



**Health and Community Services**

**The *Personal Health Information Act*  
Facilitated Education Program**

**Participant Resource Materials  
(Half-Day Session)**

Version:  
Date:

1.0  
September, 2010



## WARNING AND DISCLAIMER

These resource materials have been prepared by the Department of Health and Community Services as a general guide to assist custodians of personal health information and others to meet their obligations under Newfoundland and Labrador's *Personal Health Information Act*.

- These resource materials are for general information purposes only.
- These resource materials reflect interpretations and practices regarded as valid when it was published based on information available at that time.
- These resource materials are not intended, and should not be construed, as legal or professional advice or opinion.
- Custodians and others that are 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 these resource materials; a second edition may be published in due course.

## **ACKNOWLEDGEMENT**

These resource materials were 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 Policy and Standards 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*: Resources for Implementation**

### **Resources for implementation**

In partnership with several provincial stakeholders, the Department of Health and Community Services has created several resources to assist custodians of personal health information to meet their obligations under the Act. Custodians are not obligated to use these resources. Custodians should review the materials carefully and make appropriate use them to facilitate their compliance with the *Personal Health Information Act*.

1. PHIA Risk Management Toolkit
2. PHIA Policy Development Manual
3. PHIA Online Education Program

**Please note: these resources may be accessed or downloaded from the Department of Health and Community Services' website at <http://www.health.gov.nl.ca/health>.**

These resource materials are for general information purposes only, and should be adapted to the circumstances of each custodian using them. The materials reflect interpretations and practices regarded as valid at the time of publication based on information available at that time. The materials are not intended, and should not be construed, as legal or professional advice or opinion. Custodians that are concerned about the applicability of privacy legislation to their activities are advised to seek legal or professional advice based on their particular circumstances.

This section of the website is currently under development and will be updated. Please visit this site regularly to obtain more resources on the *Personal Health Information Act*.

### **The PHIA Risk Management Toolkit**

The *Personal Health Information Act* requires that custodians protect the personal health information in their custody or control. The Act requires that custodians take steps that are reasonable in the circumstances to ensure that personal health information in their custody or control is:

1. protected against theft, loss and unauthorized access, use or disclosure;
2. protected against unauthorized copying or modification; and,
3. retained, transferred and disposed of in a secure manner.

To meet these obligations custodians should incorporate risk management processes into their projects, activities and systems as early as possible; ideally, during the design or planning phases. 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 PHIA Risk Management Toolkit is intended to:

- 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;
- Assist custodians in assessing their current state of compliance with PHIA;
- Assist custodians in assessing the effectiveness of the physical, administrative and technological controls that they have established to protect the personal health information in their custody or control; and,
- Assist custodians in identifying any gaps or areas for improvement that there might be in their physical, administrative and technological controls.

The PHIA Risk Management Toolkit contains the following items:

1. Information Security Management Overview
2. Privacy Checklist
3. Preliminary Privacy Impact Assessment
4. Privacy Impact Assessment
5. Privacy Audit
6. Privacy Breach Guidelines
7. Privacy Breach Reporting Form

### **PHIA Policy Development Manual**

The *Personal Health Information Act* requires that custodians have policies and procedures in place that describe the ways that they collect, use and disclose personal health information. The PHIA Policy Development manual is intended to provide custodians with a framework for developing their own policies and procedures to meet this obligation.

The PHIA Policy Development Manual sets out the legal requirements of the *Personal Health Information Act* and arranges those requirements into a policy framework. The manual provides custodians with sample policy and procedure language: the sample policy language reflects custodians' obligations under the *Personal Health Information Act* while the sample procedure language contains suggestions as to how the policies could be implemented.

Custodians should not simply adopt the sample policies and procedures in this policy development manual as their own; rather, custodians should review the samples provided and customize them in order to make them applicable to their particular activities and line of business. It should always be kept in mind that, while

custodians may customize the sample language provided in the PHIA Policy Development Manual, custodians should be careful to ensure that whatever policies or procedures they develop are legally compliant with the requirements of the Act. Custodians should consult the Act, their regulatory authority and/or solicitor for interpretation of or for guidance on the provisions of the *Personal Health Information Act*, where necessary and as applicable.

### **PHIA Online Education Program**

PHIA requires that custodians of personal health information ensure that their employees, agents, contractors and volunteers, and those health professionals who have a right to treat persons at a health care facility operated by the custodian are aware of the duties imposed by the Act and regulations and by the custodian's information policies and procedures. The PHIA Online Education Program is intended to help custodians to understand their obligations under the Act, as well as to assist them in providing education and training to those for whom they have a responsibility under the Act.

## FURTHER READING

### Appendix “A”:

- Information Security Management Overview

### Appendix “B”:

- Privacy Breach Guidelines

### Appendix “C”:

- The Circle of Care: Sharing Personal Health Information for Health Care Purposes

### Appendix “D”:

- Limited Consent under PHIA



## The *Personal Health Information Act*

### Appendix “A”

## Information Security Management Overview

---

### Introduction

The Newfoundland and Labrador *Personal Health Information Act* (PHIA) requires that custodians take steps that are reasonable in the circumstances to ensure that:

4. Personal health information in their custody or control is protected against theft, loss and unauthorized access, use or disclosure;
5. Records containing personal health information in their custody or control are protected against unauthorized copying or modification; and
6. 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 custodians must implement information security 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 manage the information with due diligence and take appropriate measures to safeguard it from injury.

The contents of this document are intended to serve as a very brief introduction to information security and to some of the aspects of information security that custodians of personal health information may need to consider in order to fulfill their responsibilities and obligations under PHIA.

### Information Security is a Process

Information security is simply the process by which information confidentiality, integrity, and availability are safeguarded and ensured. No one product, process or technology alone can provide for every information security issue faced by a custodian; rather, effective information security requires the successful integration of:

- **Physical** security controls, such as door locks, alarm systems and segregated working areas;

- **Administrative** security controls, such as policies, procedures and guidelines documents; and,
- **Technological** security controls, such as firewalls, intrusion detection systems and encryption applications.

Controls of all three types must be developed to work in concert with one another in order to create an effective information security framework.

Personal health information must be safeguarded according to baseline security requirements and continuous security risk management. Continued delivery of services must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

### **Information Security Management – Key Practices**

The following is a list of key information security practices that custodians of personal health information should consider when implementing their information security program. These practices have been derived from the internationally-recognized ISO 27002 information security standard published by the International Organization for Standardization (ISO), and represent the different aspects that comprise a comprehensive information security management program.

It should be noted that while addressing each of the following practices will result in a comprehensive security framework, custodians may not need to address certain of the following, depending on the nature and scope of their operations. These practices should be read as being guidelines to inform the development and implementation of an information security management framework: rather than being a comprehensive list of things that custodians *must* do, these practices should be viewed as being a list of things that custodians should consider the necessity of, in the context of their particular work, line of business and / or operations.

### **Common Information Security Practices**

- 1. Security Policy Management**
  - 1.1. Establish a comprehensive information security policy
- 2. Corporate Security Management**
  - 2.1. Establish an internal security organization
  - 2.2. Control external party use of your information
- 3. Organizational Asset Management**
  - 3.1. Establish responsibility for your organization's assets
  - 3.2. Use an information classification system
- 4. Human Resource Security Management**
  - 4.1. Emphasize security prior to employment
  - 4.2. Emphasize security during employment

4.3. Emphasize security at termination of employment

**5. Physical and Environmental Security Management**

5.1. Use secure areas to protect facilities

5.2. Protect your organization's equipment

**6. Communications and Operations Management**

6.1. Establish procedures and responsibilities

6.2. Control third party service delivery

6.3. Carry out future system planning activities

6.4. Protect against malicious and mobile code

6.5. Establish backup procedures

6.6. Protect computer networks

6.7. Control how media are handled

6.8. Protect exchange of information

6.9. Protect electronic commerce services

6.10. Monitor information processing facilities

**7. Information Access Control Management**

7.1. Control access to information

7.2. Manage user access rights

7.3. Encourage good access practices

7.4. Control access to network services

7.5. Control access to operating systems

7.6. Control access to applications and systems

7.7. Protect mobile and tele-working facilities

**8. Systems Development and Maintenance**

8.1. Identify information system security requirements

8.2. Make sure applications process information correctly

8.3. Use cryptographic controls to protect your information

8.4. Protect and control your organization's system files

8.5. Control development and support processes

**9. Information Security Incident Management**

9.1. Report information security events and weaknesses

9.2. Manage information security incidents and improvements

**10. Business Continuity Management**

10.1. Use continuity management to protect your information

**11. Compliance Management**

11.1. Comply with legal requirements

11.2. Perform security compliance reviews

11.3. Carry out controlled information system audits

## **12. Risk Assessment**

- 12.1. Threat and risk assessment and identification
- 12.2. Risk mitigation

### **Implementation of Information Security Program**

Information security management is generally considered to be a specialized field for subject-matter experts in Information Management and Information Technology. Custodians of personal health information should consult with internal or external subject-matter experts when developing and implementing their information security management strategies.

## The *Personal Health Information Act*

### Appendix “B”

#### Privacy Breach Guidelines

---

##### Introduction

The Newfoundland and Labrador *Personal Health Information Act* (PHIA) sets out the rules that persons or organizations defined as custodians of personal health information must follow when collecting, using, disclosing, retaining and disposing of personal health information.

PHIA recognizes the unique character of personal health information as being extremely sensitive and also recognizes that it is frequently collected, used and disclosed for a variety of authorized purposes. These purposes include care and treatment, health research, quality control and risk management.

PHIA balances individuals’ right to privacy with respect to their own personal health information with the legitimate needs of health information custodians to collect, use and disclose this information. With certain limited exceptions, PHIA requires custodians of personal health information to obtain consent before they collect, use or disclose the information in their custody or control. PHIA also makes custodians responsible for the secure storage and destruction of personal health information. Additionally, individuals have the right to access and request correction of their own personal health information.

The purpose of this document is to provide guidance to custodians when they are faced with a privacy breach.

##### What is a privacy breach?

A privacy breach is any collection, use or disclosure of personal health information that is not authorized under PHIA. In essence, a privacy breach occurs whenever a person has contravened or is about to contravene a provision of PHIA, or of the regulations passed under PHIA.

As an example, section 15 of PHIA requires that custodians take steps that are reasonable in the circumstances to ensure personal health information in their custody or control is:

- (1) Protected against theft, loss and unauthorized use or disclosure,

- (2) Retained, transferred and disposed of in a secure manner; and,
- (3) Protected against unauthorized copying, modification or disposal.

A failure to meet these requirements represents some of the more common circumstances under which a privacy breach could arise. Again, however, it is important to bear in mind that any collection, use or disclosure of personal health information which is not in accordance with the PHIA could also be considered a breach.

A custodian of personal health information may become aware of a privacy breach in a number of ways. It is frequently the case that a custodian may itself identify a breach during the normal course of its business or operations. A custodian may also be contacted by the Newfoundland and Labrador Office of the Information and Privacy Commissioner (NL OIPC) if a concern about its operations has been raised by a member of the public. Finally, the NL OIPC could initiate its own investigation if it determined that such was in the public interest.

This appendix will focus primarily on situations where a custodian has itself identified a privacy breach or where the custodian has been contacted by the NL OIPC regarding a potential breach. Such situations often arise where personal health information has been stolen, lost or accessed by unauthorized persons. Many of these situations will involve unintentional breaches of PHIA. For example, personal health information may be lost (a patient's file is misplaced), stolen (laptop computers are a prime example) or inadvertently disclosed to an unauthorized person as a result of an honest mistake (a letter addressed to patient A is actually mailed to patient B). However, a custodian may also become aware of breaches that are intentional; for example, an instance where intentional, unauthorized access of patient files by staff has occurred.

Where a privacy breach has occurred, custodians are encouraged to contact the NL OIPC so that assistance can be provided to the custodian in fulfilling its obligations under PHIA (e.g. notification of persons involved) and in taking whatever steps might be necessary to prevent similar occurrences in the future.

### **The Benefits of Having a Privacy Breach Protocol**

It is recommended that a custodian of personal health information develop a privacy breach "protocol", or a process for systematically responding to privacy breaches. A privacy breach protocol should include provisions for addressing all of the actions outlined in this document. Having a privacy breach protocol in place *before* an adverse privacy event occurs is strongly advised; this will yield several benefits:

- Custodians can respond quickly and in a coordinated manner;
- Roles and responsibilities of staff will be understood beforehand;
- A process for effective investigations will be documented and can be set into motion;
- Effective containment of the breach will be aided;

- Remediation efforts will be easier; and
- Custodians will be properly prepared for the potential involvement of the NL OIPC.

## **Health Information Privacy Breach Guidelines**

Upon learning of a privacy breach, a custodian must take immediate action. Many of the following guidelines need to be carried out simultaneously or in rapid succession.

### **Step 1: Containment – Identify the scope of the potential breach and take steps to contain it**

- Retrieve the hard copies of any personal health information that has been disclosed;
- Ensure that no copies of the personal health information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required; and,
- Determine whether the privacy breach involved unauthorized access to any other records of personal health information (e.g., an electronic information system) and take whatever steps are necessary and appropriate (e.g., change passwords, identification numbers and / or temporarily shut down a system) to prevent further breaches from occurring.

### **Step 2: Evaluate – Respond immediately by implementing the privacy breach protocol**

- Ensure appropriate staff within your organization are immediately notified of the breach, including the Chief Privacy Officer or the designated contact person for the purposes of the Act;
- Depending on the nature or seriousness of the privacy breach, there may be a need to contact senior management, patient relations or the information and technology and/or communications department within your organization;
- Depending on the nature or seriousness of the privacy breach, there may be a need to inform the NL OIPC of the privacy breach and work together constructively with its staff (see section 15(4) of PHIA); and
- Address the priorities of containment and notification as set out in the following steps.

### **Step 3: Notification – Identify those individuals whose privacy was breached and notify them of the breach**

Any individuals whose information was the subject of a privacy breach **must be notified, unless certain criteria are met.** Specifically, there is **no**

requirement under PHIA to notify those individuals where the theft, loss, unauthorized disposition, or improper disclosure or access of their personal health information will not have an adverse impact on either:

1. the provision of health care or other benefits to the individual who is the subject of the information; or,
2. the mental, physical, economic or social well-being of the individual who is the subject of the information

**Otherwise**, PHIA requires health information custodians to notify individuals of the breach at the first reasonable opportunity.

Regarding notification:

- PHIA does not specify the manner in which notification must be carried out. However, for example, notification can be by telephone or in writing, or depending on the circumstances, a notation made in the individual's file to be discussed at their next appointment;
- There are many factors that may need to be taken into consideration when deciding on the best form of notification (e.g., the sensitivity of the personal health information). As a result, the health information custodian may want to contact the NL OIPC to discuss the most appropriate form of notification;
- There may also be exceptional circumstances when a custodian may want to discuss notification with the NL OIPC before proceeding; for example, when notification is not reasonably possible or may be detrimental to the individual. In cases such as these, the health information custodian is encouraged to contact the NL OIPC to discuss the circumstances and potential approaches to notification;
- When notifying individuals affected by the breach, custodians should provide details of the extent of the breach and the specifics of the personal health information involved in the breach;
- Custodians should advise affected individuals of the steps that have been or will be taken to address the breach, both immediate and long-term;
- Custodians should advise affected individuals that the NL OIPC has been contacted to ensure that all obligations under the Act are fulfilled, where applicable (certain circumstances actually require custodians to notify the NL OIPC about a breach – see section 15(4) of PHIA); and,
- Custodians should advise affected individuals that those individuals may contact the NL OIPC directly if they are not satisfied with the measures taken by the custodian to respond to the breach.



#### **Step 4: Investigation and Prevention**

- Conduct an internal investigation into the matter. The objectives of an internal investigation are to:
  - (1) ensure the immediate requirements of containment and notification have been addressed;
  - (2) review the circumstances surrounding the breach; and
  - (3) review the adequacy of existing policies and procedures in protecting personal health information.
- Address the situation at a systemic level. In some cases, program-wide procedures may warrant review (e.g., responding to telephone inquiries from family members regarding patients or clients);
- Advise the NL OIPC of your findings and work together with that Office to make any necessary changes;
- Ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of PHIA; and,
- Cooperate in any further investigation into the incident undertaken by the NL OIPC.

#### **What happens when the Commissioner investigates a privacy breach?**

When investigating a privacy breach, depending on the circumstances, the NL OIPC may:

- Ensure any issues surrounding containment and notification have been addressed;
- Interview individuals involved with the privacy breach or individuals who can provide information about a process;
- Obtain and review the health information custodian's position on the privacy breach;
- Ask for a status report of any actions taken by the health information custodian;
- Review and provide input and advice on current policies and procedures and any other relevant documents and recommend changes; and,
- Where appropriate or necessary, issue a Report containing recommendations at the conclusion of the review.

## Steps custodians can take to avoid a privacy breach

Custodians governed by PHIA are strongly urged to proactively adopt measures to prevent privacy breaches from occurring. These measures would normally include:

- Ensuring that policies and procedures are in place that comply with the privacy protection provisions of PHIA and that staff are properly trained in this respect;
- Safeguarding personal health information when it is physically removed from the office or institution; for example, by ensuring that all laptops and PDA's are password protected and data is encrypted;
- Ensuring that a baseline of logging and auditing is in place on all systems, particularly those containing electronic health records and that staff are aware that regular audits will occur;
- Conducting a privacy impact assessment (PIA) where appropriate. The PIA is a process that helps determine whether new technologies, information systems and proposed programs or policies meet basic privacy requirements (For further assistance with PIAs, see the "privacy impact assessment Guidelines for the Newfoundland and Labrador *Personal Health Information Act*", available on the Department of Health and Community Service's website);
- When in doubt, obtaining advice from your organization's legal department and/or Chief Privacy Officer; and,
- Encouraging a culture of privacy within your organization.

## The Personal Health Information Act

### Appendix “C”

#### The Circle of Care:

#### Sharing Personal Health Information for Health Care Purposes

---

##### Introduction

The purpose of this informational piece is to clarify the circumstances in which a custodian of personal health information may rely on implied consent for the collection, use and disclosure of personal health information within the “circle of care”, and the options available to a custodian where consent cannot be assumed to be implied.

The term “circle of care” is a defined term in the Newfoundland and Labrador *Personal Health Information* (PHIA). PHIA defines the circle of care as follows:

*...[T]he expression "circle of care" means the persons participating in and activities related to the provision of health care to the individual who is the subject of the personal health information and includes necessarily incidental activities such as laboratory work and professional consultation.*

Thus, the circle of care is a term commonly used to describe the ability of certain health information custodians to *assume* an individual’s *implied consent* to collect, use or disclose personal health information for the purpose of providing health care to that individual.

##### Circumstances under which a custodian may assume implied consent

A custodian may only deal with an individual’s personal health information within the circle of care (*i.e.*, may only assume to an individual’s implied consent to collect, use or disclose personal health information) where all of the following six conditions are satisfied:

1. *The custodian must fall within one of the categories of custodians that is authorized to rely upon implied consent (i.e., that can be considered to be within the circle of care).*

2. *The personal health information to be collected, used or disclosed by the custodian must have been received from the individual, his or her substitute decision-maker or another health information custodian.*
3. *The health information custodian must have received the personal health information that is being collected, used or disclosed for the purpose of providing or assisting in the provision of health care to the individual.*
4. *The purpose of the collection, use or disclosure of personal health information by the health information custodian must be for the provision of health care or assisting in the provision of health care to the individual.*
5. *Regarding disclosure of personal health information within the circle of care, the disclosure by a custodian must be made for the sole purpose of providing health care to the individual.*
6. *The implied consent of the individual must be valid and the individual must not have expressly withheld or withdrawn their consent to the collection, use or disclosure.*

### Further analysis

Taking each of the above six conditions in turn:

1. ***The custodian intending to act within the circle of care must fall within one of the categories of custodians that is authorized to rely upon implied consent (i.e., that can be considered to be within the circle of care).***

PHIA identifies only three categories of custodians that may rely on implied consent (i.e., that can be considered to be within the circle of care):

- (1) a regulated health care professional, such as a physician or a nurse, where that professional is in the course of providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;
- (2) a health care provider (i.e., a person, other than a health care professional, who is paid by MCP, or another person or entity to provide health care services to an individual); or,
- (3) a person who operates one of the following:
  - (a) a health care facility (as defined under PHIA),
  - (b) a licensed pharmacy as defined in the *Pharmacy Act*,
  - (c) an ambulance service, or;

- (d) 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.

**2. *The personal health information to be collected, used or disclosed by the custodian within the circle of care must have been received from the individual, his or her substitute decision-maker or another health information custodian.***

Personal health information is defined in PHIA as being identifying information relating to the physical or mental health of an individual, the provision of health care to an individual, the identification of the substitute decision-maker for the individual and the payments or eligibility of an individual for health care or coverage for health care, including the individual's health number.

A substitute decision-maker is a person authorized under PHIA to consent on behalf of an individual to the collection, use or disclosure of personal health information.

If the personal health information to be collected, used or disclosed was received from a third party – other than the substitute decision-maker for the individual or another authorized health information custodian (refer to #1, above) – the necessary consent cannot be assumed to be implied.

**3. *The custodian must have received the personal health information that is being collected, used or disclosed within the circle of care for the original purpose of providing or assisting in the provision of health care to the individual.***

The personal health information to be collected, used or disclosed within the circle of care must have been received for the purpose of providing health care or assisting in the provision of health care to the individual to whom it relates.

A health information custodian may not rely on implied consent if the personal health information was received for other purposes, such as research, fundraising, marketing or providing health care or assisting in providing health care to another individual or group of individuals.

- 4. *The purpose of the collection, use or disclosure of personal health information by the custodian acting within the circle of care must be for the provision of health care or assisting in the provision of health care to the individual.***

The collection, use or disclosure must be for the purposes of providing health care or assisting in the provision of health care to the individual to whom the personal health information relates.

A health information custodian may not rely on assumed implied consent if the collection, use or disclosure is for other purposes, such as for research, fundraising, marketing or providing health care or assisting in the provision of health care to another individual or group of individuals.

- 5. *Regarding the disclosure of personal health information within the circle of care, the disclosure by a custodian must be for the sole purpose of providing health care to the individual.***

Where, for the purpose of providing health care or assisting in the provision of health care to the individual as part of a circle of care, a custodian referred to in condition #1, above, either:

1. collects personal health information from and with the consent of the individual who is the subject of the information; or
2. receives personal health information about an individual from another custodian,

the custodian is entitled to assume that it has the individual's continuing implied consent to use or disclose the information to another custodian or person, but only for the purpose of providing health care to that individual. This will be so unless the custodian collecting or receiving the information becomes aware that the individual has withdrawn their consent (see condition #6, within, for further information).

- 6. *The implied consent of the individual must be valid and the individual must not have expressly withheld or withdrawn their consent to the collection, use or disclosure.***

The concept of the circle of care operates on the basis of a type of consent: *implied* consent.

Implied consent can only be presumed to exist where an individual can be said to have *implicitly* provided knowledgeable consent. In order for implied consent to arise and to be considered valid, it must be reasonable to believe that the individual is aware of the purpose of the collection, use or disclosure and knows that they can either give or withhold consent. It is, in turn, reasonable to believe that an individual knows the purpose of the collection, use or disclosure if the health information custodian posts or makes readily available an adequate notice generally describing these purposes in a location where it is likely to come to the individual's attention or provides the individual with such a notice.

PHIA permits an individual to expressly withhold or withdraw consent to the collection, use or disclosure of his or her personal health information, unless the collection, use or disclosure is permitted or required by PHIA to be made without their consent. An individual may withdraw their consent for collections, uses or disclosures that occur within the circle of care; however, custodians may continue to act on the basis of implied consent until and unless an individual expressly withdraws their consent.

In most circumstances, if an individual decides to withhold or withdraw consent, PHIA requires the receiving custodian to be notified if the disclosing health information custodian is prevented from disclosing all of the information that is considered to be reasonably necessary for the provision of health care.

For further information about the ability of an individual to expressly withhold or withdraw consent to the collection, use or disclosure of personal health information for health-care purposes, and the obligations on health information custodians in this context, please refer to G", "*Limited Consent under PHIA*".

### **Other factors to be considered when relying on implied consent**

In addition to the above six conditions, PHIA requires that a custodian not collect, use or disclose personal health information if other information will serve the purpose. Custodians are also required to not collect, use or disclose more personal health information than is reasonably necessary for the intended, authorized purpose. These general limiting principles apply even where a health information custodian is entitled to rely on an individual's assumed implied consent.

### **Options available when custodians cannot rely on implied consent within the "circle of care"**

When consent cannot be assumed to be implied (*i.e.*, where any of the above six requirements have not been met), custodians should consider other options. Depending on the circumstances, a health information custodian may be permitted

to collect, use or disclose personal health information (a) without an individual's consent or (b), with the express consent of that individual.

*(a) Without Consent*

Health information custodians may collect, use or disclose personal health information without consent if the collection, use or disclosure is either permitted or required by PHIA to be made without consent.

For example, under section 39 of PHIA, all custodians of personal health information are permitted to disclose personal health information without consent for (among other purposes) review and planning activities that relate to the provision of health care by the custodian.

In addition, in certain circumstances set out in section 37 of PHIA, custodians may use or disclose personal health information without consent where it is reasonably necessary for the provision of health care and the individual has not expressly instructed otherwise. This provision would apply, for example, in emergency situations where the individual to whom the information relates cannot provide consent of any type, or be presumed to have done so.

Sections 31 and 34 of PHIA, respectively, set out the circumstances in which personal health information may be collected and used without consent and sections 39 - 46 set out the circumstances in which personal health information is permitted or required to be disclosed without consent.

*(b) With Express Consent*

In all other circumstances, health information custodians may only collect, use or disclose personal health information with the express consent, (*i.e.*, either verbal or written consent) of the individual to whom the personal health information relates, or their substitute decision-maker. In order to rely on express consent, health information custodians must be satisfied that all of the required elements of consent are fulfilled.

**A note on consent for treatment or care**

PHIA governs circumstances involving the collection, use and disclosure of personal health information. As such, wherever PHIA addresses issues involving consent, it is dealing with consent for the collection use and disclosure of information – it is important to note that PHIA does not govern matters of consent as they relate to the provision of treatment or care. Consent for the provision of treatment or care must be obtained separately and as per applicable legislative requirements, standards of practice and / or professional guidelines.

**Required elements of consent**



Regardless of whether the consent being obtained is express or implied (*i.e.*, implied, as in the case of the circle of care), the consent of an individual for the collection, use or disclosure of personal health information by a custodian:

- Must be the consent of the individual or their substitute decision-maker;
- Must be knowledgeable;
- Must relate to the information that will be collected, used or disclosed; and,
- Must not be obtained through deception or coercion.

In order for consent to be considered knowledgeable, it must be reasonable under the circumstances to believe that the individual is aware of the purpose of the collection, use or disclosure and knows that they can either give or withhold consent.

## The *Personal Health Information Act*

### Appendix “D”

#### Limited Consent under PHIA

---

##### Introduction

The Newfoundland and Labrador *Personal Health Information Act* (PHIA) gives residents of the province control over the collection, use and disclosure of their personal health information by requiring that custodians can only collect, use and disclose an individual’s personal health information with the express or (under certain circumstances) implied consent of that individual, or as otherwise specifically authorized under the Act.

Integral to the concept of consent is the idea that individuals have the ability to withhold or withdraw their consent for the collection, use or disclosure of their personal health information for a particular purpose, including for the provision of health care.

Section 23(2) of PHIA makes it clear that individuals may withhold or withdraw their consent to the collection, use or disclosure of their personal health information by custodians where their consent is required. Further, under certain circumstances, individuals may provide express instructions to custodians to not use or disclose their personal health information without their consent. These provisions are sometimes referred to as the “limited consent” provisions under PHIA, though “limited consent” is not a defined term in the Act.

##### **To what information does “limited consent” apply, and to whom can individuals limit disclosure?**

The withholding or withdrawal of consent or the express instructions may take various forms, including communications from individuals to health information custodians:

- to not collect, use or disclose a particular **item** of information contained in their record of personal health information (for example, a particular diagnosis);
- to not collect, use or disclose the contents of their **entire** record of personal health information;

- to not **disclose** their personal health information to a particular health information custodian, a particular agent of a health information custodian or a class of health information custodians or agents (e.g. physicians, nurses or social workers); or
- not to permit a particular health information custodian, a particular agent of a health information custodian or a class of health information custodians or agents (physicians or nurses, for example) to **use** their personal health information.

Although it is up to an individual to decide what limitations (if any) they wish to impose in respect of the collection, use or disclosure of their personal health information, and to whom the limitation should apply, a custodian should discuss with the individual how limiting their consent might affect the provision of their health care, and why a custodian might require access to more personal health information than the individual has allowed in to provide the best possible care.

### **What are the exceptions to “limited consent” requirements?**

Section 23(2) of PHIA makes it clear that an individual may withhold or withdraw their consent to the collection, use or disclosure of their personal health information where their consent is required.

However, where PHIA specifically authorizes a particular collection, use or disclosure of personal health information without the consent of an individual (refer to sections 37 and 39 of PHIA for examples), the individual cannot withdraw their consent for that particular collection, use or disclosure – *i.e.*, the individual cannot restrict the custodian from engaging in a collection, use or disclosure that PHIA specifically authorizes them to engage in without obtaining the individual’s consent.

Additionally, section 27(2) of PHIA makes it clear that an individual cannot prohibit or restrict a recording of personal health information by the custodian where the recording is required by law or by established standards of professional or institutional practice. As an example, such circumstances would include the recording of demographic and care-encounter information at hospitals and clinics during the admission and provision of care to an individual.

Finally, the limited consent provisions of PHIA do not have retroactive effect. This means that, where an individual validly withholds or withdraws their consent for the collection, use or disclosure of their personal health information, a custodian will only have to ensure that they comply with that instruction on an ongoing basis; custodians will not be required to revisit or remedy collections, uses or disclosures that were made under previous valid authority.

## What “limited consent” obligations are there for custodians?

Custodians of personal health information are required to respect the decisions of individuals to withhold or withdraw their consent to the collection, use or disclosure of their personal health information for purposes of providing or assisting in providing health care, and to respect express instructions not to use or disclose their personal health information for health care purposes requiring consent.

To ensure that no unauthorized collection, use or disclosure occurs, it is important for health information custodians to record any express “limited consent” instructions or directives upon obtaining consent to the collection, use or disclosure of personal health information for health care purposes. Individuals may also provide, withdraw or modify “limited consent” directives at any point after they provide consent initially.

Compliance with the “limited consent” provisions of PHIA may be achieved by health information custodians through:

- policies, procedures or manual processes;
- electronic or technological means;
- a combination of policies, procedures; or,
- manual processes and technological means,

depending on the avenue chosen by the custodian. Frequently, the proper implementation of “limited consent” directives will involve a combination of the above measures.

Once an individual limits the collection, use or disclosure of their personal health information by withholding, withdrawing or limiting their consent, a custodian who is subject to the express instruction cannot collect, use or disclose (as the case may be) that personal health information for health care purposes unless:

- the individual changes their mind and informs the health information custodian accordingly; or

the collection, use or disclosure can be made without the individual’s consent. (Examples of such circumstances can be found under sections 37 and 39 of PHIA.)

## GLOSSARY

**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 that 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**, in the context of this policy framework, 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 a 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 policy framework, is an instruction given by an individual or by their representative to a custodian or their representative as to how their personal health information may be collected, used or disclosed.

**Contact person(s)** are individuals appointed by a 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 individuals (e.g., individuals are assigned a code name and the custodian retains a list that links the code name with the particular individual's actual name so data can be re-linked if necessary.) Custodians who have access to the code and the data will be considered to have identifiable information.

**Designate** is an individual that a 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 a 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 an intent to defraud.

**Identifying information** is information that identifies a specific individual 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 an individual 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 person or organization other than an employee of a custodian that processes, retrieves, stores or disposes of personal health information for a custodian, or provides information management or information technology services to a 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 a 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 information about themselves.

**Registry**, in the context of this policy framework, 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.

**Risk management**, in the context of PHIA policy framework, is the identification, assessment, and prioritization of risks followed by a coordinated application of resources to minimize, monitor and control the probability and / or severity of the impact of adverse privacy events. Risks can come from legal liabilities, accidents, natural causes and disasters as well as deliberate attacks from an adversary.

**Successor**, in the context of the PHIA policy framework, is defined as the entity that will assume the responsibilities of the custodian upon the incumbent custodians resignation of responsibilities under the *Personal Health Information Act*.

**Use**, in relation to personal health information in the custody or control of a 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.

**Willful** means deliberate.