The *Personal Health Information Act* Policy Development Manual

Version	1.2
Date:	February, 2011

WARNING AND DISCLAIMER

The PHIA Policy Development Manual 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*.

- The PHIA Policy Development Manual 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 Manual are for general information purposes only. They should be adapted to the circumstances of each custodian using the manual.

- This manual reflects interpretations and practices regarded as valid when it was published based on information available at that time.

- This manual 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 second edition of the PHIA Policy Development Manual; subsequent editions may be published in due course.

ACKNOWLEDGEMENT

The PHIA Policy Development Manual 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 Policy and Standards Working Group and the Newfoundland and Labrador Office of the Information and Privacy Commissioner for their assistance in preparing these materials.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

Introduction

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

The Act is available on the Government of Newfoundland and Labrador's website at:

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

(Please note that the copy of the Act and regulations made available in this policy development manual were prepared by the Office of the Legislative Counsel. As they are not published by the Queen's Printer they are not an official version of the laws of the Province. You should contact the Queen's Printer to obtain the official statement of the law.)

Purposes of the Act

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

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

Who is a Custodian?

The information in this policy development manual has been developed for use by all custodians of personal health information in the province of Newfoundland and Labrador. Entities that are and are not a "custodian" of personal health information are defined in section 4 of the *Personal Health Information Act*.

Entities that have been designated as custodians under the Act include (but are not limited to):

- Health care professionals and health care providers (Physicians, nurses, chiropractors, optometrists, etc.),
- Regional Integrated Health Authorities,
- Departments of the provincial government when engaged in health care activities,
- The Public Health Laboratory,
- The Centre for Health Information,
- The Workplace Health and Safety Compensation Commission,
- Etc.

What is Personal Health Information?

The policies in this manual apply to "personal health information" held by custodians. Personal health information is defined in section 5 of the Act. The section states as follows:

Personal health information means identifying information in oral or recorded form about an individual that relates to:

> (a) the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family;
>
> (b) the provision of health care to the individual, including information respecting the person providing the health care; the name, business title, address and telephone number; licence number; and profession, job classification and employment status.
>
> (c) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;
>
> (d) registration information;
>
> (e) payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;

(f) an individual's entitlement to benefits under or participation in a health care program or service;

(g) information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;

(h) a drug as defined in the *Pharmacy Act*, a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or

(i) the identity of a person referred to in section 7 of the *Personal Health Information Act*.

Please see Part I of the *Personal Health Information Act* for exceptions to the general rules regarding what constitutes personal health information.

Purpose of this Manual

This manual was designed to help custodians of personal health information meet their obligations under the *Personal Health Information Act*. Under the Act, all custodians of personal health information are required to have policies and procedures in place that facilitate the implementation of, and ensure compliance with the *Personal Health Information Act*. This manual is intended to provide custodians with a framework for developing their own policies and procedures.

Who should use this Manual

The *Personal Health Information Act* requires that all custodians of personal health information have policies and procedures to ensure that they comply with the requirements of the Act. Any custodian who is developing new policies or updating existing policies may use this manual to assist them as they do so.

In addition, the information in this policy development manual may be useful for decision makers, information managers, direct care providers, employees, volunteers, vendors and those with practicing privileges within an organization operated by a custodian.

How to use this Manual

This policy development manual is a starting point. It is intended to assist custodians as they create or update their own policies and procedures. The manual sets out the legal requirements of the *Personal Health Information Act* and arranges them into a policy development framework.

The manual provides custodians with sample language for policies and for procedures: the sample policy language provided reflects custodians' obligations under the *Personal Health Information Act*; the sample procedure language contains suggestions as to how the sample 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 adapt them to make them applicable to their particular activities and lines of business.

The *Personal Health Information Act* does not require health information custodians to completely set aside their existing information practices. Where a custodian already has a set of policies and procedures, the Act may simply necessitate a change to existing information-handling practices to make existing policies and procedures compliant with the new requirements of the *Personal Health Information Act*. Regardless of whether a custodian is creating a full set of policies and procedures or simply updating an existing set it is important that a custodian's policies and procedures accurately describe the ways that they collect, use and disclose personal information in their custody. Custodians should *say what they do*

and *do what they say*: policies are official statements, and custodians will be held to what they say in them.

It should always be kept in mind that while custodians may customize the sample language provided in this manual, custodians should always be careful to ensure that whatever policies or procedures they develop are legally compliant with the requirements of the *Personal Health Information Act*. This manual should not be construed as legal advice; it is only a policy and procedure development aid. 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.

The manual contains a glossary of commonly-used terms as well as brief discussion papers expanding on some of the more common questions that arise under the Act. The discussion materials can be found in the appendices at the end of the manual.

Evaluation of the Policy Development Manual

Using evaluation criteria designed for the purpose and in conjunction with key stakeholders, the Department of Health and Community Services will evaluate the effectiveness of this manual in fostering compliance with the *Personal Health Information Act*.

Responsibility for Manual Review, Revisions and Additions

The Department of Health and Community Services will review this manual for sufficiency a minimum of every five years. Any revised or additional policies will be made available through the Department's website.

Custodians will be responsible for updating their own policies and for informing persons using or adhering to their policies of any changes made.

Glossary of Terms

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

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

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

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

  (1) 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;
  (2) a health care provider;
  (3) a person who operates:
    (a) a health care facility,
    (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

- **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 development manual 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 development manual 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 development manual 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 this policy development manual, 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 this policy development manual, is defined as the entity that will assume the responsibilities of the custodian upon the incumbent custodian's resignation of responsibilities under the *Personal Health Information Act*.

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

CHAPTER 2: SAMPLE POLICIES AND PROCEDURES

1.10 Security of Personal Health Information

PURPOSE:

To provide custodians with a basis for a common and consistent approach regarding the steps that a custodian is required to take to protect the personal health information in its custody or control.

SAMPLE POLICY:

A custodian must take steps that are reasonable in the circumstances to ensure that:

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

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

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

The phrase "disposed of in a secure manner" in relation to the disposing of a record of personal health information does not include the *destruction* of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances.

SAMPLE PROCEDURE:

Custodians of personal health information must implement information security controls to protect the personal health information in their custody or control.

Appendix "C" (*Information Security Management Overview*), which is attached to this policy development manual, contains a 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 the *Personal Health Information Act*.

THINGS TO REMEMBER:

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.

Custodians should be aware of health sector and industry "best practices" when determining what steps are "reasonable' in the circumstances of their particular line of business or operations.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

Appendix "C" – Information Security Management Overview

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 15.

1.20 Oath or affirmation of confidentiality

PURPOSE:

To provide custodians with a basis for a common and consistent approach regarding the Oath or Affirmation of Confidentiality that is required to taken by its employees, agents, contractors and volunteers, as well as health professionals with the right to treat persons at a health care facility operated by the custodian .

DEFINITIONS:

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.

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.

SAMPLE POLICY:

A custodian must ensure that all its employees, agents, contractors and volunteers, as well as health professionals with the right to treat persons at a health care facility operated by the custodian take an Oath or Affirmation of Confidentiality.

The Oath or Affirmation of Confidentiality must include a statement that the custodian has informed the individual about their duties and obligations under the *Personal Health Information Act*, the regulations and the custodian's information policies and procedures.

The Oath or Affirmation of Confidentiality must include a statement that the personal health information to which the individual has had access during the course of their employment, contract or service, must remain confidential both during and after employment/engagement, in perpetuity.

The Oath or Affirmation of Confidentiality must include a statement that individual signing the agreement understands the terms and provisions of the agreement, and agrees to abide by them.

The Oath or Affirmation of Confidentiality must become part of an individual's Human Resources record and will be retained for as long as their Human Resources record exists.

SAMPLE PROCEDURE:

An Oath or Affirmation of Confidentiality should be taken:

- Preferably at the commencement of employment, contract or term of service;
- In the course of employment, contract or term of service, when new or revised policy and procedures come into effect; or
- A minimum of every five years or according to the employer's policy.

The custodian should maintain the original signed oath / affirmation document and will provide a copy to the individual who has signed it.

THINGS TO REMEMBER:

An Oath or Affirmation of Confidentiality is a written document provided by the custodian and signed by those who take the oath or affirmation.

Custodians must ensure that those individuals have read the oath or affirmation prior to signing.

Custodians should develop standard form documents to be signed by all employees, agents, contractors and volunteers, as well as health professionals with the right to treat persons at a health care facility operated by the custodian.

Standard forms should be updated as necessary to reflect any changes in the Act or policies.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

Appendix "B" – Sample Oath / Affirmation of Confidentiality

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 13 and 14.

Province of Newfoundland and Labrador: *Oaths Act*, RSNL 1990, c. O-1

1.30 Awareness of obligations

PURPOSE:

To provide custodians with a consistent approach to providing education relating to the regulations, policies and procedures and duties imposed by the *Personal Health Information Act*.

SAMPLE POLICY:

A custodian's employees, agents, contractors and volunteers, as well as health professionals with the right to treat persons at a health care facility operated by the custodian must be made aware of the duties imposed by *Personal Health Information Act* and the regulations, as well as of the information policies and procedures of the custodian relating to same.

SAMPLE PROCEDURE:

Employee awareness: A custodian's employees will be required to receive a programme of education / training administered or organized by the custodian to inform them of the duties imposed by *Personal Health Information Act*. The specific depth and level of detail required in a given programme of education must be determined by the individual's role within the organization. Upon completion, it is considered "best practice" to have the individual and a representative of the custodian co-sign a document indicating that a specific programme of education has been completed.

An educational programme may include, but is not limited to:

- Small group education sessions; and,
- Web-based learning modules

The custodian is responsible for ongoing education related to changes in policy, regulations or future legislative amendments.

Contractor / volunteer awareness: A custodian's agents, contractors, vendors, information managers and volunteers must be informed of the duties imposed by *Personal Health Information Act* in a manner appropriate to the nature of the

relationship between the custodian and the entity. This might include the inclusion of a statement of the duties in a contract, or may consist of a programme of education / training administered or organized by the custodian.

THINGS TO REMEMBER:

- The requirement articulated in the within sample policy applies only to those employees, agents, contractors and volunteers, as well as health professionals with the right to treat persons at a health care facility operated by the custodian that have access to personal health information in the course of their duties or provision of services to the custodian.
- Continuing education credits may be available for the programme of education through a specific health care professional's / health care provider's regulatory authority.
- Custodians may choose to provide an oath of confidentiality as a component of the education sessions.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.20 Oath or Affirmation of Confidentiality
1.80 information manager Agreements

Appendix "A" – Information Management Agreement Principles
Appendix "B" – Sample Oath / Affirmation of Confidentiality

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 13 and 14.

1.40 Accuracy of personal health information

PURPOSE:

To provide custodians with a consistent approach to ensuring accuracy when collecting, using or disclosing personal health information.

SAMPLE POLICY:

Upon collection, a custodian should include the date the information was collected and the name of the individual providing the information.

Before either using or disclosing personal health information that is in its custody or under its control, a custodian must:

(a) take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purpose for which the information is used or disclosed;

(b) clearly set out for the recipient of the information the limitations, if any, on the accuracy, completeness or up-to-date character of the information; and

(c) take reasonable steps to ensure that the recipient is the person intended and authorized to receive the information.

SAMPLE PROCEDURE:

Prior to using personal health information, the custodian must:

- Confirm the correctness of the referenced personal health information by confirming data elements such as an individual's:
    - Name;
    - Date of birth;
    - MCP number, or other unique identifier, (where available); and / or
    - Address.

- Make appropriate changes, if possible when the individual using the information has any concerns related to the accuracy, completeness or up-to-date status of the personal health information.

- Contact the appropriate individuals to have the deficiencies addressed and documenting the inaccuracies if it is not possible for the individual using the information to make the required changes.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

4.20 Indirect Collection of Personal Health Information
6.30 Accuracy of Disclosed Information

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 16 and 64.

1.50 Designation of decision maker

PURPOSE:

To provide custodians with a consistent approach to designating an individual to make decisions on behalf of the custodian.

DEFINITIONS:

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*.

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

SAMPLE POLICY:

A custodian must make any and all decisions required of a custodian that may be required from time to time under the *Personal Health Information Act*.

In the alternative, a custodian must designate a person that is a part of their organization to make decisions on their behalf.

THINGS TO REMEMBER:

Examples of custodians include Regional Health Authorities, a Government Department when it is engaged in a function related to the delivery of or administration of health care and/or a health care professional such as a doctor, nurse or pharmacist, when they are not in the employ of another identified custodian.

Examples of designates are Office Managers, Privacy Officers and/or Chief Information Officers.

The decision to appoint an individual other than the custodian as the designate and decision-maker must be documented in a custodian's policies.

In the case where a custodian is a public body, the person designated by the custodian to make decisions under the *Personal Health Information Act* may be the same individual designated under the *Access to Information and Protection of Privacy Act* to discharge its statutory obligations under that Act.

The custodian must document in its policies who the designated decision-maker is and who the contact person is. The designate and the contact person may be one and the same.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 17 and 18.

1.60 Designation of contact person

PURPOSE:

To provide custodians an understanding of the requirement for the appointment of and designation of responsibilities for a contact person.

DEFINITIONS:

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

SAMPLE POLICY:

A custodian that is not an individual must appoint one or more contact persons to perform the following functions:

(a) facilitate the custodian's compliance with the *Personal Health Information Act*;

(b) ensure that employees, contractors, agents and volunteers of the custodian and those health care professionals who have the right to treat persons at a health care facility operated by a custodian are informed of their duties under the *Personal Health Information Act*;

(c) respond to inquires from the public in respect of the custodian's information policies and procedures; and

(d) respond to requests by an individual for access to or correction of personal health information about the individual that is in the custody or under the control of the custodian.

A custodian that is an individual may also designate a contact person to perform the functions set out above. Where no contact person is designated by such a custodian, a custodian themselves will considered to be the contact person for the above-noted purposes.

A custodian is required to prepare a written statement that sets out the name and contact information for the designated contact person and to make that statement available to those who are or who are likely to be affected by the custodian's activities. This may be done in several ways, examples of which include:

- Publication of the information on a website;
- Posting a notice at the custodian's facilities, in a highly-visible area; and / or
- Making the information available in a pamphlet or other hand-out, available at the custodian's facilities.

Where a custodian is an individual and no contact person has been designated, the custodian must make their own contact information available to those who are or who are likely to be affected by the custodian's activities.

THINGS TO REMEMBER:

The custodian must make it easy for individuals to determine who the custodian's contact person is and how to contact them.

Custodians are expected to know and understand the needs of their particular clientele and be able to provide information in public statements in other forms / formats for individuals who for whatever reason might not be able to read or understand the written public statements. Examples of alternate forms of presentation might include video, Braille and / or translations into other languages.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 17 and 18.

1.70 Notification of uses and public statements

PURPOSE:

To inform custodians of the required components of the public statement required under the *Personal Health Information Act*.

SAMPLE POLICY:

Where a custodian collects personal health information directly from the individual who is the subject of the information or from their representative, the custodian must take reasonable steps to inform the individual or their representative:

(a) of the purpose for the collection, use and disclosure of the information;

(b) of the identity of and other relevant information relating to the designated contact person; and,

(c) of other information prescribed in the regulations.

Custodians may inform individuals or their representatives by way of a written statement.

Custodians are required to provide a written statement that includes the following information:

- A general description of the custodian's information policies and procedures related to collection, use and disclosure of personal health information;
- Identification of the custodian or the designated contact person and their associated contact information;
- Direction on how an individual may obtain access to or request correction of personal health information; and,

- The process an individual would use to make a complaint to the Privacy Commissioner.

Custodians may make their written statements available to their clientele by posting them in high traffic areas (e.g., waiting rooms) where they are likely to come to individuals' attention and/or provide individuals with a brochure that contains the information contained in the public statement.

Where a custodian uses or discloses personal health information about an individual without the individual's consent, in a manner that is inconsistent with their policies and procedures, the custodian must:

> (a) inform the individual who is the subject of the information of the use or disclosure at the first reasonable opportunity except where, under section 58 of the Act, the custodian would be required or permitted to refuse access to the record of personal health information;
>
> (b) make a note of the use or disclosure; and
>
> (c) retain the note as part of the record of personal health information about the individual that it has in its custody or under its control

unless a custodian reasonably believes that the use or disclosure of 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.

THINGS TO REMEMBER:

Custodians are expected to know and understand the needs of their particular clientele and be able to provide information in public statements in other forms/formats for individuals who for whatever reason might not be able to read or understand the written public statements. Examples of alternate forms of presentation might include video, Braille and/or translations into other languages.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 15, 19, 20, 53 and 58.

1.80 Agreements between custodians and information managers

PURPOSE:

To define the requirements of agreements between custodians and information managers.

DEFINITIONS:

An **information manager** is a person or body 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.

SAMPLE POLICY:

Where a custodian engages the services of an information manager, the custodian must enter into a formal agreement with the information manager regarding the provision of those services.

SAMPLE PROCEDURE:

Agreements between custodians and information managers must have the following characteristics:

- The agreement must be in writing;
- The agreement must provide for the protection of personal health information against unauthorized access, use, disclosure, disposition, loss or modification in compliance with the Act;
- The agreement must specify the purposes for which the information manager may use and disclose personal health information, and must set out all applicable restrictions to such use(s) and / or disclosure(s);

- The agreement must contain a meaningful description of all of the personal health information maintained by the information manager;

- The agreement must document the security measures used by the information manager to protect the personal health information in its custody or control;

- The information manager must agree to comply with the *Personal Health Information Act* and with the provisions of the agreement, and must acknowledge both obligations in the agreement;

- The information manager must agree to adhere to the polices and procedures of the custodian;

- The agreement must identify the situations under which the information manager may disclose personal health information to another person or entity;

- The agreement must identify all stakeholders involved in the management of the personal health information including contractors or subcontractors and define the relationships with the identified individuals or groups;

- The agreement must reference any other related Service Level Agreements pertaining to the custodian / information manager relationship;

- The agreement must permit the custodian to review the policies and procedures of the information manager related to the protection and management of personal health information to verify they are consistent with those of the custodian; and

- The agreement must define notification and other change management processes as they relate to the provision of services by the information manager.

<u>THINGS TO REMEMBER:</u>

information managers are third-party service providers. The definition of Information Manger can be found in the *Personal Health Information Act*.

Requirements as expressed in the *Personal Health Information Act* may be integrated into contracts with information managers and other service providers.

This sample policy applies to information managers within the province of Newfoundland and Labrador, outside the province and/or outside the country.

An agreement with an information manager does not relieve the custodian of any of their obligations under the *Personal Health Information Act.*

Custodians must take additional care when engaging the services of information managers where the personal health information under the custody or control of the custodian is to be stored outside of the province of Newfoundland and Labrador. There may be significant legal issues to consider regarding the laws of the receiving jurisdiction, as they could impact the collection, use and disclosure of information in that jurisdiction. Custodians should engage persons with sufficient subject-matter expertise to conduct an assessment of the receiving jurisdiction's laws as they relate to the collection, use and disclosure of information prior to any such engagement.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

Appendix "A" – Information Management Agreement Principles

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 22.

1.90 Individual's representative

PURPOSE:

To inform custodians of who may act as a representative of an individual in relation to the collection, use and disclosure of the individual's personal health information.

SAMPLE POLICY:

In certain circumstances, custodians are authorized to take instructions regarding the management of an individual's personal health information from persons other than the individual to whom the personal health information pertains. Custodians are authorized to take such instructions from:

(a) a person with written authorization from the individual who is the subject of the information to act on the individual's behalf;

(b) a substitute decision maker appointed by the individual in accordance with the *Advance Health Care Directives Act*, where the individual lacks the competency to exercise the right or power or is unable to communicate, and where the collection, use or disclosure of his or her personal health information is necessary for or ancillary to a "health care decision", as defined in the *Advance Health Care Directives Act*, or, where a substitute decision maker has not been appointed, a substitute decision maker determined in accordance with section 10 of the *Advance Health Care Directives Act*;

(c) a court appointed guardian of a mentally disabled person, where the exercise of the right or power relates to the powers and duties of the guardian;

(d) the parent or guardian of a minor where, in the opinion of the custodian, the minor does not understand the nature of the right or power and the consequences of exercising the right or power;

(e) by the individual's personal representative, where the individual is deceased, or, where there is no personal representative, by the deceased's

nearest relative, and for this purpose, the identity of the nearest relative may be determined by reference to section 10 of the *Advance Health Care Directives Act*;

(f) where the individual is a neglected adult within the meaning of the *Neglected Adults Welfare Act*, by the Director of Neglected Adults appointed under that Act; or

(g) where an individual has been certified as an involuntary patient under the *Mental Health Care and Treatment Act*, by a representative as defined in that Act, except as otherwise provided in this Act.

THINGS TO REMEMBER:

This sample policy is intended to inform custodians of who may act as a representative of an individual in relation to the collection, use and disclosure of the individual's personal health information, and does not address or deal with who may or may not act as a substitute decision-maker in relation to care.

An individual's personal representative is authorized to exercise any right or power of the individual they represent that the individual himself/herself would be entitled to exercise under the *Personal Health Information Act*.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 7.

Province of Newfoundland and Labrador: *Advance Health Care Directives Act*, SNL 1995, c. A-4.1

Province of Newfoundland and Labrador: *Neglected Adults Welfare Act*, SNL 1990, c. N-3

Province of Newfoundland and Labrador: *Mental Health Care and Treatment Act*, SNL 2006, c. M-9.1.

Newfoundland Labrador Health and Community Services	*PERSONAL HEALTH INFORMATION ACT* **Policy Development Manual** **Section: 2.0 - Consent** Sample Policy: 2.10 CONSENT REQUIREMENTS

2.10 Consent requirements

PURPOSE:

To provide custodians with a consistent approach for obtaining knowledgeable consent for the collection, use and disclosure of personal health information where such consent is required.

DEFINITIONS:

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:

(1) 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;

(2) a health care provider;

(3) a person who operates:

(i) a health care facility,
(ii) a licensed pharmacy as defined in the *Pharmacy Act*,
(iii) an ambulance service, or
(iv) a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider;

Persons within an individual's circle of care will include health care professionals such as doctors and nurses, but will also include necessarily incidental functions such as laboratory and diagnostic services as well as a range of professional consultation services.

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.

Unless the individual takes action to "opt in" to the purpose — in other words, says "yes" to it in some way — the organization cannot assume consent, as is the case with implied consent.

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

SAMPLE POLICY:

Where consent is required for the collection, use or disclosure of personal health information by a custodian, whether express or implied, the consent must be knowledgeable.

Consent is considered knowledgeable if it is reasonable in the circumstances to believe that when the individual gave consent they were informed:

1. of the purpose of the collection, use and disclosure of the information;
2. that they may withdraw their consent (where consent is required for the collection, use or disclosure); and
3. that the information may only be collected, used or disclosed without their consent in accordance with the provisions of the *Personal Health Information Act*.

Implied consent is appropriate where:

- Personal health information is collected from an individual within the circle of care, for the purpose of providing health care or assisting in the provision of health care.

- "Circle of care" is a term that 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:

  (1) 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;

  (2) a health care provider;

  (3) a person who operates:

  (i) a health care facility,
  (ii) a licensed pharmacy as defined in the *Pharmacy Act*,
  (iii) an ambulance service, or

(iv) a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider.

- Persons within an individual's circle of care will include health care professionals such as doctors and nurses, but will also include necessarily incidental functions such as laboratory and diagnostic services as well as a range of professional consultation services.

- Persons authorized to receive information within the circle of care will also include any person or entity that is providing care to the individual who is the subject of the information. This could include a family member or a home care worker. Again, it is important to note that the receiving entity *must* be providing health care to the individual that is the subject of the information in order to be a part of the circle of care.

- Implied consent ends when the custodian becomes aware that the individual has withdrawn consent.

Express consent will be required where:

- The custodian discloses personal health information to another custodian for a purpose other then providing or assisting in providing health care; or,

- The custodian discloses personal health information to a person that is not a custodian.

The requirement to obtain express consent does not apply to the disclosure of personal health information by the following custodians to a third party who provides (or who is requested to provide) payment for the medication or goods and services provided by that custodian to the individual:

(a) an authority;
(b) a board, council, committee, commission, corporation or agency established by an authority;
(c) 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;

Consent for the collection, use or disclosure of personal health information may be obtained by a custodian or a duly appointed representative of the custodian.

SAMPLE PROCEDURE:

Knowledgeable consent

In order for consent to be considered knowledgeable it must be:

1. Obtained directly from the individual or someone authorized as a representative under Section 7 of the *Personal Health Information Act*; and,

2. Given freely and voluntarily by the individual or the authorized representative, as the case may be.

In order to obtain knowledgeable consent custodians must:

- Determine whether or not there are any potential barriers to effective communication, such as illiteracy;
- Inform the individual of how their personal health information will be used, in a manner which they understand. This may be accomplished through posters, brochures, video presentations or other methods as appropriate;
- Advise the individual that they may give or withhold consent (where consent is required for the collection, use or disclosure); and,
- Advise the individual that their information may only be collected, used or disclosed without their consent in accordance with the provisions of the *Personal Health Information Act*.

THINGS TO REMEMBER:

Consent is required for the collection, use and disclosure of personal health information within the circle of care. However, custodians do not have to obtain **express** consent for the collection, use and disclosure of personal health information within the circle of care; custodians may rely on **implied** consent within the circle of care where individuals do not expressly indicate otherwise.

Consent for the collection, use and/or disclosure of personal health information is separate and different from consent requirements related to the provision of health care treatment.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.70 Notification of Uses and Public Statements
2.20 Circle of Care
2.30 Limited Consent
2.40 Withdrawal of Consent
2.50 Disclosure without Consent

Appendix "F" – The Circle of Care: Sharing Personal Health Information for Health Care Purposes
Appendix "G" – Limited Consent under PHIA

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s 23, 24 and 25.

Province of Newfoundland and Labrador: *Pharmacy Act*, SNL 1994, c. P-12.1

2.20 Circle of care

PURPOSE:

To provide custodians with a common and consistent definition of the "circle of care".

DEFINITIONS:

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:

(1) 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;

(2) a health care provider;

(3) a person who operates:

(i) a health care facility,
(ii) a licensed pharmacy as defined in the *Pharmacy Act*,
(iii) an ambulance service, or
(iv) a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider;

Persons within an individual's circle of care will include health care professionals such as doctors and nurses, but will also include necessarily incidental functions such as laboratory and diagnostic services as well as a range of professional consultation services.

Persons authorized to receive information within the circle of care will also include any person or entity that is providing health care to the individual who is the subject of the information. This could include a family member or a home care worker.

Again, it is important to note that the receiving entity *must* be providing health care to the individual that is the subject 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.

Unless the individual takes action to "opt in" to the purpose — in other words, says "yes" to it in some way — the organization does not assume consent, as is the case with implied consent.

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

This applies to situations where the intended use or disclosure is obvious from the context and the organization can assume with little or no risk that the individual, in providing the personal health information in the first place, is aware of and consents to the intended use or disclosure.

SAMPLE POLICY:

"Circle of care" is a term that describes the health care professionals, providers and persons providing necessary services that form an individual's health care team.

Implied consent is permitted when a custodian or representative of the custodian is sharing an individual's personal health information for the purpose of providing health care or assisting in the provision of health care as part of the circle of care unless the individual has expressly withdrawn their consent.

Persons within an individual's circle of care will include health care professionals such as doctors and nurses, but will also include necessarily incidental functions such as laboratory and diagnostic services as well as a range of professional consultation services.

Persons authorized to receive information within the circle of care will also include any person or entity that is providing care to the individual who is the subject of the information. This could include a family member or a home care worker. Again, it is important to note that the receiving entity *must* be providing health care to the individual that is the subject of the information.

Implied consent can no longer be relied upon if and when the custodian becomes aware that the individual has withdrawn their consent.

THINGS TO REMEMBER:

Consent is required for the collection, use and disclosure of personal health information within the circle of care. However, custodians do not have to obtain **express** consent for the collection, use and disclosure of personal health information

within the circle of care; custodians may rely on **implied** consent within the circle of care where individuals do not expressly indicate otherwise.

A previous care provider or other person who is not currently providing health care to the individual is not part of the current circle of care. As such they cannot obtain an individual's personal health information without the individual providing their express consent.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.70 Notification of Uses and Public Statements
2.10 Consent Requirements
2.30 Limited Consent
2.40 Withdrawal of Consent
2.50 Disclosure without Consent

Appendix "F" – The Circle of Care: Sharing Personal Health Information for Health Care Purposes
Appendix "G" – Limited Consent under PHIA

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 24.

2.30 Consent directives and limited consent

PURPOSE:

To provide custodians information with a common and consistent understanding regarding the requirements of limited consent.

DEFINITIONS:

Consent directive for the purpose of this policy development manual 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.

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:

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

Institutional Standards are clearly articulated statements that guide institutional behaviour and identify expected levels of performance.

Professional Standards are authoritative statements that set out the legal and professional basis for practice. The primary purpose of professional standards is to identify for the profession, the public, government, and other stakeholders the desired and achievable level of performance expected of the professional in their practice, against which actual performance can be measured.

SAMPLE POLICY:

A custodian must protect the personal health information of individuals as required by an individual's consent directives.

Consent directives limiting consent must be obtained by a custodian, or where applicable, their designate.

Consent directives limiting consent are valid for as long as the subject information exists, unless the limitation is revoked by the individual. Consent directives limiting consent survive disclosure to another custodian.

Consent directives limiting consent do not prohibit or restrict a recording of personal health information by the custodian where the recording is required by law or by standards of professional or institutional practice.

Where a custodian discloses information to another custodian for the purpose of providing health care and the disclosing custodian does not have the consent of the individual to disclose all personal health information about the individual that they feel is reasonably necessary for the receiving custodian's purpose, the disclosing custodian must inform the receiving custodian that restrictions have been placed on the disclosure by the individual.

SAMPLE PROCEDURE:

When an individual provides a consent directive that limits the way in which a custodian may collect, use or disclose their information, the custodian will:

- Require the individual to complete, date and sign a form that identifies to the custodian the specific conditions placed on the collection, use or disclosure of their personal health information.
- Ensure that the individual is informed of how the specific consent directive limiting collection, use or disclosure may impact the individual's health care, including risks to the provision of the best possible care.
- Ensure that the documentation related to the individual's consent directive is featured prominently in the individual's health record.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.50 Designate
1.60 Contact Person

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s 17, 18 and 27.

2.40 Withdrawal of consent

PURPOSE:

To provide custodians with a common and consistent approach for administering an individual's directive for the withdrawal of consent for the collection, use and disclosure of their personal health information.

SAMPLE POLICY:

Where an individual consents to the collection, use or disclosure of their personal health information, the individual may withdraw their consent, whether it is express or implied, by providing notice to the custodian.

The withdrawal of the consent will not have retroactive effect.

Withdrawal of consent can only be obtained by a custodian, or, where applicable, the appointed contact person or designate, as defined in policies 2.50 ("Designate") and 2.60 ("Contact Person").

Consent directives limiting or withdrawing consent do not have the effect of restricting collection, use or disclosure required or permitted by law.

Consent directives limiting or withdrawing consent do not have the effect restrict the recording of personal health information required by standards of professional or institutional practice.

Custodians are responsible for informing individuals that:

- Whether express or implied, where consent is required for a collection, use or disclosure it may be withdrawn by the individual at any time;
- Withdrawal of consent is effective as of the date of its withdrawal but will not have a retroactive effect;
- Withdrawal of consent may have an adverse impact on the provision of care to the individual, including risks arising from delay; and

- Withdrawal of consent is valid until a different consent directive is provided by the individual or by a person with legal authority to consent for the individual.

SAMPLE PROCEDURE:

When an individual withdraws consent for the collection, use or disclosure of their personal health information, the custodian will require:

- The individual to complete a form advising the custodian that consent has been withdrawn;
- The custodian, designate or contact person record that the individual was provided information and education on the risks and potential risks of withdrawing the use of personal health information;
- That the withdrawal of consent document is dated and witnessed; and
- Documentation of the individual's withdrawal of consent be recorded in their health record.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

2.10 Consent Requirements
2.30 Limited Consent
2.50 Disclosure without Consent

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, Parts III and IV.

2.50 Disclosure without consent

PURPOSE:

To provide custodians with common and consistent direction regarding when personal health information can be disclosed without an individual's consent.

DEFINITIONS:

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.

SAMPLE POLICY:

Disclosure of personal health information can, under certain limited circumstances, be disclosed without an individual's consent.

The circumstances under which information can be disclosed without an individual's consent are those that are permitted or required by the *Personal Health Information Act*.

There are two categories of situation in which disclosure without consent may occur; discretionary disclosure and mandatory disclosure. Sections A and B, below, deal with discretionary disclosures that may be made without consent, while section C deals with mandatory disclosures that must be made without consent.

A. Discretionary disclosure without consent for the provision of health care

Consent is not required for the following discretionary disclosures of personal health information:

Providing Health Care

- Unless the disclosure is contrary to an express directive of the individual, without the express consent of the individual and where the disclosure is

necessary for the purpose of providing health care or health care services, a custodian may disclose personal health information to:

- A health authority,
- A health professional,
- A health provider; or,
- a person who operates:
  (i) a health care facility,
  (ii) a licensed pharmacy as defined in the *Pharmacy Act* ,
  (iii) an ambulance service, or
  (iv) a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider;

but only where either:

- Consent cannot be obtained from the individual in a timely manner; or
- When the individual is certified as an involuntary patient or is the subject of a community treatment order under the *Mental Health Care and Treatment Act.*

Disclosure to Relatives

- Unless the disclosure is contrary to an express consent directive of the individual, a person who operates a health care facility may disclose personal health information about an individual who is a patient or resident in a health care facility operated by the custodian, without the express consent of the individual, to a person that the custodian reasonably believes is a member of the individual's immediate family, a relative or a person with whom the individual has a close personal relationship where:

  (a) the custodian offers the individual the option, at the first reasonable opportunity after admission to the facility, to object to that disclosure and the individual does not do so; and

  (b) the disclosure is made in accordance with accepted professional practice.

B. Discretionary disclosure without consent for health-related purposes

Consent is not required for the following discretionary disclosures of personal health information:

Eligibility and Payment

- For the purpose of determining or verifying the eligibility of the individual to receive health care or related goods, services or benefits funded by the provincial or federal governments;

- For the purpose of determining or providing payment to the custodian for the provision of care or the processing, monitoring, verifying or reimbursing claims for payment for the provision of health care;

- To obtain payment for health care provided to the individual from a department, the government of another jurisdiction or to an agency of that government; and / or,

- For disclosure outside the province in accordance with sample policy 5.100

Individual or Public Health and Safety

- For disclosure that is necessary to prevent or reduce harm to the mental or physical health or safety of the individual the information is about or another individual;

- For disclosure that is necessary for public health or public safety;

Posthumous Requirements

- For the purpose of identifying a deceased individual; and,

- To the personal representative of the deceased for a purpose related to administration of the estate of the deceased individual.

- To allow the spouse, partner, siblings or descendants of a deceased individual to make decisions about his or her own health care or the health care of his or her child or where the disclosure is necessary to provide health care to the recipient as per sample policy 5.40.

Research

- For research purposes approved by a research ethics board or research ethics body under the *Health Research Ethics Authority Act*.

Health Care Planning

- For the purpose of delivering, evaluating or monitoring a program of the custodian that relates to the provision of heath care or payment for health care;

- To an information manager retained by the custodian to provide services;

- To provide review and planning related to the provision of health care such as audits for or to provide legal services, error management services or risk management services;

- To report to the Canadian Institute of Health Information or other entities as set out in the regulations to this Act for management, evaluation and monitoring of resources, health care planning and delivery; and

- To allow for the superintendent of a correctional facility in which the individual is lawfully detained or the administrator of a psychiatric unit in which the individual is detained to make arrangements for the provision of health care to the individual or the appropriate placement of the individual as per sample policy 5.60.

Succession Planning

- To provide information to a successor or a potential successor who has signed a confidentiality agreement when the custodian intends to transfer records as a result of retirement or relocation. (*Note that a custodian who transfers a record of personal health information to its successor must make reasonable efforts to give notice to the individual who is the subject of the information prior to the transfer or, where this is not possible, as soon as possible after the transfer that it has ceased to be a custodian of the information and identifying its successor.*)

Legal Proceedings

- A proceeding or contemplated proceeding in which the custodian is or is expected to be a party or a witness;

- A peer review or quality assurance committee as referred to in subsection 8.1(2) of the *Evidence Act*;

- To a proposed guardian or legal representative for the purpose of the appointment of a person as a guardian or representative for an individual;

- To a guardian appointed under an Act of the province or the *Rules of the Supreme Court, 1986*, to commence, defend or continue a proceeding on behalf of the individual or to represent the individual in a proceeding;

- For the purpose of laying an information, order or making an application for an order where the personal health information relates to or is a matter in issue in the information or application;

- To another custodian where the custodian where the custodian disclosing the information has a reasonable expectation that disclosure will detect or prevent fraud, limit abuse in the use of health care or prevent the commission of an offence under an Act of the province or of Canada.

C. Mandatory disclosure without consent for health-related purposes

Consent is not required for the following mandatory disclosures. Regardless of an individual's consent directive, a custodian must disclose personal health information without the consent of the individual who is the subject of the information:

Health Care Delivery

- Where the custodian is a minister, to a department of government or to a regional health authority to obtain health care cost recovery;

- To a person conducting an audit or reviewing application for or reviewing accreditation, where the audit or review relates to the services provided by the custodian;

- To or via an information network designated in the regulations in which personal health information is recorded for the purpose of facilitating
    - the delivery, evaluation or monitoring of a program that relates to the provision of health care or payment for health care,
    - review and planning that relates to the provision of health care or payment for health care, or
    - the construction or creation of an integrated electronic record of personal health information in accordance with the regulations;

- To a Custodian designated in the regulations who compiles or maintains a registry for facilitating or improving the provision of health care or relating to the storage or donation of body parts or bodily functions;

- To the chief medical officer and other medical officers where the disclosure is required by another Act or an Act of Canada;

- To a public health authority that is similar to a chief medical officer and other medical officers established under a law of Canada, another province or other jurisdiction; and,

- To permit a minister to monitor or verify claims for payment for health care funded in part or wholly by the government of the province.

Legal Proceedings

- For disclosure that is necessary for various proceedings as identified in sample policy 5.70;

- For disclosure that is necessary as a requirement of law as identified in sample policy 5.80;

- The disclosure is required to carry out or facilitate an inspection, investigation or similar procedure for the purpose that is authorized by or under;
    - The *Personal Health Information Act*;
    - The *Child, Youth and Family Services Act*;
    - Another provincial Act; or
    - An Act of Canada.

THINGS TO REMEMBER:

Disclosure of personal health information without consent must be limited to the minimum amount of information required.

A custodian must not disclosure personal health information if other information will serve the purpose.

A recipient does not necessarily become a custodian by virtue of receiving personal health information.

CROSS REFERENCES TO OTHER SAMPLE POLICIES:

1.80 information manager Agreements
2.30 Limited Consent
5.10 Requirements for Disclosure
5.30 Preventing Unauthorized Disclosure of Personal Health Information
5.30 Accuracy of Disclosed Information
5.40 Disclosure of Personal Health Information to Relatives
5.50 Disclosure of Personal Health Information to a Successor
5.60 Disclosure of Personal Health Information for Health and Safety Purposes
5.70 Disclosure of Personal Health Information for Proceedings
5.80 Disclosure of Personal Health Information for Enforcement Purposes
5.90 Disclosure of Personal Health Information for Research Purposes
5.100 Disclosure of Personal Health Information outside the Province
5.110 Disclosure to a Registry

Appendix "A" – Information Management Agreement Principles

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Health Research Ethics Authority Act,* SNL 2006, c. H-1.2.

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 36 – 46 and 49 and 50.

Province of Newfoundland and Labrador: *Workplace Health, Safety and Compensation Act,* RSNL 1990, c. W-11.

3.10 Collection of personal health information - Generally

PURPOSE:

To provide custodians with an understanding of the general requirements relating to the collection of personal health information.

DEFINITIONS:

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

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.

SAMPLE POLICY:

Prior to collecting personal health information from an individual, custodians are required to notify individuals of the purpose for which their information is being collected, and of all reasonably foreseeable uses and disclosures. (See sample policy 1.70, "Notification of Uses and Public Statements").

A custodian must not collect personal health information about an individual unless:

- The individual who is the subject of the information has consented to its collection and the collection is necessary for a lawful purpose; or

- The collection is permitted or required by the *Personal Health Information Act*.

As is permitted under the *Personal Health Information Act*, a custodian may collect personal health information about an individual without that individual's consent

where the individual is incapable of providing consent and the collection is necessary for the provision of health care to the individual when:

- There is no authorized representative who can provide consent on behalf of the individual or, consent cannot be obtained in a timely manner; or

- The individual has been certified as an involuntary patient or is the subject of a community treatment order under the *Mental Health Care and Treatment Act*.

A custodian must not collect personal health information if other information will serve the purpose of the collection, unless the custodian is required by law to collect the information.

Except as provided for in PHIA, as described in sample policy 3.20 ("Indirect Collection of Personal Health Information"), a custodian must collect personal health information directly from the individual who is the subject of the information.

A custodian must not collect more personal health information than is reasonably necessary to meet the purpose of the collection unless there is a legal requirement to collect that information.

Consent directives limiting or withdrawing consent do not have the effect of restricting the recording of personal health information required by standards of professional or institutional practice.

THINGS TO REMEMBER:

There may be situations where direct collection of personal health information is not possible and indirect collection is required or authorized as per sample policy 3.20.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.40 Accuracy of Information
1.70 Notification of Uses and Public Statements
3.20 Indirect Collection of Personal Health Information
4.30 Transforming Personal Health Information

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s.20, 29 and 32.

Newfoundland Labrador Health and Community Services	*PERSONAL HEALTH INFORMATION ACT* **Policy Development Manual** Section: 3.0 COLLECTION Sample Policy: 3.20 COLLECTION OF PERSONAL HEALTH INFORMATION - GENERALLY

3.20 Indirect collection of personal health information

PURPOSE:

To inform custodians of the exceptions to the general requirement to collect personal health information directly from an individual who is the subject of the information.

DEFINITIONS:

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

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.

SAMPLE POLICY:

Indirect collection of personal health information is permitted in the following situations:

Where Consent is Provided

- Where the individual authorizes collection from another source.

Health Care Delivery

- Where the individual is not able to provide information in an accurate or timely manner;

- Where the individual is unable to provide information and the custodian collects the information from:
    - A person with written authorization from the individual to act on their behalf;

- A substitute decision maker in accordance with the *Advance Health Care Directives Act;*
- A court appointed guardian of a mentally disabled person;
- The parent or guardian of a minor;
- The personal representative or next of kin when an individual is deceased
- By the Director of Neglected Adults where the individual is a neglected adult under the *Neglected Adults Welfare Act*; or
- A representative for an involuntary patient as defined under the *Mental Health Care and Treatment Act.*

- For the purpose of assembling a family or genetic history where the information collected will be used in the context of providing a health service to the individual;

- For determining or verifying the individual's eligibility to participate in a health care program or to receive a benefit, product or health care service;

Authorized Research

- To carry out a research project that has been approved by the research ethics board or a research ethics body in accordance with the *Health Research Ethics Authority Act*.

Legal Proceedings

- When an Act, an Act of Canada, a treaty, agreement or arrangement made under an Act or an Act of Canada permits or requires the collection or disclosure;

- Custodians including the Regional Health Authorities, boards, councils, committees, commissions, corporations or agencies established by the board, departments created under the Executive Council Act and/or the minister, is collecting information related to

  - the investigation of a breach of an agreement or a contravention or an alleged contravention of the laws of the province or of Canada,
  - the conduct of a proceeding or a possible proceeding, or
  - a statutory function of the custodian

  and the method of collection is authorized by law; or

Health Care Planning

- Where the custodian collects information for the purpose of analysis or compiling statistical information respecting the management, evaluation or monitoring of the allocation of resources to, or planning for the health care system.

THINGS TO REMEMBER:

A custodian must not collect more personal health information than is reasonably necessary to meet the purpose of the collection unless there is a legal requirement to collect that information.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.40 Accuracy of Personal Health Information
1.70 Notification of Uses and Public Statements
1.90 Individual's Representative
3.10 Requirements for Collection

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Advance Health Care Directives Act*, SNL 1995, c. A-4.1.

Province of Newfoundland and Labrador: *Executive Council Act*, SNL 1995, c. E-16.1

Province of Newfoundland and Labrador: *Mental Health Care and Treatment Act*, SNL 2006, c. M-9.1.

Province of Newfoundland and Labrador: *Neglected Adults Welfare Act*, SNL 1990, c. N-3.

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 30 and 31.

Newfoundland Labrador Health and Community Services	*PERSONAL HEALTH INFORMATION ACT* **Policy Development Manual** **Section: 4.0 - Use** Sample Policy: 4.10 USE OF PERSONAL HEALTH INFORMATION

4.10 Use of personal health information

PURPOSE:

To provide custodians with an understanding of the requirements relating to the use of personal health information.

DEFINITIONS:

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.

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.

SAMPLE POLICY:

A custodian cannot use personal health information about an individual except in the following situations:

1) The purpose is lawful and consent has been obtained for that use; or

2) The use is required or permitted by the *Personal Health Information Act.*

A custodian must limit the use of personal health information by its employees, agents, contractors and volunteers, as well as health professionals with the right to treat persons at a health care facility operated by the custodian to those individuals who need to know the information to carry out the purpose for which the information was collected.

A custodian must not use personal health information if other information will serve the purpose.

A custodian must limit the use of personal health information in its custody or control that to the minimum amount necessary to achieve the purpose, unless it is a requirement of law.

Uses permitted without consent

Regardless of an individual's consent directives, a custodian may use personal health information without the consent of the individual who is the subject of the information for the following purposes.

Purpose for Collection

- In accordance with the purpose for which the information was collected or created, as well as all the functions reasonably necessary for carrying out that purpose;

- In accordance with the purpose for which the information was disclosed to the custodian in compliance with an Act or an Act of Canada, or;

- Another use to which the individual who is the subject of the personal health information consents

Health Care Delivery and Planning

- For seeking the consent of the individual or his or her representative, where the personal health information used by the custodian for this purpose is limited to the name and contact information of the individual or the individual's representative;

- For the delivery of health care programs or services that are provided or funded by the custodian including planning, delivering, evaluating, monitoring or preventing fraud or unauthorized receipt of services or benefits;

- Where the custodian is a minister or a department, for the purpose of obtaining health care cost recovery;

- For obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services;

- Where the custodian is a rights advisor under the *Mental Health Care and Treatment Act* for the performance of functions referred to in the *Mental Health Care and Treatment Act*, or;

- Where the custodian is an authority; a board, council, committee, commission, corporation or agency established by an authority, a department created under the *Executive Council Act*, or a branch of the executive

government of the province, engaged in the delivery or administration of health care in the province; the minister, or the Centre for Health Information the following functions are permitted within the geographic area in which the custodian has jurisdiction:

- planning and resource allocation,
- health system management,
- public health surveillance, and
- health policy development.

Quality and Risk Management

- Risk management or error management;

- Activities to improve or maintain the quality of care or activities to improve or maintain the quality of related programs or services, or;

- To prevent or reduce a risk of serious harm to:

    - the mental or physical health or safety of the individual the information is about or another individual; or
    - public health or public safety

Proceedings or Legal Requirements

- A proceeding or contemplated proceeding in which the custodian is or is expected to be a party or witness and the information relates to the proceeding, or;

- As permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada

Research and/or Transforming into De-Identified Information

- For research projects that are approved by a research ethics board or research ethics body under the *Health Research Ethics Authority Act*;

- Disposing information in compliance with the Act; or modifying it to conceal the identity of the individual who is the subject of the personal health information; or

- To produce information that does not, either by itself or in combination with other information in the custody of or under the control of the custodian, permit an individual to be identified.

THINGS TO REMEMBER:

Prior to using personal health information, the custodian must ensure that the information is accurate, complete and up-to-date.

Consent directives limiting or withdrawing consent do not have the effect of restricting collection, use or disclosure required or permitted by law. Consent directives limiting or withdrawing consent also do not have the effect of restricting the recording of personal health information required by standards of professional or institutional practice.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.40 Accuracy of Information
1.70 Notification of Uses and Public Statements
2.10 Consent Requirements
2.40 Withdrawal of Consent
4.20 Confidential Use of Personal Health Information

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Health Research Ethics Authority Act*, SNL 2006, c. H-1.2.

Province of Newfoundland and Labrador: *Mental Health Care and Treatment Act*, SNL 2006, c. M-9.1.

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 33 - 35.

4.20 Confidential use of personal health information

PURPOSE:

To inform custodians of the confidentiality and privacy requirements that must be met before personal health information can be used.

DEFINITIONS:

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

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

SAMPLE POLICY:

Custodians, their employees, agents, contractors and volunteers, as well as health professionals with the right to treat persons at a health care facility operated by the custodian are responsible for maintaining all personal health information in a confidential manner and comply with all legislative requirements and confidentiality policies and procedures.

Custodians must also protect the confidentiality of personal health information in their custody or control that will be stored or used in a jurisdiction outside the province.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.20 Oath or Affirmation of Confidentiality
1.70 Notification of Uses and Public Statements

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 13 and 15.

4.30 Transforming personal health information

PURPOSE:

To provide custodians with a common and consistent approach to transforming personal health information into de-identified and other forms of information.

DEFINITIONS

The following definitions from the "Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans", (2008, p 44-45) are useful for decision making related to transforming personal health information into de-identifiable information.

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

2. 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.

3. 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.

4. Anonymized Information: Information is irrevocably stripped of identifiers, and a code is not kept to allow future linkages.

5. Anonymous Information: Information never had identifiers associated with it (*e.g.*, as in the case of anonymous surveys).

SAMPLE POLICY:

A custodian must not disclose more personal health information than is reasonably necessary to meet the purpose.

When identifiable personal health information is not required, the custodian is permitted to strip, encode or otherwise transform personal health information to create de-identified health information for use or disclosure.

THINGS TO REMEMBER:

When identifiable personal health information is transformed into de-identified health information, it is no longer "personal health information" as defined by or for the purposes of the *Personal Health Information Act*.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

5.90 Disclosure of Personal Health Information for Research Purposes
5.110 Disclosure of Personal Health Information to a Registry

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 21.

REFERENCES:

Interagency Advisory Panel on Research Ethics. (2008, December). *Draft 2nd Edition of the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.* Government of Canada.

Newfoundland Labrador Health and Community Services	*PERSONAL HEALTH INFORMATION ACT* **Policy Development Manual** **Section: 5.0 - Disclosure** Sample Policy: 5.10 DISCLOSURE OF PERSONAL HEALTH INFORMATION

5.10 Disclosure of personal health information

PURPOSE:

To inform custodians of the requirements that must be met before personal health information can be disclosed.

DEFINITIONS:

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.

SAMPLE POLICY:

Custodians are responsible for protecting the confidentiality of the information and the privacy of the individual when disclosing personal health information.

A custodian must not disclose more personal health information than is reasonably necessary to meet the purpose.

Prior to the disclosure of personal health information, custodians are required to ensure that the following requirements are met:

- The information is being disclosed as permitted or required by the *Personal Health Information Act*;
- Consent to disclose the information, if required, has been obtained;
- Reasonable steps are taken to identify that the correct information is being disclosed and that it is accurate, complete and up-to-date;
- The information is being disclosed to the intended and authorized recipient;

- When the information for disclosure is not in electronic form, but it is paper, films, or other medium, the following information is recorded:

    - The name of the person to whom the custodian disclosed the information;
    - The date of the disclosure;
    - The purpose of the disclosure; and
    - A description of the information disclosed.

- When disclosure of personal health information is electronic and provided via access to an information system, that the following information be logged:

    - The identity of the user;
    - The date and time the information was accessed; and
    - A description of the information accessed or available for access.

    If the information system does not capture the above information in electronic log files, details must be recorded manually as with other disclosures.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

2.50 Disclosure without Consent
5.20 Preventing Unauthorized Disclosure
5.30 Accuracy of Disclosed Personal Health Information

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 16, 48 and 49.

5.20 Preventing unauthorized disclosure of personal health information

PURPOSE:

To provide custodians with a common and consistent approach to preventing the unauthorized disclosure of personal health information.

SAMPLE POLICY:

Custodians are responsible for protecting the personal health information in their custody or control from unauthorized disclosure through the use administrative, technical and physical safeguards that are reasonable under the circumstances.

Custodians are required to take appropriate measures to authenticate the identity of the individual to whom information is being disclosed, prior to the disclosure of such information.

Personal health information stored electronically must only be held on a computer, server or network that is designated for that purpose.

SAMPLE PROCEDURE:

The following non-exhaustive list of measures should be in place to protect personal health information from unauthorized disclosure:

- Where and as appropriate. electronically-stored personal health information should be protected via privacy-enhancing technologies such as encryption, access controls, routine audits and firewalls. Subject matter experts should be consulted to determine the appropriate methodologies for protecting electronically-stored personal health information;

- Computer monitors must exhibit features such as privacy screens, screensavers and timeout mechanisms or be situated to prevent unauthorized access to the information on the screen;

- Fax machines and printers should be located in secure areas;

- All email or facsimile disclosures must include confidentiality clauses that state the following:

    - The information is confidential and intended only for the recipient;
    - Instructions to delete or shred any information obtained in error; and
    - Include contact information with a request to notify the sender immediately if received in error.

- All file cabinets must be locked when not in use;

- A clean desk practice should be implemented to ensure that personal health information is stored securely when not in use;

- All paper-based personal health information should be signed out of a storage area by an authorized person; and,

- Security systems should be implemented to secure physical premises.

THINGS TO REMEMBER:

Preventative strategies must be the focus to stop unauthorized disclosure of personal health information.

Unauthorized disclosure of personal health information can negatively impact the individual who is the subject of the personal health information, the custodian responsible for the unauthorized disclosure and the health care system as a whole, and is an offence under the Act.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 13, 15 and 16.

REFERENCES:

Office of the Privacy Commissioner of Canada, (2008). *PIPEDA Self Assessment Tool: Personal Information Protection and Electronic Documents Act*, p. 23-26.

5.30 Accuracy of disclosed personal health information

PURPOSE:

To provide custodians with a common and consistent approach to ensuring the accuracy of the personal health information disclosed.

SAMPLE POLICY:

Custodians must take reasonable steps to ensure that personal health information is disclosed for the intended purpose and is accurate, complete and up-to-date.

SAMPLE PROCEDURE:

Prior to the disclosure of information, a custodian must:

- Confirm that the personal health information being disclosed pertains to the correct individual. This should be done by cross referencing the individual's
  - Name;
  - Date of birth;
  - MCP number, or other unique identifier, if available; and
  - Address.

- Determine the specific information requested. Disclosures should be limited to the minimum amount of personal health information necessary to meet the request.

- Review the personal health information intended for disclosure to determine the accuracy, completeness and up-to-date status of the information.

- If the custodian has any concerns related to the accuracy, completeness or up-to-date status of the personal health information, they must inform the recipient.

- If the custodian discloses personal health information about an individual with a limited consent directive in place and the personal health information is

limited to less than the disclosing custodian considers reasonably necessary for the provision of health care to the individual, the custodian must notify the receiving entity of that fact.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.40 Accuracy of Personal Health Information
2.30 Limited Consent
5.10 Disclosure of Personal Health Information

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 16.

5.40 Disclosure of personal health information to relatives

PURPOSE:

To identify situations where disclosure of personal health information to relatives without consent is permitted.

DEFINITIONS:

A **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.

SAMPLE POLICY:

Unless the disclosure is contrary to an express request of the individual, without the consent of the individual who is the subject matter of the information, a custodian may disclose personal health information to a person other than a custodian for the purpose of contacting a relative, friend or potential substitute decision-maker of the individual, where the individual is injured, incapacitated or ill and unable to give consent personally.

A person who operates:

(i) a health care facility,
(ii) a licensed pharmacy as defined in the *Pharmacy Act*,
(iii) an ambulance service, or
(iv) a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider;

is permitted to disclose personal health information about an individual who is a patient or resident in a health care facility operated by the custodian to a person that the custodian reasonably believes is a member of the individual's immediate family,

a relative or a person with whom the individual has a close personal relationship where:

(a) the custodian offers the individual the option, at the first reasonable opportunity after admission to the facility, to object to that disclosure and the individual does not do so; and,

(b) the disclosure is made in accordance with accepted professional practice.

A custodian may also disclose personal health information to relatives in the following situations where the individual is deceased or presumed to be deceased:

1. To identify an individual who is deceased or presumed to be deceased;

2. To inform a person that the individual is deceased or presumed to be deceased and the circumstances of the death, where appropriate;

3. To the personal representative of the deceased for a purpose related to administration of the estate of the deceased individual;

4. To allow the spouse, partner, siblings or descendants of a deceased individual to make decisions about his or her own health care or the health care of his or her child or where the disclosure is necessary to provide health care to the recipient.

THINGS TO REMEMBER:

Disclosure should be limited to the minimum amount of personal health information necessary.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Advance Health Care Directives Act*, SNL 1995, c. A-4.1, s. 10.

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 37 and 38.

5.50 Disclosure of personal health information to a successor

PURPOSE:

To identify the situations where disclosure of personal health information without consent to a successor is permitted under the *Personal Health Information Act*.

DEFINITION:

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

SAMPLE POLICY:

Custodians are permitted to disclose personal health information to a successor or potential successor without the consent of individuals for the following purposes and under the following circumstances:

- To provide a potential successor the opportunity to assess and evaluate the operations of the custodian on condition that the potential successor first enters into an agreement with the custodian to keep the information confidential and secure and not to retain the information any longer than is necessary for the purpose of the assessment or evaluation; or

- Where the custodian transfers records to the successor as a result of the custodian ceasing to be a custodian or ceasing to provide health care within the geographic area in which the successor provides health care and the successor is a custodian.

A custodian transferring personal health information to another custodian must make reasonable efforts to inform individuals whose information is to be transferred prior to the transfer taking place.

When prior notice of the transfer is not possible, information regarding the transfer must be made available by way of public notice of the transfer. The public notice must contain the following information:

- That the custodian has ceased or will cease to be a custodian within the jurisdiction;
- The identity and contact information of the successor; and
- How an individual whose personal health information is in the custody or control of the custodian may access his or her record after the transfer.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 39.

5.60 Disclosure of personal health information for health and safety purposes

PURPOSE:

To identify situations where disclosure of personal health information is permitted for reasons related to health and safety without the consent of the individual.

SAMPLE POLICY:

A custodian is permitted to disclose personal health information without the consent of that individual where the custodian reasonably believes that disclosure is required:

- To prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual the information is about;
- To prevent or reduce a risk of serious harm to the mental or physical health or safety of another individual; or
- For public health or safety.

A custodian is permitted to disclose personal health information without the consent of that individual to the superintendent of a correctional facility in which the individual is lawfully detained or to the administrator of a psychiatric unit in which the individual is detained to assist the facility or unit in making a decision respecting the following:

- Making arrangements for the provision of health care to the individual; or
- Placing the individual into custody, detention, release, conditional release, discharge or conditional discharge under the following:
    - *Mental Health Care and Treatment Act;*
    - *Prisons Act*;
    - *Young Persons Offences Act* and regulations under that Act;

- Part XX.1 of the *Criminal Code*;
- *Prisons and Reformatories Act* (Canada); and
- *Youth Criminal Justice Act* (Canada).

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 40.

Province of Newfoundland and Labrador: *Mental Health Care and Treatment Act*, SNL 2006, c. M-9.1.

Province of Newfoundland and Labrador: *Prisons Act*, RSNL 1990, c. P-21.

Government of Canada: *Youth Criminal Justice Act*, S.C. 2002, c. 1.

Government of Canada: *Criminal Code*, R.S.C. 1985, c. 46.

Government of Canada: *Prisons and Reformatories Act*, R.S. 1985, c. P-20.

5.70 Disclosure of personal health information for legal proceedings

PURPOSE:

To identify situations where disclosure without the consent of the individual of personal health information is permitted for reasons related to proceedings.

SAMPLE POLICY:

Mandatory disclosures

A custodian is obligated to disclose personal health information without the consent of that individual, in the following situations:

- To a body responsible for the discipline of a health care professional or for the quality or standards of professional services provided by a health care professional, including an investigation by that body; or

- For the purpose of complying with a summons, subpoena, warrant, demand, order or similar requirement issued by a court, person or entity, including the commissioner, with jurisdiction to compel the production of personal health information or with a rule of court concerning the production of personal health information in a proceeding.

Discretionary disclosures

A custodian is permitted to disclose personal health information without the consent of the individual for the following purposes:

- A proceeding or contemplated proceeding in which the custodian is or is expected to be a party or a witness where the information relates to or is a matter in issue;

- A committee as referred to in subsection 8.1(2) of the *Evidence Act*;

- To a proposed guardian or legal representative for the purpose of the appointment of a person as a guardian or representative for an individual;

- To a guardian authorized under an Act of the province or the *Rules of the Supreme Court, 1986*, to commence, defend or continue a proceeding on behalf of the individual or to represent the individual in a proceeding; or

- For the purpose of laying an information, order or making an application for an order where the personal health information relates to or is a matter in issue in the information or application.

THINGS TO REMEMBER:

Information relating to the health care provider can be included in personal health records disclosed for proceedings.

Disclosures should be limited to the personal health information requested.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 41.

Province of Newfoundland and Labrador: *Evidence Act*, RSNL 1990, c.E-16, s. 8.1(2).

Province of Newfoundland and Labrador: *Rules of the Supreme Court*, SNL 1986, c.42, Schedule D.

5.80 Disclosure of personal health information for law enforcement purposes

PURPOSE:

To identify the situations where disclosure of personal health information without consent is permitted for law enforcement purposes.

SAMPLE POLICY:

Mandatory disclosures

A custodian must disclose any personal health information required without the consent of that individual in the following situations:

- The disclosure is required by a provincial Act, federal Act or by a treaty, agreement or arrangement made under these Acts, to authorized recipients under those Acts or instruments.

- The disclosure is required to carry out or facilitate an inspection, investigation or similar procedure for the purpose that is authorized by or under:

    - The *Personal Health Information Act*;
    - The *Child, Youth and Family Services Act*;
    - Another provincial Act; or
    - An Act of Canada

  to authorized recipients under those Acts, where the disclosure is for the purpose of facilitating an inspection, investigation or similar procedure.

Discretionary disclosures

A custodian is permitted to disclose personal health information without the consent of the individual to another custodian where the custodian disclosing the information has a reasonable expectation that disclosure will:

- Detect or prevent fraud;
- Limit abuse in the use of health care; or
- Prevent the commission of an offence under an Act of the province or of Canada.

THINGS TO REMEMBER:

Information relating to the health care provider can be included in personal health records disclosed for enforcement purposes.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 42 and 43.

5.90 Disclosure of personal health information for research purposes

PURPOSE:

To identify the situations where disclosure of personal health information without consent is permitted for research purposes.

SAMPLE POLICY:

A custodian is permitted to disclose personal health information without the consent of the individual who is the subject of the information for the purposes of research where a research project has been approved by a research ethics board or research ethics body under the *Health Research Ethics Authority Act*.

A custodian must not disclose personal health information if other information will serve the purpose of the disclosure.

THINGS TO REMEMBER:

Disclosure should be limited to the minimum amount of personal health information necessary.

A person who is not a custodian does not become a custodian because they hold personal health information disclosed to them by a custodian.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Health Research Ethics Authority Act*, SNL 2006, c. H-1.2.

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 36, 44 and 50.

Newfoundland Labrador Health and Community Services	*PERSONAL HEALTH INFORMATION ACT* **Policy Development Manual** Section: 5.0 DISCLOSURE Sample Policy: 5.100 DISCLOSURE OF PERSONAL HEALTH INFORMATION OUTSIDE THE PROVINCE

5.100 Disclosure of personal health information outside the province

PURPOSE:

To provide custodians with a common and consistent understanding of the circumstances under which the disclosure of personal health information to entities outside of the province of Newfoundland and Labrador is permitted.

SAMPLE POLICY:

A custodian is permitted to disclose personal health information to entities outside of the province of Newfoundland and Labrador under any of the following circumstances:

- The individual who is the subject of the information consents to the disclosure;

- The disclosure is permitted by the *Personal Health Information Act* or the regulations enacted under the *Personal Health Information Act*;

- The person receiving the information performs functions similar to the functions performed by the superintendent of a correctional facility or the administrator of a psychiatric unit in the province of Newfoundland and Labrador;

- The disclosure meets all the following conditions:
    - The purpose of the disclosure is health planning or health administration;
    - The information relates to health care provided in the province to a person who is a resident of another province or territory of Canada, and
    - The disclosure is made to the government of that province or territory of Canada;

- The disclosure is reasonably necessary for the provision of health care to the individual; or

- The disclosure is reasonably necessary for the administration of payment or for contractual or legal requirements in connection with the provision of health care to the individual.

If the custodian discloses personal health information about an individual with a limited consent directive in place and the personal health information is limited to less than the disclosing custodian considers reasonably necessary for the provision of health care to the individual, the custodian must notify the receiving entity of that fact.

THINGS TO REMEMBER:

information managers whose services are engaged outside of the province of Newfoundland and Labrador must comply with provisions of the *Personal Health Information Act.*

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.70 information manager Agreements

Appendix "A" – Information Management Agreement Principles

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 47.

Newfoundland Labrador Health and Community Services	*PERSONAL HEALTH INFORMATION ACT* **Policy Development Manual** Section: 5.0 DISCLOSURE Sample Policy: 5.110 DISCLOSURE OF PERSONAL HEALTH INFORMATION TO A REGISTRY

5.110 Disclosure of personal health information to a registry

PURPOSE:

To identify the situations where disclosure of personal health information to a registry, without consent, is permitted within the *Personal Health Information Act*.

DEFINTION:

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

SAMPLE POLICY:

Custodians must disclose personal health information, without the consent of the individuals, to a custodian designated in the regulations under the *Personal Health Information Act* who maintains a registry for:

- Facilitating or improving the provision of health care; or
- Relating to the storage or donation of body parts or bodily functions.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 39.

6.10 Access to personal health information

PURPOSE:

To provide custodians with a common and consistent approach to providing individuals access to their personal health information.

SAMPLE POLICY:

Right of Access

With certain exceptions, an individual has a right of access to a record containing their personal health information that is in the custody or under the control of a custodian.

A custodian may require an access request to be in writing unless the individual making the request:

- has limited ability to read or write English; or
- has a disability or a condition that impairs his or her ability to make a request in writing.

Exceptions

A custodian must refuse to permit an individual to examine or receive a copy of a record of their personal health information where:

- Where another Act, an Act of Canada or a court order prohibits disclosure of the record or the information contained in the record to the individual;

- Where granting access would reveal personal health information about an individual who has not consented to disclosure; or

- Where the information was created or compiled for the purpose of

- A committee as referred to in s.8.1(2) of the *Evidence Act*;
- Studying or evaluating health care practice by a standards or quality assurance committee; or
- The disciplinary process of health care professionals by a statutory body or for the quality or standards of professional services provided by health care professionals.

A custodian may refuse to permit an individual to examine or receive a copy of a record of his or her personal health information where:

- The record or the information in the record is subject to a legal privilege (e.g., solicitor-client privilege) that restricts disclosure of the record or the information;

- The information in the record was collected or created for use in a proceeding and the proceeding, together with all appeals or processes resulting from it, has not been concluded;

- The following conditions are met:

    - the information was collected or created during an inspection, investigation or similar procedure authorized by law or for detecting, monitoring or preventing the receipt of a service or benefit under an Act or program operated by the minister, or a payment for that service or benefit, and
    - the inspection, investigation or all proceedings, appeals or processes resulting from it, have not been concluded; or

- Granting access could reasonably be expected to:

    - result in a risk of serious harm to the mental or physical health or safety of the individual who is the subject of the information or another individual,
    - lead to the identification of a person who was required by law to provide information in the record to the custodian, or
    - lead to the identification of a person who provided information in the record to the custodian in confidence under circumstances in which confidentiality was reasonably expected.

Refusing an Access Request

A custodian may further refuse to grant a request for access to a record of personal health information where the custodian believes on reasonable grounds that the request for access to the record is:

- Frivolous or vexatious;
- made in bad faith; or
- for information already provided to the individual.

Informing the Individual

Where the requested personal health information is outside the access provisions of the *Personal Health Information Act,* the custodian must inform the individual in writing that the request is refused and why.

The custodian must also inform the individual that they may appeal the refusal to the Trial Division or request a review of the refusal by the Information and Privacy Commissioner.

The custodian is required to respond to the access request from the individual in a prompt manner and within sixty days of receiving the request. An extension of thirty (30) days is available when the request meets the following criteria and the custodian has informed the individual in writing of the reasons for the needed extension:

- Meeting the sixty (60) day time limit would unreasonably interfere with the operations of the custodian; or

- The information consists of numerous records or locating the information cannot be completed within the time limit.

The custodian may grant or refuse the individual's request as soon as possible and in any event not later than the expiration of the time limit as extended.

The custodian may provide personal health information to an individual from a record that is not a record dedicated primarily to personal health information about the individual who is requesting access, by severing all additional information from the record prior to providing access.

If after reasonable efforts the requested record is not located or does not exist, the custodian must inform the individual in writing of this fact.

Where a custodian fails to respond to a request for access within the sixty (60) or ninety (90) day time period he or she must be considered to have refused the request for access and the individual requesting access may appeal that refusal to the Trial Division or request a review of the refusal by the Information and Privacy Commissioner.

SAMPLE PROCEDURE:

When the request for access is from the individual who is the subject of that information, the custodian can grant access to his or her personal health information based on an oral request for access or without request, provided that access is authorized under the Act.

It is recommended that prior to providing an individual access to their personal health information, the custodian require the following:

- The request in writing unless the individual making the request
    - has limited ability to read or write English; or
    - has a disability or a condition that impairs his or her ability to make a request in writing;
    - In these situations, other acceptable methods of facilitating access should be explored.

- Where possible, the request should identify when the personal health information would have been collected, used and/or disclosed;
- The request must contain sufficient information to allow for information retrieval with reasonable effort;
- The requester must be agreeable to any fees related to the request; and
- The individual when presenting to review the personal health information must provide two pieces of identification.

Requests for access to personal health information must be dated when received.

The custodian must contact the individual to clarify the request if the information on the request form is incomplete or unclear.

The custodian, if requested by the individual, may provide a copy of the personal health information.

THINGS TO REMEMBER:

A custodian has a legal obligation to provide personal health information as expeditiously as is necessary for the provision of health care to the individual.

An individual must not be refused access to a certificate of involuntary admission or a community treatment order issued under the *Mental Health Care and Treatment Act* in respect of that individual.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Evidence Act*, RSNL 1990, c.E-16, s.8.1.

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 51 - 59.

6.20 Correction and amendment of personal health information

PURPOSE:

To provide custodians with a common and consistent approach to responding to requests for correction or amendment of records containing personal health information.

SAMPLE POLICY:

Where a custodian has granted an individual access to a record containing their personal health information, and where the individual believes that the record is inaccurate or incomplete, the individual may request that the custodian correct the information.

Custodians may accept a request for correction or amendment from the individual in either oral or written form. Requests must contain the following information:

- The individual's
  - Name;
  - Date of birth;
  - MCP number, or other unique identifier; and
  - Address.

- Sufficient information to allow for record retrieval with reasonable effort, such as the dates the personal health information would have been collected, used and/or disclosed.

The custodian is required to respond to the access request from the individual in a prompt manner and within thirty (30) days of receiving the request. An extension of thirty (30) days is available when the request meets the following criteria and the custodian has informed the individual in writing of the reasons for the needed extension:

- Meeting the thirty (30) day time limit would unreasonably interfere with the operations of the custodian; or
- The information that is the subject of the correction or amendment request is located in numerous records and cannot be completed within the time limit.

The custodian may grant or refuse the individual's request for correction or amendment as soon as possible and in any event not later than the expiration of the time limit as extended.

The custodian cannot charge a fee to an individual when requesting a correction of their personal health information.

The custodian must grant the request for correction where the individual making the request demonstrates to the satisfaction of the custodian that the record is incomplete or inaccurate for the purposes for which the custodian uses the information, and provides the custodian the information necessary to enable the custodian to correct the record; or

The custodian may refuse to grant the request for correction in the following situations:

- The record was not originally created by the custodian and the custodian does not have sufficient knowledge, expertise and authority to correct the record;
- The information which is the subject of the request consists of a professional opinion or observation that a custodian has made in good faith about the individual; or
- The custodian believes on reasonable grounds that the request is frivolous, vexatious or made in bad faith.

Where a custodian fails to respond to a request for correction or amendment within the thirty (30) or sixty (60) day time period he or she shall be considered to have refused the request for correction and the individual requesting correction may appeal that refusal to the Trial Division or request a review of the refusal by the Information and Privacy Commissioner.

Where a request for a correction is granted, the custodian will make the requested correction by recording the correct information in the record and:

- Striking out the incorrect information in a manner that does not obliterate the record, or
- Where it is not possible to strike out the incorrect information, label the information as incorrect, sever the incorrect information from the record, store the incorrect information separately from the record, and maintain a link in the record that enables a person to trace the incorrect information, or
- where it is not possible to record the correct information in the record, by ensuring that there is a practical system in place to inform a person accessing

the record that the information in the record is incorrect and to direct the person to the correct information.

Where a request for a correction is granted, the custodian will provide written notice to the individual who made the request for correction of the specific action taken. The custodian must also provide written notice of the requested correction, to the extent reasonably possible, to a person to whom the custodian has disclosed the information within the 12 month period immediately preceding the request for correction, unless the custodian reasonably believes that the correction will not have an impact on the ongoing provision of health care or other benefits to the individual or where the individual requesting the correction has advised that notice is not necessary.

Where a custodian refuses to grant a request for correction they must:

- Annotate the personal health information with the correction that was requested and not made and, where practicable, notify a person to whom the information was disclosed within the 12 month period immediately preceding the request for correction of the notation unless the custodian reasonably expects that the notation will not have an impact on the ongoing provision of health care or other benefits to the individual or the individual requesting the correction has advised that notice is not necessary; and

- Provide the individual requesting the correction with a written notice setting out the correction that the custodian has refused to make, the refusal together with reasons for the refusal, and the right of the individual to appeal the refusal to the Trial Division or request a review of the refusal by the Information and Privacy Commissioner.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 60 - 63.

7.10 Duty to notify individual

PURPOSE:

To provide custodians with a common and consistent understanding of the requirements relating to notifying individuals of breaches of privacy under the *Personal Health Information Act*.

SAMPLE POLICY:

With specific exceptions, where personal health information in a custodian's custody or control has been:

(a) stolen;
(b) lost;
(c) disposed of, except as permitted by this Act or the regulations; or
(d) disclosed to or accessed by an unauthorized person.

a custodian must notify the individual who is the subject of the information at the first reasonable opportunity.

Exceptions

A custodian does not have to notify the individual who is the subject of the information where a custodian reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal health information will not have an adverse impact upon either:

(a) the provision of health care or other benefits to the individual who is the subject of the information; or

(b) the mental, physical, economic or social well-being of the individual who is the subject of the information.

unless advised to do so by the Privacy Commissioner.

Where a custodian is a researcher who has received personal health information from another custodian, they may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person, unless the custodian who provided the information to the researcher first obtains the individual's consent to contact by the researcher and informs the researcher that the individual has given consent.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

7.20 Duty to notify Commissioner

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 20 and 44.

7.20 Duty to notify Privacy Commissioner

PURPOSE:

To provide custodians with a common and consistent understanding of the requirements relating to notifying the Privacy Commissioner of breaches of privacy under the *Personal Health Information Act*.

SAMPLE POLICY:

Where a custodian reasonably believes that there has been a material breach, as defined in the regulations under the *Personal Health Information* Act, involving the unauthorized collection, use, or disclosure of personal health information, the custodian must inform the commissioner of the breach at the first reasonable opportunity.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

7.10 Duty to Notify Individual

Appendix "H" – Privacy Breach Incident Reporting Form

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 15.

Newfoundland Labrador Health and Community Services	*PERSONAL HEALTH INFORMATION ACT* **Policy Development Manual** **Section: 8.0 - Accountability** Sample Policy: 8.10 DEFINITION OF COMPLIANCE

8.10 Definition of compliance

PURPOSE:

To provide custodians with a consistent definition and common understanding of the compliance as it relates to the responsibilities and obligations arising under the *Personal Health Information Act*.

SAMPLE POLICY:

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

THINGS TO REMEMBER:

It is the responsibility of custodians to ensure compliance with the *Personal Health Information Act* in relation to their operations and also in relation to the activities of persons and/or entities acting under their authority, such as employees, volunteers or contractors.

Key criteria for establishing an effective compliance program which would be reasonably capable of reducing the prospect of breaching the *Personal Health Information Act* are:

- Oversight by high-level personnel;
- Exercising due care in delegating substantial discretionary authority (*i.e.*, exercising the degree of care that an ordinary and reasonable person would normally exercise under circumstances like those at issue);
- Effective communication to all levels of employees, volunteers and / or contractors;
- Taking reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal;

- Consistent enforcement of compliance standards including disciplinary mechanisms; and,
- Taking reasonable steps to respond to and prevent further similar incidents of non-compliance upon detection; and,
- Continuing review and revision of policies and procedures related to personal health information by high-level personnel with experience, knowledge and expertise in matters of personal health information, security and privacy.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 13, 14 and 22.

8.20 Responsibilities related to review by Privacy Commissioner

PURPOSE:

To provide custodians with a basis for a common and consistent approach to responsibilities and obligations related to the conduct of a review by the Privacy Commissioner arising under the *Personal Health Information Act*.

DEFINITIONS:

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) a denial by a custodian of a request for access or correction; or
(b) an alleged breach of a provision of this Act or the regulations.

SAMPLE POLICY:

Where an individual believes on reasonable grounds that a custodian has contravened or is about to contravene a provision of this Act or the regulations in respect of his or her personal health information or the personal health information of another, they may file a complaint with the Privacy Commissioner.

In conducting a review, the commissioner may receive and accept any evidence and other information that the commissioner sees fit, whether on oath or by affidavit or otherwise, and whether or not it is or would be admissible in a court of law.

In conducting a review, the commissioner may:

(a) demand from the custodian a copy of a book, record or document or extract from a book, record or document relevant to the subject-matter of the review;

(b) inquire into all information, records, information practices of the custodian and other matters that are relevant to the subject-matter of the review; and

(c) use a data storage, processing or retrieval device or system belonging to the custodian under investigation in order to produce a record in readable form of a book, record or other document relevant to the subject-matter of the review.

A custodian having custody of a record, book or document requested by the commissioner must make a copy and produce it to the commissioner and must, on the request of the commissioner, provide whatever assistance is reasonably necessary, including using any data storage, processing or retrieval device to produce a record in readable form.

A custodian must not obstruct the commissioner who is exercising powers under the *Personal Health Information Act* or provide the commissioner with false or misleading information.

A custodian must produce to the commissioner a copy of the information requested by the commissioner within 14 days of receipt of the request, except where it is impractical to do so.

Where it is impractical to comply with the commissioner's request, a custodian may require the commissioner to examine the original at its site.

Within 15 days after receiving a report of the commissioner that contains a recommendation, the custodian must decide whether or not to comply with the recommendation in whole or in part and must give written notice of their decision to both the commissioner and to the complainant.

Where a custodian decides not to comply with a recommendation made by the commissioner, in whole or in part, the written response of the custodian must advise the complainant of their right to appeal to the Supreme Court of Newfoundland and Labrador, Trial Division under Part VII of the *Personal Health Information Act* and must include the time limit for commencement of an appeal provided in that part.

<u>THINGS TO REMEMBER:</u>

In conducting a review, the commissioner has the powers, privileges and immunities that may be conferred on a commissioner under the *Public Inquiries Act, 2006* except as otherwise provided under the *Personal Health Information Act*.

The burden of proof in respect of the subject-matter of the complaint is on the custodian, meaning that it will be the responsibility of the custodian to prove on a balance of probabilities that a breach or contravention of the Act has occurred.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

8.30 Consequences of Willful Disregard of the Act

Appendix "H" – Privacy Breach Incident Reporting Form

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 65 - 79.

Province of Newfoundland and Labrador: *Public Inquiries Act*, *2006*, SNL 2006, c. P-38.1.

8.30 Consequences of the willful disregard of the Act

PURPOSE:

To provide custodians with a basis for a common and consistent understanding of the potential consequences of willfully disregarding provisions of the *Personal Health Information Act*.

DEFINITIONS:

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

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

Willful means deliberate.

SAMPLE POLICY:

A person who wilfully:

(a) obtains or attempts to obtain another individual's personal health information by falsely representing that the person is entitled to the information;

(b) makes a false statement to, or misleads or attempts to mislead, the commissioner or another person performing duties or exercising powers under this Act;

(c) obstructs the commissioner or another person performing duties or exercising powers under this Act; or

(d) destroys or erases personal health information with the intent to evade a request for access to the information,

is guilty of a criminal offence and is liable to a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.

THINGS TO REMEMBER:

This sample policy is intended to apply to situations involving the willful or deliberate disregard of a provision of the *Personal Health Information Act*.

Other provisions of the Act may have application to situations involving an unintentional or inadvertent failure to comply with the Act; this would have to be determined by reference to the facts of the situation(s) on a case-by-case basis.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 88.

8.40 Consequences of failing to protect personal health information

PURPOSE:

To provide custodians with a basis for a common and consistent understanding of the potential consequences of failing to protect personal health information as required by the *Personal Health Information Act*.

SAMPLE POLICY:

A custodian or information manager who:

(a) collects, uses or discloses personal health information contrary to the *Personal Health Information Act*;

(b) fails to protect personal health information in a secure manner as required by the Act; or

(c) discloses personal health information contrary to this Act with the intent to obtain a monetary or other material benefit or to confer such a benefit on another person,

is guilty of an offence and may be liable to a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.

A custodian or information manager will not be found to have contravened the Act if the custodian or information manager can establish that all reasonable steps were taken to prevent the contravention.

THINGS TO REMEMBER:

This sample policy is intended to apply to situations involving either the intentional or unintentional failure to comply with the Act, and to intentional disclosures of personal

health information contrary to the *Personal Health Information Act* with the intent to obtain a monetary or other material benefit.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

1.80 information manager Agreements

Appendix "A" – Information Management Agreement Principles

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 88.

8.50 Immunity from suit

PURPOSE:

To provide custodians with a basis for a common and consistent understanding of the circumstances under which they will be immune from civil liability under the *Personal Health Information Act* for actions relating to the custody of personal health information.

DEFINITIONS:

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.

SAMPLE POLICY:

A civil action does not lie against a custodian, or a person acting for or under the direction of a custodian, for damages resulting from a collection, use or disclosure of or a failure to disclose personal health information under this Act where the act or failure to act was done or made in good faith.

THINGS TO REMEMBER:

This sample policy is intended to apply to circumstances involving potential civil actions, and addresses the circumstances under which a custodian or a person acting for or at the direction of a custodian will be immune from a civil action.

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 87.

8.60 Non-retaliation

PURPOSE:

To provide custodians with a common and consistent understanding of their responsibilities in relation to individuals who report contraventions or possible contraventions of the *Personal Health Information Act*.

DEFINITIONS:

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

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.

SAMPLE POLICY:

A person cannot dismiss, suspend, discipline, demote, harass or otherwise disadvantage or penalize an individual where:

(a) the individual, acting in good faith and on the basis of reasonable belief, has disclosed to the commissioner that another person has contravened or is about to contravene a provision of the *Personal Health Information Act* or the regulations;

(b) the individual, acting in good faith and on the basis of reasonable belief has done or stated an intention of doing something that is required to avoid having a person contravene a provision of the Act or the regulations;

(c) the individual, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention to refuse to do something that is in contravention of the Act or the regulations; or

(d) another person believes that the individual will do an act described in paragraph (a), (b) or (c).

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 89.

8.70 Information asset profile

PURPOSE:

To provide custodians with guidance on how to manage the various information assets containing personal health information in their custody and control.

DEFINITIONS:

An **information asset** in the context of this policy development manual is any compiled set of records of personal health information held by a custodian. For example, an information asset can be a set of patient records held in paper form, or a database of patient records held electronically.

SAMPLE POLICY:

A custodian of personal health information must ensure that an accurate and up-to-date information asset profile is prepared for each discrete information asset over which it has custody or control.

The purpose of an information asset profile is to maintain on an ongoing basis a record of key information about an information asset that can be made available to authorized information asset stakeholders.

SAMPLE PROCEDURE:

1. An information asset profile will form a part of a custodian's information handling policies and procedures, and must be maintained by a party possessing the skills and experience to do so.

2. Each information asset profile must be reviewed and updated as required no less frequently than on an annual basis.

3. In addition to regular annual reviews, each information asset profile must be reviewed and updated where the information that forms the subject matter of

the information asset profile is collected, used or disclosed in a manner not addressed in the Information Asset Profile.

THINGS TO REMEMBER:

Records-management procedures adopted must meet Information Management industry standards.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

Appendix "D" – Sample Information Asset Profile

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 15.

8.80 Frequency of privacy audits

PURPOSE:

To provide custodians with guidance on how frequently to conduct audits of their privacy practices.

DEFINITIONS:

Risk management in the context of this policy development manual 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.

Privacy audit in the context of this policy development manual means a tool or process that 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.

SAMPLE POLICY:

A custodian of personal health information must ensure that a privacy audit is conducted on a regularly scheduled basis in order to ensure that the physical, administrative and technological controls it has established to protect the confidentiality of the personal health information in its custody or control are effective in accomplishing same.

A privacy audit must be conducted as required, but no less frequently than on an annual basis.

The management, executive or other controlling entity of the custodian (*i.e.*, in certain circumstances, the custodian themselves) must conduct / review the results of all privacy audits.

The results of a privacy audit must be incorporated into a custodian's risk management strategy. This may include effecting revisions to a custodian's privacy impact assessment(s), policy statement(s), and / or physical or technological security control(s).

THINGS TO REMEMBER:

Templates for a privacy impact assessment and a privacy audit are included in the PHIA Risk Management Toolkit as produced by the Newfoundland and Labrador Department of Health and Community Services.

Risk management activities such as conducting privacy impact assessments and privacy audits allow a custodian to identify and understand the risks to which it is exposed, and should enable it to implement controls sufficient to mitigate that risk.

Information security management is 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.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

Appendix "C" – Information Security Management Overview

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 15.

9.10 Appeal by individual

PURPOSE:

To provide custodians with a common and consistent understanding of their responsibilities in relation to individuals who appeal decisions made by custodians regarding access and correction.

SAMPLE POLICY:

1. Right of Appeal

An individual may appeal the decision of a custodian to refuse access to a record to which they believe they may be entitled to have access.

An individual may appeal the decision of a custodian to refuse to amend or correct a record which they believe they may be entitled to have corrected.

An individual may appeal a decision made by a custodian by filing a notice of appeal, naming the custodian as the respondent, with the Registrar of the Supreme Court and by serving a copy of the notice of appeal on the minister responsible for health and on the Privacy Commissioner.

2. Circumstances of Appeal

A. Where no Review by Privacy Commissioner Requested by Individual

Where an individual has made a request to a custodian for access to or correction of personal health information under the *Personal Health Information Act* and has not requested a review by the Privacy Commissioner, the individual may appeal the decision of the custodian refusing to grant access to or make a correction of a record of personal health information. The appeal must be made by the individual within 30 days following receipt of a notice of refusal provided by the custodian where such notice is provided or where no notice provided, where the time to do so has expired.

B. Where no Review by Privacy Commissioner Conducted, or Where no Recommendation to Custodian by Privacy Commissioner yet Made

Where an individual has made a request to a custodian for access to or correction of personal health information under the *Personal Health Information Act* and the Privacy Commissioner has not conducted a review or, where a review has been conducted, has not made a recommendation to the custodian, the individual may appeal within 30 days of receipt of:

(i) the notice of the Privacy Commissioner where the Privacy Commissioner has refused to conduct a review, or

(ii) the report of the Privacy Commissioner where the Privacy Commissioner has conducted a review but has not made a recommendation.

C. Where Recommendation to Custodian by Privacy Commissioner Has Been Made

Where an individual has made a request to a custodian for access to or correction of personal health information under the *Personal Health Information Act* and the Privacy Commissioner has made a recommendation to the custodian and the custodian has decided not to comply with the recommendation either in whole or in part, an appeal by an individual must be made within 30 days of the receipt of the notice of the custodian or, where the custodian has not provided notice, within 30 days of the date on which notice should have been provided.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

6.10 Access To Personal Health Information
6.20 Correction and Amendment of Personal Health Information
8.20 Responsibilities Related to Review by Privacy Commissioner

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 83.

Newfoundland Labrador Health and Community Services	*PERSONAL HEALTH INFORMATION ACT* **Policy Development Manual** Section: 9.0 APPEALS Sample Policy: 9.0 APPEAL BY PRIVACY COMMISSIONER

9.20 Appeal by Privacy Commissioner

PURPOSE:

To provide custodians with a common and consistent understanding of their responsibilities in relation to an appeal made by the Privacy Commissioner in relation to decisions made by custodians regarding access and correction.

SAMPLE POLICY:

Right of Appeal

Where a custodian has provided notice that they have decided not to comply with a recommendation of the Privacy Commissioner, the Privacy Commissioner may, with the consent of the individual who made the request for access or correction, appeal that decision in accordance with the provisions of the *Personal Health Information Act*.

Where an individual has made a request to a custodian for access to or correction of personal health information under the *Personal Health Information Act* and either:

(a) the Privacy Commissioner has not conducted a review or, where a review has been conducted, has not made a recommendation to the custodian, or

(b) the Privacy Commissioner has made a recommendation to the custodian and the custodian has decided not to comply with the recommendation either in whole or in part

The Privacy Commissioner may intervene as a party to the appeal.

CROSS REFERENCE TO OTHER SAMPLE POLICIES:

6.10 Access To Personal Health Information
6.20 Correction and Amendment of Personal Health Information
8.20 Responsibilities Related to Review by Privacy Commissioner

LEGISLATIVE REFERENCES:

Province of Newfoundland and Labrador: *Personal Health Information Act*, SNL 2008, c. P-7.01, s. 84.

APPENDICES

Appendix "A":
- Information Management Agreement Principles

Appendix "B":
- Sample Oath / Affirmation of Confidentiality

Appendix "C":
- Information Security Management Overview

Appendix "D":
- Sample Database Profile

Appendix "E":
- Privacy Breach Guidelines

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

Appendix "G":
- Limited Consent under PHIA

Appendix "H":
- Privacy Breach Incident Reporting Form

Appendix "A"
Information Management Agreement Principles

Introduction

Under the Newfoundland and Labrador *Personal Health Information Act* (PHIA), a custodian of personal health information may engage the services of contractors or service providers to support their operations. Under certain circumstances, where the engagement requires the contractor or service provider to have access to, use or disclose personal health information in the custodian's control, a custodian is required by PHIA to enter into a written agreement with that contractor, known as an Information Management Agreement. The Information Management Agreement must ensure that the personal health information being accessed by the information manager is appropriately safeguarded.

This document is intended to provide custodians of personal health information with some guidance regarding the main principles that should be addressed when entering into an agreement with an information manager, as defined under PHIA.

The principles set out in this document are not exhaustive and this document is not intended to provide any conclusions regarding the potential risks or benefits of any particular service being provided by an information manager. Each custodian of personal health information should assess the potential risks and benefits in the context of their individual circumstances. As the stewards of very sensitive information, custodians must carefully consider the extent to which the personal health information in their custody or under their control will be used and / or disclosed in the context of a contract for service. Whenever personal health information is disclosed to an information manager, it is imperative that there be an agreement in place that governs the accountabilities for the protection of the information.

Information manager

An information manager is any third-party or external contractor or service provider that deals with a custodian's personal health information, on behalf of that custodian. PHIA defines an information manager as being a person or body, other than an employee of a custodian, acting in the course of their employment, that:

(1) processes, retrieves, stores or disposes of personal health information for the custodian, or

(2) provides information management or information technology services to the custodian.

Examples of information managers include contractors or service providers providing:

- Information technology services (*e.g.*, software vendors or developers),
- Information management services (*e.g.*, records classification)
- Data storage services
- Data destruction services
- Quality assessment services
- Risk management services

Information Management Agreements

When a custodian discloses personal health information to an information manager, the information manager may only use or disclose that information for the purposes authorized by the agreement. An agreement with an information manager must be in writing, and has to include clauses that provide for the protection of the personal health information the Information Manger will be dealing with on behalf of the custodian. The agreement has to address the protection of the information against unauthorized access, use, disclosure, disposition, loss or modification, in accordance with requirements of PHIA. The agreement must also includes provisions indicating that they will adhere to both PHIA as well as to the terms of the agreement itself.

This document does not establish either the specific form or the specific contents of Information Management Agreements; rather, it sets out some of the main issues that custodians of personal health information need to carefully consider in the context of engaging the services of external contractors or service providers. The provisions or clauses of each individual Information Management Agreement will have to be developed by custodians on a case-by-case basis in order to appropriately encompass the type and scope of service being provided, and to address the related privacy and security issues.

This document recognizes that there may be many different scenarios under which a custodian might engage the services of an information manager; however, the principles that underlie and inform the development of the required agreements will remain consistent, regardless of the type of service or the scope of the agreement being developed. This document is intended to provide an overview of the relevant principles of information management applicable in multiple contexts, regardless of the type of contract or agreement that is being considered.

Principles

This document provides an overview of the following principles that should, at a minimum, be considered in an agreement with an information manager under PHIA:

1. Custodianship of Information
2. Confidentiality and Privacy
3. Security and Access
4. Accuracy and Data Quality
5. Services and Functionality

1. Custodianship of Information

Importance

PHIA states that entering into an Information Management Agreement with an information manager does not relieve the custodian of its obligations under the Act. This means that, even though a custodian might, for example, engage the services of an information manager in respect of the storage of a certain set of personal health information, the custodian will be considered to be in custody of that information for legal purposes. Although the custodian remains in *legal custody and control of the information* under PHIA, it is the information manager that will have the *contractual responsibility* for the protection of the information under the Information Management Agreement.

Recommendations

The responsibilities for the protection of the information between the custodian and the information manager must be clearly defined and delineated in the Information Management Agreement. A custodian will be obligated to establish and critically assess the means by which an information manager will protect the information being disclosed to it; it is the responsibility of the information manager to ensure that all agreed-upon measures to protect the information are implemented appropriately. Due diligence will be required in selecting a service provider

2. Confidentiality and Privacy

Importance

PHIA requires that a custodian protect individuals' right to privacy by ensuring the confidentiality of the personal health information in their custody. This requirement includes taking all reasonable steps to ensure that the confidentiality of information is maintained when it is being used, stored, disclosed or otherwise dealt with by information managers.

Recommendations

An Information Management Agreement between a custodian and an information manager must adequately address the protection of the information against unauthorized access, use, disclosure, disposition, loss or modification, in accordance with requirements of PHIA. The agreement should set out all permitted uses and disclosures in order to properly limit the activities of the information manager to those that are necessary to the performance of the service that is the subject of the agreement.

3. Security and Access

Importance

PHIA requires that a custodian of personal health information take steps that are reasonable in the circumstances to ensure that:

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

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

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

Recommendations

An Information Management Agreement between a custodian and an information manager must adequately address the protection of the information against unauthorized access, use, disclosure, disposition, loss or modification, in accordance with requirements of PHIA. The main elements of information security are confidentiality, integrity and accessibility, and each of these aspects of the protection of personal health information should be addressed in an Information Management Agreement.

4. Accuracy and Data Quality

Importance

PHIA requires that a custodian take reasonable steps to ensure that information in its custody or control is as accurate, complete and as up-to-date as is necessary for the purpose for which it is being used or disclosed. In addition, prior to any disclosure of personal health information, PHIA requires that a custodian be able to clearly set out

for a recipient of information any limitations there may be on the accuracy, completeness or up-to-date character of the information.

Recommendations

An Information Management Agreement should include provisions that address the obligations of the information manager to maintain the accuracy of the personal health information that is the subject of the agreement, and to notify the custodian in a timely manner of any errors or other occurrences that might impact on the accuracy of the information.

5. Terms, Services and Functionality

Importance

PHIA states that entering into an Information Management Agreement with an information manager does not relieve the custodian of its obligations under the Act. In practice, this means that a custodian remains in *legal custody and control of the information* under PHIA, while the information manager that will have the *contractual responsibility* for the protection of the information under the Information Management Agreement. Because the legal responsibility for the personal health information continues to reside with the custodian, it is important for a custodian to have the Information Management Agreement clearly define the services and functionality being provided by the information manager.

Recommendations

In order to clearly define the services and functionality being provided by the information manager, an Information Management Agreement should define both:

(a) the nature and scope of the personal health information being dealt with by the information manager and,

(b) the nature and scope of the specific type(s) of service(s) and functionality being provided under the agreement.

Common elements addressed in an Information Management Agreement would include the following, as may be required:

1) Details of the service offering;
2) Functionality of the service;
3) Hardware requirements;
4) Software requirements;
5) Documentation;
6) Financial terms;
7) Vendor ownership;

8) Term of agreement;
9) Performance expectations;
10) Service levels;
11) Consequences of failure to meet service levels;
12) Support and maintenance obligations;
13) Reporting;
14) Termination;
15) Indemnification and limitation of liability; and
16) Representations and warranties
17) Governing law / jurisdiction

The agreement should include any assumptions that form the basis of the agreement as well as any relevant limitations of or exceptions to the service or functionality being provided by the information manager.

Appendix "B"
Sample Oath / Affirmation of Confidentiality

Introduction

The *Personal Health Information Act* requires that custodians of personal health information ensure that all employees, agents, contractors, volunteers and, where the custodian is an operator of a health care facility, those health care providers and professionals who have the right to treat persons at a health care facility operated by the custodian, sign an Oath or Affirmation of confidentiality.

****

Sample Oath / Affirmation of Confidentiality

This Oath / Affirmation of Confidentiality encompasses confidential personal health information of patients / residents / clients and staff of [*organization name*]. As a person / entity engaged by [*organization name*], it is understood that access may be granted to confidential information. Such access will be gained only through appropriate authorization and be used only for the purpose for which the access was granted. All information must be protected to ensure maintenance of full confidentiality and privacy.

I, _____, of _____, solemnly
(Print name) (City / Town, Province of residence)

Swear / Affirm [circle one] the following:

1. I have received a copy of the [*organization name*]'s Policy Manual and / or other documentation provided by the [*organization name*]. I have read and reviewed the Policy Manual and understand my role and obligations under the policies contained therein.

2. I have been informed regarding policies and procedures of the [*organization name*] as they relate to the Newfoundland and Labrador *Personal Health Information Act* and regulations and understand my role and obligations under same.

3. I understand that it is my duty to adhere to the provisions of the [*organization name*]'s policies and procedures, and agree to same.

4. I understand that it is my duty to adhere to the provisions of the Newfoundland and Labrador *Personal Health Information Act* and regulations, and agree to same.

5. I understand that all personal health information to which I have access is confidential, and is not to be discussed with or communicated to anyone who is not authorized to know the information in any manner, except as in accordance with [*organization name*]'s policies and procedures regarding same.

6. I will not access nor use personal health information except as it is necessary to perform my duties and / or as I am authorized to do so by [*organization name*].

7. I will not disclose personal health information to any unauthorized person, allow any unauthorized person to access personal or corporate information, nor discuss personal or corporate information with, or in the presence of, any unauthorized person.

8. I will immediately report any breaches of privacy and / or confidentiality to my immediate supervisor.

9. I understand that it is my responsibility to secure information to which I have access in accordance with the policies and procedures of the [*organization name*] governing the security of information.

10. I understand that if I have questions or concerns respecting access, disclosure or use of personal and corporate information, I am responsible for addressing those questions or concerns with my immediate supervisor.

11. Should I inadvertently breach any of the provisions of the [*organization name*]'s policies regarding the access, disclosure or use of personal health information, or cause a security breach which could lead to improper disclosure of information held by the [*organization name*] or improper access by others to information held by the [*organization name*], I understand that a record of this breach will be maintained by the [*organization name*] and that I may be required to undertake additional privacy and security education.

12. Should I willfully breach any of the provisions of the [*organization name*]'s policies respecting the access, disclosure or use of personal and corporate information or cause a security breach which could lead to improper disclosure of information held by the [*organization name*] or improper access by others to information held by the [*organization name*], I understand that I may face disciplinary action, up to and including termination of my employment / contract for service.

13. I understand that this Oath / Affirmation of Confidentiality survives the termination of my employment / engagement with the [*organization name*] and that I may fined and / or face civil penalties should I breach this Oath / Affirmation of Confidentiality even after my employment / engagement with the [*organization name*] has ended.

14. I understand that this Oath / Affirmation of Confidentiality will be retained as part of my personnel file.

Sworn / Affirmed at _____, this _____day of _____, 20_____, before me.

_____	_____
Signature	Witness
_____	_____
(Print name)	(Print name)

Appendix "C"
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:

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 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.

Appendix "D"
Sample Information Asset Profile

Introduction

The Newfoundland and Labrador *Personal Health Information Act* (PHIA) requires that custodians of personal health information establish and implement policies and procedures that are compliant with the Act regarding the collection, storage, transfer, copying, modification, use, disclosure and disposition of information. Additionally, the Act requires custodians to take reasonable physical, administrative and technical security measures to ensure that information in its custody is:

(a) protected against theft, loss and unauthorized access, use or disclosure;
(b) protected against unauthorized copying or modification; and
(c) retained, transferred and disposed of in a secure manner.

In order to be able to properly safeguard informational assets, a custodian must be able to maintain accurate and up-to-date records of its informational holdings. One tool that can assist with the maintenance of such records is a Information Asset Profile. The purpose of an information asset profile is to maintain on an ongoing basis a record of key information about a information assets that can be made available to authorized stakeholders. Such stakeholders might include new employees, an organization's management group or entities within government, depending on the nature and prescribed uses of the information asset.

An information asset profile is, among other purposes, intended to:

- Identify the history of the information asset – i.e., when and for what purpose the asset was commissioned / compiled;
- Identify the purpose for maintaining the information asset;
- Identify the data elements maintained in the information asset;
- Identify the legal authority for collecting the information maintained in the information asset;
- Identify any uses and / or disclosures of the information maintained in the information asset, and the legal authority for same;
- Identify any policies that bear upon the use of or access to the information asset; and,
- Assist in the production of records for persons requesting access to informational holdings that contain their personal health information.

An information asset profile should not be produced a static document, but should instead be maintained on an ongoing basis as a “living document”. An information asset profile should be reviewed on a regular, scheduled basis to ensure that the information relating to the information asset maintained in the profile is current and accurate.

When properly maintained, Information Asset Profiles will enable an organization to monitor what data it is the custodian of and to gauge at a glance the level of sensitivity of the information assets under its custodianship, which activities can and should be fed into the organization’s enterprise-level Risk Management strategy.

Sample Information Asset Profile

Name of information asset	
Date profile last reviewed	
Scheduled date of next review	
Name of information asset owner (Person or entity having accountability for the ongoing maintenance and operation of the database)	
Purpose of information asset	
History of the information asset	
Authority for the collection, use and or disclosure of the information	
Identified uses of information maintained in the information asset	
Identified disclosures of information maintained in the information asset	

Appendix "E"
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 "PHIA Risk Management Toolkit", available on the Department of Health and Community Service's website at www.gov.nl.ca/health/PHIA);
- 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*
Policy Development Manual

Appendix "F"
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 <u>all</u> 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.

Appendix "G"
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.)

Appendix "H"
Privacy Breach Incident Reporting Form

Introduction

The purpose of this privacy breach incident reporting form is to assist custodians in notifying the Office of the Information and Privacy Commissioner (OIPC) of any material breaches involving personal health information. Notifying the OIPC may enhance the public's understanding of the incident and confidence in the custodian. Furthermore, the OIPC may be able to provide advice or guidance to custodians regarding whether to notify affected individuals, as well as other issues relating to the breach.

Custodians are required under section 15(4) of the *Personal Health Information Act* (PHIA) to inform the OIPC of material breaches. A material breach includes an unauthorized collection, use or disclosure of personal health information as further defined in the Regulations. Although custodians are not required to inform the Commissioner of breaches which do not meet the definition of "material," they are welcome to do so.

Custodians should refer to the provisions relating to a privacy breach, as set out in section 15 of PHIA, as well as their corresponding policies and procedures in order to take the correct steps following the occurrence of a breach.

To report a privacy breach to the Commissioner, please fill out this form and send a printed copy to the OIPC at the address below. Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer. Should you need further assistance in completing this form, or if you have any other questions, please contact the OIPC.

Forward to:

Office of the Information and Privacy Commissioner
2nd Floor, 34 Pippy Place
P.O. Box 13004, Station "A"
St. John's, NL A1B 3V8

(709) 729-6309 (t)
(709) 729-6500 (f)

PHIA Privacy Breach Incident Report Form

Background Information:

Name of custodian	
Contact information (contact name, telephone number, facsimile, email and mailing address)	

Details of Incident:

Date breach occurred	
Date breach discovered	
Location of breach	
Description of incident	
Estimated number of individuals affected	
Description of action taken to contain breach	
Was the affected party(s) notified of the incident? If so, what was the date of notification?	
Was the affected party(s) notified of his/her right to complain to the OIPC?	
Was anyone else notified of the incident (i.e. professional bodies, law enforcement, etc.)? If so, who and when were they notified?	

_____ _____

Signature of Custodian or Representative Date