



Health and Community Services

The *Personal Health Information Act* Risk Management Toolkit

Version

1.1

Date:

February, 2011

WARNING AND DISCLAIMER

This PHIA Risk Management Toolkit has been prepared by the Department of Health and Community Services as a general guide to assist custodians of personal health information to meet their obligations under Newfoundland and Labrador's *Personal Health Information Act*.

- This Toolkit is designed to assist in complying with the law and meeting the changing expectations of patients and the public.
- The resource materials provided in this Toolkit are for general information purposes only. They should be adapted to the circumstances of each custodian using the Toolkit.
- This Toolkit reflects interpretations and practices regarded as valid when it was published based on information available at that time.
- This Toolkit is not intended, and should not be construed, as legal or professional advice or opinion.
- Custodians concerned about the applicability of privacy legislation to their activities are advised to seek legal or professional advice based on their particular circumstances.

This is the first edition of the Toolkit; a second edition may be published in due course.

ACKNOWLEDGEMENT

This PHIA Risk Management Toolkit was prepared by the Department of Health and Community Services with the assistance of several stakeholders in the province's health and community services sector. The Department would like to thank the members of the PHIA Provincial Implementation Steering Committee, the PHIA Risk Management Toolkit Working Group and the Newfoundland and Labrador Office of the Information and Privacy Commissioner for their assistance in preparing these materials.



The *Personal Health Information Act* Risk Management Toolkit

Introduction and Overview

The *Personal Health Information Act*

In the spring of 2008, the Newfoundland and Labrador *Personal Health Information Act* (PHIA) was passed by the government of Newfoundland and Labrador. It is anticipated that PHIA will be proclaimed in force in the fall of 2010. PHIA is health-sector specific privacy legislation that applies to both public- and private-sector custodians of personal health information. A copy of PHIA is available on the Government of Newfoundland and Labrador's website at:

<http://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm>.

PHIA establishes rules for the collection, use and disclosure of personal health information, and also provides individuals with the right to access and to request correction of their own personal health information. PHIA clarifies and codifies the appropriate balance between (1) protecting individuals' privacy rights and (2) using personal health information for legitimate reasons, including for the provision of health care, for planning and monitoring of the health system, for authorized health research and for reasons relating to public health and safety.

PHIA and Risk Management

PHIA establishes that custodians have an obligation to safeguard the personal health information in their custody or control. PHIA requires that custodians take steps that are reasonable in the circumstances to ensure that:

1. Personal health information in their custody or control is protected against theft, loss and unauthorized access, use or disclosure;
2. Records containing personal health information in their custody or control are protected against unauthorized copying or modification; and
3. Records containing personal health information in their custody or control are retained, transferred and disposed of in a secure manner.

The implication of this requirement is that, under PHIA, custodians must establish, implement and maintain controls to protect the personal health information in their custody or control. Custodians must regard personal health information in their custody or control as being perhaps the most sensitive information there can be about an individual, and must adopt appropriate measures to safeguard it.

Custodians should incorporate risk management processes into their projects, processes and systems as early as possible; ideally, during the design or planning phases.

The PHIA Risk Management Toolkit

One of the ways in which custodians can establish, implement and maintain controls to protect the personal health information in their custody or control is through the process of risk management. Risk management can be defined as being the identification, assessment, and prioritization of risks followed by a coordinated and efficient application of resources to minimize, monitor, and control the likelihood and impact of adverse events.

The items in this risk management toolkit are intended to:

- (1) Assist custodians of personal health information and other stakeholders in understanding their legislative- and policy-based obligations as they relate to the safeguarding of personal health information;
- (2) Assist custodians in assessing their current state of compliance with PHIA;
- (3) Assist custodians in assessing the efficacy of the physical, administrative and technological controls that they have established to protect the personal health information in their custody or control; and,
- (4) Assist custodians in identifying any gaps or areas for improvement that there might be in their physical, administrative and technological controls.

It is important to note that the use of the tools that make up this PHIA risk management toolkit is not mandatory: the tools in the toolkit are intended to be self-assessments, and custodians are not required by law to complete assessments of the type found within the toolkit. However, PHIA does require that custodians take steps that are reasonable in the circumstances to ensure that the personal health information in their custody or control is adequately protected. As such, it is critical that custodians both assess and manage the risks inherent in their operations on an ongoing basis, and the tools in this toolkit may be used to help achieve those goals.

Overview of Contents of the Risk Management Toolkit

The PHIA Risk Management Toolkit contains the following items:

1. Information Security Management Overview
2. Privacy Checklist
3. Short Form Privacy Impact Assessment
4. Long Form Privacy Impact Assessment
5. Privacy Audit

6. Privacy Breach Guidelines
7. Privacy Breach Reporting Form

1. Information Security Management Overview (See item 1 in toolkit)

The Information Security Management Overview serves as a brief introduction to the concept of information security, and sets out common information security practices that custodians of personal health information should consider when implementing their information security programs. The practices set out in this document are based on the internationally-recognized ISO 27002 information security standard published by the International Organization for Standardization (ISO), and represent the elements that make up a comprehensive information security management program.

This document is intended to provide stakeholders with a general overview of the elements of a broad, comprehensive security strategy, and to identify where risk management activities – conducting privacy impact assessments, for example – fit into security strategies.

2. Privacy Checklist (See item 2 in toolkit)

The Privacy Checklist is a simple, one-page tool intended to provide custodians of personal health information with a very preliminary idea of where their organization stands in relation to the main requirements of PHIA.

It should be noted that this checklist does not contain a detailed, exhaustive review of all of the requirements of PHIA; rather, it is intended to be a tool by which custodians can begin to familiarize themselves with the requirements of the Act. The full requirements of PHIA are described in more detail in both the Preliminary Privacy Impact Assessment and the full Privacy Impact Assessment, and custodians should familiarize themselves with the information contained in those tools.

3. Short Form Privacy Impact Assessment (See item 3 in toolkit)

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 Privacy Impact Assessment is a question-and-answer assessment in table form, which sets out in greater detail the substantive requirements of PHIA.

A Short Form Privacy Impact Assessment 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 Privacy Impact Assessment 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 Privacy Impact Assessment is, as its name implies, a short, form of a Privacy Impact Assessment. Conducting a Short Form Privacy Impact Assessment 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 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 PIAs 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.

4. Long Form Privacy Impact Assessment (See item 4 in toolkit)

A Long Form Privacy Impact Assessment is a formal, comprehensive risk management tool that identifies actual or potential risks to personal health information posed by a proposed or existing activity or process. A Long Form Privacy Impact Assessment communicates how privacy is protected and personal health information kept confidential and secure from unauthorized access. A Long Form Privacy Impact Assessment will also enable custodians to prioritize measures that will address identified risks. The Long Form Privacy Impact Assessment template is a self-assessment tool designed to guide custodians in conducting a privacy impact assessment. The template consists of a methodology and step by step guidance and examples.

The PIA process is intended to ensure 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; however, a PIA can also be completed in relation to existing processes or systems, in order to determine how a custodian meets or intends to meet its obligations under PHIA.

Conducting a Long Form Privacy Impact Assessment may be appropriate in circumstances where larger, more complex processes or systems, such as provincial information systems or multi-site operations are being assessed. The Long Form Privacy Impact Assessment might be a more appropriate risk management tool to employ in such circumstances 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. Conducting a Short Form Privacy Impact Assessment is, as its name implies, a short, form of a Privacy Impact Assessment. Conducting a Short Form Privacy Impact Assessment 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.

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 and should be discussed during the PIA process – in fact, this is one of the main goals of conducting a PIA: by conducting a PIA, issues and solutions can be identified before they become problems. The results of conducting PIAs are directed to executive level management and boards of directors, or other decision-makers within organizations.

A PIA 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.

5. Privacy Audit (See item 5 in toolkit)

The Privacy Audit tool assesses the effectiveness of controls that a custodian has identified as being necessary to safeguard the personal health information in its custody or control in the context of its particular operation. Audits are important to risk management as an audit assesses the implementation of recommended privacy safeguards and their effectiveness in addressing identified risks. The scope of an audit may be limited to one system or project or may include all personal health information in an organization. Audits can be done internally or be conducted by external agents, and are directed to executive level management and boards of directors, or other decision-makers within organizations.

It should be noted that a Privacy Audit is a companion piece to both the PPIA and the PIA. The PPIA and the PIA are self-assessments intended to identify possible issues in operations' approaches to privacy controls and to suggest solutions and mitigation strategies; the Privacy Audit tool enables a custodian to conduct a self-assessment to determine the progress of the adoption of recommended controls and to measure the efficacy of those controls. The results of a Privacy Audit should be incorporated into the PPIA or PIA process, whenever those assessments are updated.

6. Privacy Breach Guidelines (See item 6 in toolkit)

Under certain circumstances, in the event of a breach of PHIA, the Act requires that custodians notify either or both the individual affected and the Office of the information and Privacy Commissioner. The Privacy Breach Guidelines are intended to assist custodians in determining when notification of a breach is necessary, and who must be notified.

7. Privacy Breach Reporting Form (See item 7 in toolkit)

Where, in the event that a breach of PHIA has occurred, a custodian determines that notifying the Office of the information and Privacy Commissioner is required, it should use this form to do so.