are you dealing involves personal health information as defined under the provincial *Personal Health Information Act* ("PHIA"), you are ready to complete the Short Form PIA questionnaire.

The questions you will see in the Short Form PIA questionnaire ask for information in two forms. First, the health information custodian must complete checkboxes, which provide summary responses to the questions posed in the questionnaire. The categories for the checkboxes are:

- "Yes"
- "In Progress"
- "No"
- "N/A" ("Not Applicable" or "Not Available").

Second, "note fields" or free text fields provide for elaboration of responses to the checkboxes as the health information custodian feels is appropriate. In addition, the questionnaire has a column to provide for cross-references to separate enclosures on specific responses, which the health information custodian may wish to include as supporting information. Examples of separate enclosures may include written materials about the information system, technology or program, such as the business case, project charter, technical specifications, excerpts from system manuals and interviews with relevant personnel, including vendors where appropriate. This type of information should be cited in the "Enclosure Reference" column. The health information custodian may use the note fields and enclosures in combination or

interchangeably. The Short Form PIA questionnaire can be completed in paper or electronic format.

“Note fields” versus “enclosure references”

Whether you provide your answers to the questions in the note fields or in separate enclosures is not important. What is important, however, is to do more than just check off a “Yes,” “No,” “In Progress” or “N/A” in the questionnaire’s checkboxes. In other words, you should use the note fields, the separate enclosures or both, but do NOT simply fill in the checkboxes and fail to provide any information about why you have made certain choices for those checkboxes.

One of the characteristics of a valuable Short Form PIA is that it not only clearly states how personal health information for an information system, technology or program is or will be collected, used, disclosed, retained and protected but it also clearly explains why the personal health information is or will be collected, used, disclosed, retained and protected in *specific* ways, and what broader organizational privacy management practices are in place to support those choices. In most cases, only supplementary information provided in the note fields and / or in separate reference enclosures will fulfill the latter requirement.

Organizational Privacy Management versus Project Privacy Management

The Short Form PIA questionnaire is broken into two parts: Part A, Organizational Privacy Management, and Part B, Project Privacy Management. Part A relates to the health information custodian’s information practices as a whole, while Part B relates specifically to the privacy practices of the proposed or existing information system, technology or program for which the Short Form PIA is being completed. Once a health information custodian has completed the entire questionnaire once for any information system, technology or project, Part A will likely only need to be revised for continued accuracy during the completion of each subsequent Short Form PIA, not completed anew.

**Personal Health Information Act
Short Form Privacy Impact Assessment Questionnaire**

PART A: Organizational Privacy Management

The questions in this section relate to privacy management throughout your organization. They are not limited to the information system, technology or program. Specific questions related to the information system, technology or program appear in Section B.

Remember to identify the relevant section or page(s) of any materials you reference in the "Enclosed Reference" column, whenever you provide an enclosure. In this regard, you may want to number the pages of your enclosure sequentially from beginning to end, for ease of reference; this is particularly important if external stakeholders / entities will be reviewing your PPIA, since these entities are less likely to be familiar with the details of the proposed information system, technology or program.

#	Question	Yes	In progress	No	Not applicable	Enclosed / reference
<p>The questions in this section of the Short Form PIA questionnaire relate to privacy management throughout your <u>organization</u>; they are not limited to the information system, technology or program being assessed. Questions related to the specific <u>information system</u>, <u>technology</u> or <u>program</u> appear in Section B.</p>						
A.1	Is there an organizational strategic plan or business plan that addresses privacy protection?					
<p>NOTES – A.1: Health information custodians often address privacy considerations in their information management / information technology plans. Some custodians may also have departmental business or strategic plans; if such plans address privacy issues, they may also be enclosed. (e.g. a business plan for a new health information system, a new clinical department, a new fundraising initiative or a new research program may include information that addresses privacy protection).</p>						

A.2	Does your organization have a written privacy policy or statement of information practices?					
<p>NOTES – A.2: Question A.1 refers to organizational plans that include privacy measures; question A.2 refers to a policy or mission statement that is specifically related to the information handling practices and protection of privacy within your organization as a whole. Such documents are often referred to as privacy or information practices policies or charters, and are required under section 13 of <i>PHIA</i>. Documents that are responsive to this question will normally apply to the entire organization, not just to a specific business area or project.</p>						
A.3	Have privacy policies or procedures been developed for various aspects of the organization's operations?					
<p>NOTES – A.3: This question relates to privacy-related policies or procedures applying to <u>specific aspects</u> of the organization's operations – to specific or initiatives or projects, for example. Such policies or procedures, if they exist, are typically separate from organization-wide privacy policies or charters, which are dealt with in question A.2. Privacy policies or procedures applying to specific aspects of the organization's operations may form part of the broader policies or procedures dealt with in question A.2. If so, please indicate in "encl. ref." field where in the enclosure this information may be found.</p>						
A.4	<p>Do the privacy policies or procedures that you identified in response to questions A.2 and A.3 ensure the following?</p> <ul style="list-style-type: none"> ▪ Personal health information is collected in accordance with <i>PHIA</i> and other applicable legislation; ▪ Individual consent is obtained in accordance with Part III (sections 23 - 28) of <i>PHIA</i>, 					

	<p>where consent is required;</p> <ul style="list-style-type: none"> ▪ A written public statement about the organization's information practices, who to contact with privacy questions or complaints, and how to obtain access to or request correction of a record of personal health information, is readily available to individuals as outlined in section 19 of <i>PHIA</i>; ▪ Individuals are entitled to request access to and correction of their own personal health information as provided for under Part V (sections 51 - 64) of <i>PHIA</i>, subject to certain exceptions; ▪ There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained as well as procedures outlining the manner by which personal health information will be securely destroyed. 					
<p>NOTES – A.4: This question relates to several key aspects of the contents of various policies or procedures that may have been identified in questions A.2 and A.3. The individual bullet points in this question are key elements of <i>PHIA</i> and are generally-accepted fair information practices.</p>						
A.5	Are administrative, technical and physical safeguards in place at the organization to protect personal health information against theft, loss,					

	unauthorized use or disclosure and unauthorized copying, modification or disposal pursuant to section 15 of <i>PHIA</i> ?					
<p>NOTES – A.5: This question relates to whether or not your organization has in place administrative, technical and physical safeguards. These types of safeguards are critical to minimizing privacy risks and protecting the confidentiality and integrity of personal health information. If your organization has developed an information security plan or policy, you should enclose a copy of the plan in your Short Form PIA in response to this question.</p> <p><i>**If your organization adheres to a generally accepted industry or government standard for information security, such as ISO 17799 / 27002, you should identify that standard in your elaboration for this question and indicate whether your organization has been certified.</i></p>						
A.6	Is there an appointed privacy contact person in the organization, in accordance with section 18 of <i>PHIA</i> ?					
<p>NOTES – A.6: If no person has been assigned overall responsibility for privacy issues in the organization, check “No.” However, note that section 18 of <i>PHIA</i> requires that custodians of health information have a privacy contact person. If your organization has identified a privacy contact person, you should specify in the notes field which position has been designated as the person with overall responsibility for privacy issues (e.g. Chief Privacy Officer, Chief Information Officer, etc.).</p>						
A.7	Does a reporting process exist to ensure that the organization’s management is informed of any privacy compliance issues?					
<p>NOTES – A.7: If a policy or procedure exists to report privacy compliance issues, you should enclose a copy of this policy or procedure in your Short Form PIA. If none exists, your Short Form PIA should describe how, when and at what level management would be informed of any alleged or actual failures to comply with <i>PHIA</i>, other applicable legislation or policies in regard to privacy protection.</p>						

A.8	Are senior executives actively involved in the development, implementation and/or promotion of your organization's privacy program?					
<p>NOTES – A.8: If senior executives are involved in your organization's privacy program, you should describe the nature of their involvement. If your organization has a privacy contact person, you should also describe the nature of his or her reporting relationship and position within the organization, including how closely they work with your organization's senior executives.</p>						
A.9	Are employees or agents with access to personal health information in your organization provided with training related to privacy protection?					
<p>NOTES – A.9: Under section 14 of PHIA, a custodian must ensure that its 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 comply with:</p> <p>(a) PHIA and the regulations; and</p> <p>(b) the custodians information policies and procedures (refer to section 13 of PHIA).</p> <p>A custodian also has to ensure that its 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 the information policies and procedures referred to in section 13.</p> <p>If your organization does not have any form of privacy training in place, select "no." However, note that one of the responsibilities of your organization's privacy contact person (see question A.6) is to ensure agents are appropriately informed of their duties under PHIA. Your Short Form PIA should identify any privacy-related training that your organization's employees or agents undergo. Specific training information related to the information system, technology or program should be provided in response to question B.15 in the next section of the questionnaire. The information you provide on privacy training should note the length and frequency of training,</p>						

which categories of employees or agents receive training, and how the organization documents the fact that an employee or agent has received privacy training.					
A.10	Have policies and procedures been developed concerning the management of privacy breaches, including the notification of individuals when the confidentiality of their personal health information has been breached?				
<p>NOTES – A.10: This question relates to the process following the determination that an inappropriate use or disclosure of personal health information has occurred. Such breach management processes are customarily set out in policies and will typically outline the reporting and accountability structure for a breach. Such policies will also set out procedures for notifying individuals whose personal health information was the subject of the breach and, where applicable, the Newfoundland and Labrador Privacy Commissioner. Section 15(3) of <i>PHIA</i> requires that health information custodians notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or accessed by unauthorized persons.</p>					

PART B: Project Privacy Management

The questions in this section relate to the information system, technology or program being assessed.

#	Question	Yes	In progress	No	Not applicable	Enclosed / reference
The questions in this section relate to the information system, technology or program that is the subject of this assessment.						
B.1	Has a summary of the proposed or existing information system, technology or program been prepared, including a description of the requirements for the system, technology or program and a description of how the information system, technology or program will or does meet those needs?					
NOTES – B.1: This is an important enclosure because it provides the basic rationale for the proposed or existing information system, technology or program. This information would typically be included in the proposed or existing information system, technology or program's project charter, project plan, needs assessment or other material explaining why the information system, technology or program has been or will be implemented.						
B.2	Has a listing of all personal health information or data elements that will be or are collected, used or disclosed in the proposed or existing information system, technology or program been prepared?					
NOTES – B.2: This enclosure is important because it illustrates the scope and nature of personal health information involved in the proposed or existing information						

system, technology or program.						
B.3	Have diagrams been prepared depicting the flow of personal health information in the proposed or existing information system, technology or program?					
<p>NOTES – B.3: There are many ways to prepare data flow diagrams, and your choice will depend in part on the nature of the information system, technology or program. The data flow diagram should illustrate how personal health information is collected, how it circulates within, and how it is disseminated beyond the proposed or existing information system, technology or program.</p>						
B.4	Have documents been prepared showing which persons, positions or employee categories will have access to which elements or records of personal health information?					
<p>NOTES – B.4: This enclosure is important to illustrate the application of the “need-to-know” principle in <i>PHIA</i> and to complement the data flow diagram requested in question B.3. In some cases, it may be possible to incorporate this information into the information flow diagram for question B.3; if you have done so, you should note that fact in your response to this question as well as question B.3.</p>						
B.5	Does consent from the individual or an authorized substitute decision-maker provide the primary basis for the collection, use and disclosure of personal health information for the proposed or existing information system, technology or program?					
<p>NOTES – B.5: Under <i>PHIA</i>, there are several collections, uses and disclosures of</p>						

<p>personal health information that do not require an individual's consent (see sections 23 through 50 of <i>PHIA</i>). If individual consent does not form the basis for the collection, use and disclosure of personal health information, your Short Form PIA should identify the alternative authority that applies.</p>						
B.6	Have you documented the purposes for which personal health information will be or is collected, used or disclosed in the information system, technology or program?					
<p>NOTES – B.6: Your Short Form PIA should include any documentation which clearly sets out the purposes for which personal health information will be collected, used or disclosed. If this information has been provided in response to other questions, you may cross-reference as necessary in your Short Form PIA. This question also relates to question B.5 as, in the event consent provides the basis for the collection, use or disclosure of personal health information, section 23 of <i>PHIA</i> requires that the consent be knowledgeable; one of the elements of a knowledgeable consent outlined in section 23 of <i>PHIA</i> is that it must be reasonable in the circumstances to believe that the individual knows the purposes for which their personal health information is being collected, used or disclosed, as the case may be.</p>						
B.7	Is personal health information collected, used, disclosed or retained exclusively for the identified purposes?					
<p>NOTES – B.7: If you checked “Yes,” this question will probably require little elaboration. If you checked “In Progress” or “No,” you should elaborate and identify in your Short Form PIA any measures you will take to ensure that the collection, use or disclosure of personal health information is consistent with identified purposes. Note that section 13 of <i>PHIA</i> requires health information custodians to comply with their information practices.</p>						
B.8	Will personal health information in the proposed or existing information system, technology or program be linked or cross-referenced to other information					

	in other information systems, technologies or programs?					
<p>NOTES – B.8: If you checked “Yes” in response to this question, you should indicate how this link or cross-reference will be accomplished, who has custodianship of the information system, technology or program for which you are undertaking this Short Form PIA and an explanation of why the link or cross-reference is required, as well as the effect if such linkage or cross-reference was not possible. For the purpose of this questionnaire, “link” means to create a new combined record from two or more separate records of personal health information through the use of an identifier, and “cross-reference” means to identify a record of personal health information by using an identifier from another record of personal health information, but without creating a new record.</p>						
B.9	Will personal health information collected or used in the information system, technology or program be disclosed to any persons who are not employees or agents of the responsible organization?					
<p>NOTES – B.9: A “No” response to this question identifies an information system, technology or program for which personal health information is limited to the internal purposes of a single health information custodian. Such systems, technologies or programs may be contrasted with those in which personal health information serves the purposes of more than one health information custodian or, while serving one health information custodian, is disseminated beyond that health information custodian.</p>						
B.10	Have arrangements been made to provide full disclosure of all purposes for which the information system, technology or program will collect personal health information?					
<p>NOTES – B.10: Disclosure of the purposes to which personal health information is to be put is an important privacy protection measure, especially when consent is being sought, and is a requirement of <i>PHIA</i>. Your elaboration should identify the measures</p>						

that will be taken to ensure that this information is communicated appropriately to the individuals affected by the information system, technology or program (e.g. patients or clients). Under <i>PHIA</i> , the requirement for a consent to be knowledgeable (discussed in question B.6, above) may be satisfied in part through posting or making available a notice of purposes for which personal health information will be collected, used or disclosed, as described in section 20 of <i>PHIA</i> .						
B.11	Have communications products and/or a communications plan been developed to fully explain the information system, technology or program to individuals and how their personal health information will be protected?					
NOTES – B.11: Providing information to individuals whose personal health information will be collected, used or disclosed by the information system, technology or program about the technical, administrative and physical safeguards to protect their privacy and to maintain the confidentiality of their personal health information, will engender confidence in the information system, technology or program.						
B.12	Does the proposed or existing information system, technology or program involve the collection, use or disclosure of any personal health information outside of the province of Newfoundland and Labrador?					
NOTES – B.12: The trans-border movement of personal health information raises a number of special privacy issues, among them the application of <i>PHIA</i> , the federal <i>Personal Information Protection and Electronic Documents Act</i> , the adequacy of contractual provisions to protect privacy and the equivalence of privacy legislation in other jurisdictions. If the information system, technology or program involves the international transfer of personal health information, these issues may be further complicated. Your Short Form PIA should provide full details of any plans to transfer personal health information between Newfoundland and Labrador and any other jurisdiction.						

B.13	Has any assessment been completed to identify potential risks to the privacy of individuals whose personal health information is collected, used, retained or disclosed by the proposed or existing information system, technology or program?					
-------------	--	--	--	--	--	--

NOTES – B.13: A critical part of a Short Form PIA is a review of the possible impact that the proposed or existing information system, technology or program may have on the privacy of individuals whose personal health information may be collected, used, retained or disclosed. This is an opportunity to consider what the overall privacy impact of the system, technology or program may be. In part, this involves identifying, from the perspective of the individuals whose personal health information is involved, how the existing or proposed system, technology or program may affect their privacy interests.

B.14	If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the design and/or implementation of the proposed or existing information system, technology or program?					
-------------	--	--	--	--	--	--

NOTES – B.14: If potential privacy risks have been identified in response to question B.12 or other questions, specific measures will usually need to be taken to avert or mitigate these risks. These may include the use of privacy enhancing technologies, revising consent forms, making notices about the information system, technology or program clearer and more readily available to individuals, or implementing specific privacy training on the proposed or existing information system, technology or program. Your Short Form PIA should outline the nature of these measures in response to this question. If they have already been described in response to other questions, you may cross-reference those questions or the enclosures provided in response to those questions. Your response to this question should address any issues identified in question B.12. If no response has been taken to mitigate the risks identified, you should provide a rationale for your decision in the notes field for this question.

B.15	Has an assessment been completed to identify whether other health information custodians have implemented the same or a similar information system, technology or program, the risks to privacy experienced by other health information custodians and the means implemented by these other health information custodians to avert or mitigate these risks?					
<p>NOTES – B.15: Reviewing the experiences of other health information custodians who have implemented the same or similar information system, technology or program will assist in identifying the key privacy concerns and risks and how the other health information custodians have resolved a specific privacy challenge.</p>						
B.16	Have key stakeholders been provided with an opportunity to comment on the sufficiency of any identified privacy protections and their implications on the proposed or existing information system, technology or program?					
<p>NOTES – B.16: When a proposed or existing information system, technology or program involves large volumes of personal health information, or when that information is particularly sensitive, it is worthwhile to consult those who have privacy interests in the project. If this has been done, your Short Form PIA should provide a description of the results of such consultations.</p>						
B.17	Will users be trained in the requirements for protecting personal health information and will they be made aware of the relevant notification procedures if personal health information is					

	stolen, lost or accessed by unauthorized persons?					
<p>NOTES – B.17: Your Short Form PIA should describe your plans for training related to the privacy and security measures and policies your organization plans to implement for the proposed or existing information system, technology or program. Ensuring your agents are made aware of their data protection obligations will help ensure that the operations of the proposed or existing information system, technology or program comply with <i>PHIA</i>, including section 15, which requires agents of a health information custodian to notify the health information custodian at the first opportunity if personal health information handled by the agent on behalf of the health information custodian is stolen, lost or accessed by unauthorized persons. Note that this question deals with specific training for the proposed or existing system, technology or program – more general privacy training programs should be described in response to question A.9.</p>						
B.18	Have security policies and procedures to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal been documented?					
<p>NOTES – B.18: Your Short Form PIA should include copies of security policies and procedures related to the management of personal health information in conjunction with the proposed or existing information system, technology or program. To the extent that you are relying on organization-wide security policies and procedures, your Short Form PIA should note this and make reference to any relevant enclosures provided in response to question A.5.</p>						
B.19	<p>Do the privacy policies or procedures that you identified in question B.18 ensure the following (if so, please enclose):</p> <ul style="list-style-type: none"> ▪ Personal health information in the proposed or existing information system, technology or program is collected in accordance with 					

	<p><i>PHIA</i> and other applicable legislation;</p> <ul style="list-style-type: none"> ▪ Individual consent is obtained in accordance with Part III (sections 23 - 28) of <i>PHIA</i> for the proposed or existing information system, technology or program where consent is required; ▪ A written public statement about the purposes for which the proposed or existing information system, technology or program collects, uses or discloses personal health information is readily available to individuals as outlined in section 19 of <i>PHIA</i>; ▪ Individuals are entitled to request access to and correction of their own personal health information in the proposed or existing information system, technology or program, as provided for under Part V (sections 51 - 64) of <i>PHIA</i>, subject to certain exceptions. ▪ There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained in the proposed or existing information system, technology or program, as well as procedures outlining the manner by which personal health information 					
--	--	--	--	--	--	--

	in the proposed or existing information system, technology or program may be securely destroyed.					
<p>NOTES – B.19: This question relates to several key aspects of the contents of various policies or procedures relating to the proposed or existing information system, technology or program that may have been identified. The individual points in this question are key elements of <i>PHIA</i> and are generally-accepted fair information practices.</p>						
B.20	Does the proposed or existing information system, technology or program provide functionality for the logging of the insertion, access, modification or disclosure of personal health information as well as an interface to audit those logs for unauthorized activities?					
<p>NOTES – B.20: This question relates to the technical capability to monitor unauthorized use of the proposed or existing information system, technology or program. Logging and auditing user activities is required to protect against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal. If your answer to this question is “yes,” you should provide a general description of this functionality as well as a description of your auditing procedures. If your answer is “no” to this question, you should provide an explanation as to why the proposed or existing information system, technology or program does not include such features and what alternative means you will or have already put in place to safeguard against the unauthorized insertion, access, modification or disclosure of personal health information.</p>						