The *Personal Health Information Act*
Frequently Asked Questions

Version	1.1
Date:	February, 2011

WARNING AND DISCLAIMER

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

- The materials provided are for general information purposes only. They should be adapted to the circumstances of each custodian using the materials.

- These materials reflect interpretations and practices regarded as valid when it was published based on information available at that time.

- These materials are not intended, and should not be construed, as legal or professional advice or opinion.

- Custodians concerned about the applicability of privacy legislation to their activities are advised to seek legal or professional advice based on their particular circumstances.

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

ACKNOWLEDGEMENT

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

Table of Contents

Introduction

What is the *Personal Health Information Act* (*PHIA*)?

The *Personal Health Information Act* (*PHIA*) is Newfoundland and Labrador's new health-sector specific privacy legislation. *PHIA* governs the manner in which personal health information may be collected, used and disclosed within the health care system.

PHIA creates a consistent approach to protecting personal health information across the health care system, in both the public and the private sectors. By providing a level playing field for all health care professionals, *PHIA* builds upon many of the existing high standards and protections represented in the common law, various professional codes, policies and guidelines.

The rules set out under *PHIA* were designed to give individuals greater control over how their personal health information is collected, used or disclosed. They provide health care professionals with a flexible framework to access and use health information as necessary in order to deliver adequate and timely health care.

In addition, *PHIA* confirms a patient's existing right to access one's own personal health information and allows individuals to file a complaint with the Newfoundland and Labrador Office of the Information and Privacy Commissioner when concerns arise relating to their personal health information.

The Newfoundland and Labrador Department of Health and Community Services prepared the following questions and answers to provide general guidance to Newfoundlanders and Labradorians and health care professionals in understanding their respective privacy rights and obligations.

Overview

What is the purpose of *PHIA*?

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 compliance with this Act by persons having the custody or control of personal health information.

When did *PHIA* come into force?

PHIA is anticipated to come into force in April, 2011. As of the date of proclamation, all health information custodians must comply with the Act.

Is *PHIA* retroactive?

No. *PHIA* applies to the collection, use and disclosure of personal health information by health information custodians as of April, 2011. There is no obligation for custodians to seek consent for personal health information that was collected prior to this date. However, a health information custodian must obtain consent for the use or disclosure of that information after April, 2011.

Why do we need a health privacy law in Newfoundland and Labrador?

Personal health information is among the most sensitive of personal information there can be about a person, and people have rights regarding sharing personal details relating to their medical conditions. At the same time, personal health information must flow freely between health care professionals under appropriate circumstances in order to ensure the best treatment for patients.

The nature of our health care system is that health information passes through many links in the health care chain: from a doctor's office, to a referral to a specialist, to a medical lab, to a hospital or to an insurance company for reimbursement of claims. There are also circumstances in which personal health information must be readily shared, such as in the case of a medical emergency. Beyond patient care, personal health information is needed for important activities such as health research vital to the development of new treatments and cures. The increasing use of technology to transfer and store medical data instantaneously has also increased the need for legislated rules to assure Newfoundlanders and Labradorians that their personal health information will be protected.

What is the relationship between *PHIA* and the federal *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)?

The collection, use and disclosure of personal information in the commercial sector is regulated by federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). *PIPEDA* was created to regulate the collection, use or disclosure of personal information in the hands of private sector organizations. As of January 1, 2004, *PIPEDA* has applied to all private sector organizations in Newfoundland and Labrador, including pharmacies and health care providers with operating practices that qualify as "commercial activities." *PIPEDA* does not apply to personal information in provinces and territories that have "substantially similar" privacy legislation in place.

The application of *PIPEDA* to personal health information has raised a number of concerns. The requirements under *PIPEDA* were designed to regulate marketing, electronic commerce and other activities and do not specifically address the unique characteristics of personal health information. The federal government is expected to deem the provisions of Newfoundland and Labrador's *PHIA* to be substantially similar to *PIPEDA* in order to exempt health care providers that are covered under *PHIA* from also having to comply with the provisions of *PIPEDA*.

Application and Scope of *PHIA*

To whom does *PHIA* apply?

PHIA applies to a wide variety of individuals and organizations defined as health information custodians. *PHIA* also applies to agents who are authorized to act for or on behalf of a custodian of personal health information.

What is a personal health information custodian?

A personal health information custodian is a listed individual or organization under *PHIA* that, as a result of his or its power or duties, has custody or control of personal health information.

Examples of health information custodians include:

• Independent health care practitioners, (including doctors, nurses, audiologists and speech-language pathologists, chiropractors, chiropodists, dental professionals, dieticians, medical radiation technologists, medical laboratory technologists, massage therapists, midwives, optometrists, occupational therapists, opticians, pharmacists, physiotherapists, psychologists and respiratory therapists);

• Regional Health Authorities (Eastern Health, Western Health, Central Health and Labrador-Grenfell Health);

• Nursing homes;

• Ambulance services;

• The Department of Health and Community Services, and other departments of government when they are engaged in activities related to the delivery of health care.

What is the 'circle of care?'

The "circle of care" is a defined term under *PHIA*. It means certain personal health information custodians and their authorized agents who are permitted to rely on an individual's implied consent when collecting, using, disclosing or handling personal health information for the purpose of providing direct health care.

For example:

• In a physician's office, the circle of care includes: the physician, the nurse, a specialist or other health care provider referred by the physician and any other health care professional selected by the patient, such as a pharmacist or physiotherapist;

• In a hospital, the circle of care includes: the attending physician and the health care team (e.g., residents, nurses, technicians, clinical clerks and employees

assigned to the patient) who have direct responsibilities of providing care to the individual.

The circle of care does not include:

• A physician or nurse who is not part of the direct or follow-up treatment of an individual.

What is personal health information?

Personal health information is "identifying information" collected about an individual in oral or recorded form. It includes information about an individual's health or health care history in relation to:

• The individual's physical or mental condition, including family medical history;

• The provision of health care to the individual;

• Long-term health care services;

• The individual's health card number;

• Blood or body-part donations;

• Payment or eligibility for health care;

• Drugs, 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; and

• The identity of a health care provider or a substitute decision-maker for the individual.

"Identifying information" includes health information that could identify an individual when used alone or in conjunction with other information. Personal health information does not include identifying information about an employee or agent of the custodian that is not maintained for the provision of health care. For example, a doctor's note to support an absence from work in the personnel file of a receptionist employed by a health information custodian is not considered personal health information. It is not being kept to provide health care; it is being kept for administrative purposes to verify a work absence. As such, it is not considered personal health information for the purpose of the Act.

What does 'health care' mean?

"Health care" means any observation, examination, assessment, care, service or procedure provided for a health-related purpose and that is carried out or provided:

• For diagnosis, treatment or maintenance of an individual's physical or mental condition;

• For prevention of disease or injury or the promotion of health;

• For rehabilitation; or

• As part of palliative care.

It also includes:

• The compounding, dispensing, or selling of a drug, device or equipment pursuant to a prescription.

Rights and Responsibilities

How does *PHIA* protect personal health information?

The ability of an individual to control how his or her own personal health information is collected, used and disclosed is key to their privacy rights. *PHIA* gives patients control over their own personal health information by requiring health information custodians to obtain consent for the collection, use or disclosure of personal health information, with limited exceptions.

PHIA establishes certain privacy rights for individuals and creates specific obligations on health information custodians regarding the protection of personal health information.

What rights do individuals have?

Individuals can expect to be informed about how their personal health information will be collected, used and disclosed by health information custodians. Individuals can also expect the administrative, technical and physical safeguards relating to their personal health information to continue to be in place.

PHIA gives individuals the right to:

- Understand the purposes for the collection, use and disclosure of personal health information;

- Refuse or give consent to the collection, use or disclosure of personal health information, except in circumstances specified in *PHIA*;

- Withdraw consent by providing notice to the health information custodian, except in circumstances specified in *PHIA*;

- Request access to one's own personal health information;

- Request corrections to be made to one's own personal health information; and,

- Contact the Privacy Commissioner with concerns they might have; and

PHIA establishes a formal process for individuals to access and correct their own personal health information within specified time frames and the right to raise their concerns with the Privacy Commissioner if an access or correction request is denied.

What responsibilities do health information custodians have?

PHIA requires health information custodians who have custody or control of personal health information to establish and implement information practices that comply with the Act. This does not mean that custodians are expected to completely set aside

their existing policies and practices. In fact, *PHIA* builds upon existing policies and guidelines for health care professionals and provides enforceable rules relating to the collection, use or disclosure of personal health information.

PHIA will require health information custodians to:

• Obtain an individual's consent when collecting, using and disclosing personal health information, except in limited circumstances as specified under *PHIA*;

• Collect personal health information appropriately (by lawful means and for lawful purposes), and no more than is reasonably necessary to accomplish the purpose for the collection;

• Take reasonable precautions to safeguard personal health information, including:

- Protection against theft or loss;
- Protection against unauthorized use, disclosure, copying, modification or destruction; and,
- Notification to an individual at the first reasonable opportunity if the information is stolen, lost or accessed by an unauthorized person.

• Ensure health records are as accurate, up-to-date and complete as necessary for the purposes which they use or disclose personal health information;

• Ensure health records are stored, transferred and disposed of in a secure manner;

• Designate or take on the role of a contact person who is responsible for:
- Responding to access/correction requests;
- Responding to inquiries about the custodian's information practices;
- Receiving complaints regarding any alleged breaches of *PHIA*; and
- Ensuring overall compliance with *PHIA*.

• Provide a written statement that is readily available to the public and describes:
- A custodian's information practices;
- How to reach the contact person; and
- How an individual may obtain access, request a correction or make a complaint regarding his/her personal health information.

• Inform an individual of any uses and disclosures of personal health information without the individual's consent that occurred outside the custodian's information practices; and

• Ensure that all parties acting under the authority of the custodian are appropriately informed of their duties under *PHIA*.

Consent Requirements

What is consent under *PHIA*?

The general rule is that a health information custodian needs to obtain an individual's consent to collect, use and disclose personal health information unless *PHIA* allows the collection, use or disclosure without consent. An individual's consent may be express or implied.

What is the difference between express and implied consent?

Where consent is required under *PHIA*, consent may be either *express* or *implied*.

Express consent provided by an individual for the collection, use or disclosure of personal health information is consent that is explicit, clear and direct. It may be given verbally, in writing or by electronic means, depending on the policies of the entity collecting the consent.

Implied consent permits a health care custodian to assume from the surrounding circumstances that an individual would reasonably agree to the collection, use or disclosure of his or her personal health information.

For example, when an individual discloses his or her personal health information for the purposes of filling out a prescription, a pharmacist can reasonably assume that the individual has consented to the collection of that information.

What are the requirements for consent?

Under *PHIA*, consent is considered to be valid if it is:

- Knowledgeable;
- Voluntary (not obtained through deception or coercion);
- Related to the information in question; and
- Given by the individual.

Knowledgeable consent means that an individual must know why a health information custodian collects, uses or discloses his or her personal health information and that he or she may withhold or withdraw this consent.

Administratively, a health information custodian may ensure that consent is knowledgeable by posting a conspicuous notice or distributing brochures that are readily available to the public describing the purposes for the collection, use and disclosure of personal health information.

When is implied consent sufficient?

In practice, a health information custodian is not required to obtain an individual's written or verbal consent every time personal health information is collected, used or disclosed.

PHIA permits a custodian to assume implied consent where information is exchanged between custodians within the circle of care for the purpose of providing direct health care, unless a custodian is aware that an individual has expressly withheld or withdrawn his or her consent.

Consent may never be implied for an individual who specifies that his or her personal health information may not be collected, used or disclosed.

When is express consent required?

Subject to very limited exceptions, express consent is required:

• Where personal health information is disclosed to an individual or organization, such as an insurance company, that is not a custodian of personal health information.

• Where information is disclosed by one custodian to another for a purpose other than providing or assisting in providing health care.

• Express consent is also required where a custodian:

- Collects, uses or discloses personal health information for fundraising purposes;
- Collects personal information for marketing research or activities; and
- Collects, uses or discloses personal information for research purposes, unless certain conditions and restrictions are met.

Can an individual withdraw his or her consent?

Yes. An individual may withdraw his or her consent at any time for the collection, use, or disclosure of his or her personal health information by providing notice to the health information custodian. This applies to implied as well as express consent.

A withdrawal of consent is not retroactive. This means that where a disclosure has been made on the basis of consent, the custodian is not required to retrieve information that has already been disclosed.

Can an individual control what personal health information is recorded in his or her file?

Yes, but any condition placed on the collection, use or disclosure of personal health information cannot prohibit the recording of personal health information that is required by law, professional or institutional practice.

What is "limited consent"?

"Limited consent" is a term used to describe the right of an individual to instruct a health information custodian not to disclose specified personal health information to another custodian for the purpose of providing health care.

An individual can provide a limited consent directive regarding his or her personal health information by expressly withholding or withdrawing consent for his or her health information to be collected, used or disclosed.

How does the "limited consent" work?

When an individual requests a health information custodian not to use or disclose his or her personal health information to another custodian, the custodian is obliged to inform the recipient custodian that some personal health information is inaccessible as a result of it having been "locked" by the individual. A custodian must inform the recipient custodian if the custodian considers some of the locked information to be reasonably necessary for the provision of health care.

If an individual locks only a part of their personal health information, the custodian who receives information that has not been locked may choose to discuss the matter of the locked information with the individual. The custodian would need to obtain the express consent of that individual to access and use that locked information

A custodian is permitted to disclose locked information in certain circumstances, including to a recipient custodian where, in his or her professional opinion, the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to an individual or to a group of persons.

Further, an individual's restriction may not prevent a custodian from recording personal health information about an individual that is required by law, professional or institutional practice.

What happens when an individual is incapable of providing consent?

PHIA generally presumes that individuals are capable of making their own decisions regarding the collection, use or disclosure of their personal health information if they are able to understand and appreciate the consequences of providing, withholding or withdrawing their consent.

If a custodian of personal health information believes that an individual is incapable of providing consent, *PHIA* permits a substitute decision-maker (such as a relative, spouse, child's parent, or an appointed guardian) to make a decision on an individual's behalf.

Can another person, such as a family member, provide consent on an individual's behalf when picking up or dropping off a prescription?

Yes. *PHIA* allows a pharmacist to provide prescription information to another person. An individual will have to provide express instructions to a pharmacist permitting the pharmacist to disclose information to another person before the pharmacist will be permitted to do so.

Collection, Use and Disclosure of Personal Health Information

Collection

What is a collection of personal health information under *PHIA*?

PHIA defines the term "collect" as the gathering, acquiring, receiving or obtaining of personal health information. This means that personal health information can be collected by a health information custodian under *PHIA* in several ways, such as when a doctor makes notes about a patient in his or her medical file or when a pharmacist fills a prescription and enters an individual's information into his or her computer system.

What are the rules regarding the collection of personal health information?

Custodians of personal health information within the circle of care may rely on an individual's implied consent to collect personal health information for the purpose of providing health care.

With limited exceptions, custodians of personal health information must collect personal health information directly from the individual involved and may only collect as much information as is necessary to meet the purpose of the collection.

Custodians must take reasonable steps to inform the public about their information practices and how individuals may exercise their rights under *PHIA*. Some suggested methods of meeting this requirement include the use of visible brochures, posters, notices posted on walls and verbal explanations.

What are the exceptions to the rules for collecting personal health information?

PHIA provides for the collection of personal health information directly from individuals. Custodians of personal health information may collect personal health information indirectly where, for example:

- The individual consents;

- The collection is necessary for providing health care and it is not possible to obtain the information directly from the individual in a timely manner;

- The custodian collects personal health information for the purposes of research from a person who is not a health information custodian, provided that certain conditions are met;

- The indirect collection is required or permitted by law; or

- The indirect collection is required for the purpose of health planning or management.

Use

What is a use of personal health information under *PHIA*?

"Use" of personal health information under *PHIA* is defined as the handling or dealing with personal health information that is in the custody or control of a health information custodian. Use includes accessing or reproducing health information as required by the custodian, but does not include a disclosure of the information.

What are the rules regarding the use of personal health information?

As a general rule, consent is required for any use of an individual's personal health information unless *PHIA* allows the use without consent. A custodian of health information may rely on an individual's implied consent to share personal health information, as long as the sharing is related to the provision of health care and the individual has not expressly stated otherwise.

When using personal health information, a custodian must exercise the highest level of care and must take reasonable steps to ensure that the individual's personal health information is as accurate, complete and up-to-date for the purpose which the custodian uses the information.

Where a custodian of health information is authorized to use the information, the custodian may provide the information to an employee or other agent of the custodian to use it for that purpose on behalf of the custodian. The sharing of information between a custodian and its agents is considered to be a use and *not* a disclosure for the purposes of *PHIA*.

What are the exceptions to the rules regarding the use of personal health information?

PHIA sets out a limited set of acceptable uses of personal health information without consent, including for the following purposes:

- Risk management, error management, or activities to improve or maintain the quality of care or any related program or service;

- The planning or delivering of programs or services;

- The allocation of resources to any program or service provided or funded by the custodian;

- Obtaining payment or processing, monitoring, verifying or reimbursing health care claims; and

• For research, provided that specific requirements and conditions are met.

Disclosure

What is a disclosure of personal health information under *PHIA*?

The term "disclose" under *PHIA* means to release or make available personal health information that is under the control or custody of a health information custodian, or its employee or agent, to another custodian, individual or organization. It does not include providing the same information back to a person who provided it as long as it does not include additional identifying information.

What are the rules regarding the disclosure of personal health information?

As a general rule, consent is required to disclose an individual's personal health information unless *PHIA* allows the disclosure without consent.

A custodian of health information and its employees and agents may rely on implied consent for the disclosure of personal health information within the circle of care while providing health care so long as the disclosure is reasonably necessary for the provision of health care and the individual has not expressly stated otherwise.

Although *PHIA* permits custodians to disclose personal health information in certain limited situations, disclosure is not required, unless it is necessary to carry out a statutory or legal duty.

Express consent will always be required when personal health information is disclosed by a custodian to a non-custodian; where a custodian discloses to another custodian for a purpose other than for health care; or for marketing, research (unless specific conditions are met); and for fundraising.

When disclosing personal health information, the custodian should take care to ensure that no information is inadvertently disclosed to third parties.

What are the exceptions to the rules regarding the disclosure of personal health information?

PHIA recognizes the need for a flexible approach to regulating information exchanges between custodian of health information in order to ensure the effective and efficient operation of the health system. As such, custodians may disclose personal health information without an individual's consent in certain circumstances, including the following:

• If the disclosure is reasonably necessary for providing health care and the consent cannot be obtained in a timely manner, unless there is an express request from the individual instructing otherwise;

• In order for the government to provide funding or payment to the custodian for the provision of health care services;

• For the purpose of contacting a relative or friend of an individual who is injured, incapacitated, ill or unable to give consent personally;

• To confirm to a member of a family or to a person with a close relationship with an individual that the individual is a patient or resident in a facility or to confirm the status of his or her health condition, unless there is an express request from the individual instructing otherwise (custodian must offer the individual the option, at the first reasonable opportunity after admission to the facility, to object to this disclosure);

• To identify an individual who is deceased or in order to allow a spouse, partner or relative of a deceased person to make decisions about his or her own care or the care of children or to inform estate trustees of an individual's death;

• To eliminate or reduce a significant risk of serious bodily harm to any person or to the public;

• When transferring records to a custodian's successor or to the archives for conservation;

• For the purpose of carrying out an inspection, investigation or similar procedure that is authorized by a warrant, *PHIA* or another Act, such as the *Child, Youth and Family Services Act*;

• For determining or verifying eligibility for publicly-funded health care or related benefits;

• For the purpose of administration and enforcement of various Acts by the professional Colleges and other regulatory bodies;

• To a prescribed registry listed in the regulations under *PHIA* that compiles and maintains a registry of personal health information for the purpose of improving the provision of health care or that relates to the storage or donation of body parts or bodily substances,

• For the purpose of legal proceedings if the information is, or relates to, a matter at issue;

• For the purpose of research, subject to restrictions and conditions; and

• For any purpose as required or permitted by law.

Research

What are the requirements for the collection, use and disclosure of personal health information for health care research?

In recognizing the importance of health research, *PHIA* permits the use or disclosure of personal health information for research purposes without an individual's consent if strict conditions are met.

For example, a custodian who uses personal health information for research and, similarly, a researcher who seeks disclosure of personal health information for research, must both submit an application to a Research Ethics Board (REB) for approval. In reviewing a research proposal involving the use and disclosure of personal health records, an REB will consider things like:

- Whether the research cannot be reasonably accomplished without access to the information;

- The public interest in conducting the research and in protecting privacy;

- Whether obtaining consent directly is impracticable; and

- Whether adequate safeguards are in place to protect the privacy of individuals and the confidentiality of their information.

A researcher requesting disclosure of personal health information from a custodian must submit to the custodian an application and a copy of the decision approving the application by the REB. A custodian may enter into an agreement with the researcher that may impose further restrictions on the manner in which the researcher may use and disclose the information.

A researcher with an approved application who receives personal health information from a custodian shall:

- Comply with the conditions imposed by the REB, if any;

- Use personal health information only for the purpose set out in the application;

- Not publish information in a form that could identify the individual;

- Not disclose information unless required by law to do so;

- Not attempt to contact the individual whose personal information is the subject of the research project unless the custodian obtains the consent of that individual; and

- Notify the custodian in writing of any breaches of either the agreement or *PHIA*.

Access to Personal Health Information

Are individuals permitted to access their own personal health information?

With limited exceptions, *PHIA* provides individuals with a general right to access their own personal health information held by a custodian of personal health information, and sets out a formal procedure for access requests.

How does an individual obtain access to his/her personal health information?

An individual may request access to his or her own personal health information by submitting a written request to the health information custodian who has custody or control of the individual's health records. An individual may also request his or her personal health information orally. Whether the access request is made orally or in writing, the request must contain sufficient detail to allow the custodian to locate the record in question.

The health information custodian should then either provide access to or a copy of the record. Otherwise, a written notice explaining why the record is not available must be provided to the individual seeking access.

Where the individual has not provided sufficient detail to enable the custodian to identify and locate the record, the custodian is required to assist the individual in re-stating the request.

How long does a health information custodian have to respond to an individual's request for access to personal health information?

A health information custodian must respond without delay, and no later than 60 days after the request was made.

Extensions beyond this 60-day time frame are allowed where meeting this time frame would interfere with the custodian's operations, or where the requested information consists of numerous records or where locating the information will take longer than 60 days. In such situations, the custodian must inform the individual in writing about the delay and the reasons for the delay.

Can a health information custodian refuse to provide access to an individual's personal health information?

Generally, health information custodians are responsible for assisting individuals by providing access to their health records. Custodians may only refuse access in limited situations, including:

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

• Its disclosure could reasonably be expected to result in a risk of serious bodily harm to a person;

• The information was collected as part of an investigation; or

• Another law prohibits the disclosure of that information.

If any exception applies, *PHIA* permits custodians to remove some of the information to allow partial access to the individual. If a health information custodian denies an individual access to his or her personal health information, the individual has the right to file a complaint with the Privacy Commissioner.

Is there a fee associated with an access request?

Custodians of personal health information may charge a reasonable fee for providing access to an individual's personal health records. *PHIA* also permits a custodian to waive all or part of the fee associated with an access request.

What if the health information custodian works for a non-health information custodian that is covered under public sector access and privacy legislation, such as a school board or municipality?

In that case, the individual would submit an access request under the *Access to Information and Protection of Privacy Act* (*ATIPPA*), which covers public bodies in the province, including departments of provincial government (that are not custodians under *PHIA*), and most provincial boards, agencies and commissions). The access request should be submitted in accordance with the provisions of *ATIPPA*, and will be addressed in accordance with the provisions of *ATIPPA*.

Corrections to Personal Health Information

Can an individual correct errors in his or her personal health information?

An individual who believes that his or her personal health information is incomplete or inaccurate may request that a health information custodian correct his or her record. It is the responsibility of the custodian to ensure that personal health information is complete and accurate.

How does an individual correct errors?

An individual seeking a correction to his or her personal health information is required to submit a written request to the health information custodian who has custody or control of the records. A health information custodian must respond without delay, and no later than 30 days after the request was made.

Extensions beyond this 30-day time frame are allowed where meeting this time frame would interfere with the custodian's operations, or where the requested information consists of numerous records or where locating the information will take longer than 30 days. In such situations, the custodian must inform the individual in writing about the delay and the reasons for the delay.

Can a health information custodian refuse to correct an individual's personal health information?

A health information custodian is obligated to correct personal health information where an individual demonstrates, to the satisfaction of the custodian, that the record is in fact inaccurate or incomplete and the individual gives the custodian the necessary information to correct the record. However, a custodian may refuse to correct personal health information that was not created by the custodian or that is a professional opinion or an observation of a health care provider. A custodian may also refuse to make a correction where the custodian believes that the individual's request is frivolous or vexatious.

If a correction is refused on such a basis, the custodian is required to inform the individual of the refusal, the reasons for the refusal, the individual's right to file a complaint regarding the refusal to the Privacy Commissioner.

Administration and Enforcement

How will *PHIA* be enforced?

The Privacy Commissioner has been designated as the independent oversight body responsible for ensuring that custodians of personal health information collect, use and disclose personal health information according to the rules set out under *PHIA*.

The Privacy Commissioner has various powers under *PHIA*, including the authority to investigate and to make recommendations regarding compliance with *PHIA*. For example, the Privacy Commissioner may make a recommendation for a custodian to:

- Provide the individual with access to a record of personal health information;
- Correct a record of personal health information;
- Dispose of records of personal health information; and / or
- Change or cease a particular information practice.

How does an individual initiate a complaint?

An individual who feels that his or her privacy rights under *PHIA* have been violated has the right to submit a written complaint to the Privacy Commissioner. For example, an individual may complain about:

- A health information custodian's information practices;
- A refusal to grant access to his or her personal health information; or
- A refusal to correct his or her personal health information.

Is there a time limit within which an individual may complain?

In general, an individual must file a complaint with the Privacy Commissioner regarding a request for access or correction within 60 days from when the individual received a response regarding the request for access or request from the custodian.

Where an individual believes on reasonable grounds that a custodian has contravened a provision of *PHIA*, he or she must file a complaint with the Privacy Commissioner regarding that possible contravention within one year from when the individual became aware of the problem. The legislation provides the Privacy Commissioner with the discretion to extend this one-year limitation period under certain circumstances.

What is an offence under *PHIA*?

Offences under *PHIA* include:

- Collecting, using or disclosing personal health information in contravention of *PHIA*;

- Obtaining or attempting to obtain health information under false pretenses;

• Knowingly disposing of health records to avoid providing access;

• Obstructing the Privacy Commissioner or delegates in the performance of oversight functions; or,

• Disciplining or harassing an individual who has alerted the Privacy Commissioner of an alleged contravention.

What are the consequences for committing an offence under *PHIA*?

A person found guilty of committing an offence under *PHIA* can be liable for a fine of up to $10,000, or to a sentence of up to 6 months in prison.

In addition, health information custodians who are convicted of an offence under *PHIA* may be subject to a civil suit for damages. Generally, health information custodians who have acted reasonably and in good faith will be protected from liability under *PHIA*.

Custodians' obligations

Security

What security requirements are there in PHIA?

All custodians must ensure that that the personal health information in their custody or control is kept secure. Custodians are required to take steps that area reasonable in the circumstances to ensure that:

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

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

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

What is security and what kinds of measures to I need to put in place?

All custodians are under an obligation to identify and implement reasonable 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, manage the information with due diligence and take appropriate measures to safeguard it from loss or abuse.

"Security" is simply the process by which the confidentiality, integrity, and availability of information are safeguarded and ensured. No one security 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 guideline and educational documents; and,
- **Technological** security controls, such as passwords, firewalls and encryption, where appropriate and applicable.

Where can I get additional information about information security?

The *PHIA* policy development manual contains further information about information security under *PHIA*. Please refer to Appendix "C" ("Information Security Management Overview") of the *PHIA* policy development manual.

The *PHIA* policy development manual can be found on the Department of Health and Community Services' *PHIA* resource website at:

www.gov.nl.ca/health/PHIA

Privacy policies

Who needs to have privacy policies and procedures?

All custodians that have custody or control of personal health information must have policies and procedures to facilitate the implementation of *PHIA*. A custodian's policies and procedures must address the manner of collection, storage, transfer, copying, modification, use and disposition of personal information in a custodian's custody or control whether within or outside the province.

My organization only employs a few people – do I still require privacy policies and procedures?

Yes. All custodians of personal health information must have policies and procedures in place in accordance with section 13 of the Act.

What privacy policies and procedures do I need to put in place?

The information policies that a custodian is required to have in place must, at a minimum, include policies and procedures that:

> (a) protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information;
>
> (b) restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the information was collected or will be used;
>
> (c) protect the confidentiality of personal health information that will be stored or used in a jurisdiction outside the province or that is to be disclosed by the custodian to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and

(d) provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information.

A custodian's information policies and procedures must include appropriate measures to address the risks associated with the storage of personal health information, taking into account the manner and form in which the personal health information is recorded, the location of storage and the degree of sensitivity of the personal health information to be protected.

Where can I get help preparing privacy policies and procedures? Are there templates or examples?

The Department of Health and Community Services has produced a *PHIA* policy development manual, which is available to all custodians of personal health information, and to any interested stakeholder via the Department's website.

The *PHIA* policy development manual 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 PHIA policy development manual provides custodians with sample language for policies and for procedures: the sample policy language provided reflects custodians' obligations under *PHIA*; 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.

It should be kept in mind that while custodians may customize the sample language provided in the *PHIA* policy development manual, custodians should be careful to ensure that whatever policies or procedures they develop are legally compliant with the requirements of the *Personal Health Information Act*. The *PHIA* policy development 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 as they adapt the materials in the PHIA policy development manual for their purposes.

The *PHIA* policy development manual can be found on the Department of Health and Community Services' *PHIA* resource website at:

www.gov.nl.ca/health/PHIA

What wording should I use in my policies and procedures?

Generally, custodians should refer to and adopt the language that appears in the Act itself. As an example, in describing the flow of personal health information into, within and outside of its organization, a custodian should use the terms "collection", "use" and "disclosure". These are terms that are defined in *PHIA* and, as such, have a commonly-understood meaning.

Who can review the privacy policies I create?

It is the responsibility of the custodian to create and implement policies and procedures as required under *PHIA*. Custodians should consult with their regulatory bodies (i.e., the Newfoundland and Labrador College of Physicians and Surgeons; the Association of Registered Nurses of Newfoundland and Labrador, etc.) and / or their legal counsel for further information.

What is the difference between a policy and a procedure?

A policy is "what" a custodian and its employees, agents, etc. have to do. A policy is a formal statement adopted by an entity that sets out the details of a duty or an activity that has either been adopted by the entity itself, or has been imposed on the entity by some external agent or factor.

A procedure is "how" a custodian and its employees, agents, etc., do what they are obligated by policy to do. In other words, a procedure is an operational process required to implement a policy.

As an example, a custodian could have a policy that stated that consent has to be obtained before making a particular disclosure of personal health information. The custodian could then specify that a specific type of form will have to be used to collect that consent in writing. Specifying the form to use (the procedure) supports the implementation of the requirement to collect consent (the policy).

I already have privacy policies and procedures. Do I need to change them?

If a custodian already has privacy policies and procedures in place, they should be reviewed to make sure they address all of the requirements of *PHIA*.

How can I make my staff aware of my privacy policies and procedures?

Under *PHIA*, custodians have an obligation to ensure that their employees, agents, contractors and volunteers, and those health care professionals who have the right to treat persons at a health care facility operated by the custodian comply with the provisions of *PHIA* as well as the custodian's policies and procedures. To meet this requirement, custodians should develop training strategies and materials appropriate for their circumstances that will enable them to effectively teach people working under their authority about their privacy obligations.

Do I have to file copies of my privacy policies and procedures with someone?

No, there is currently no requirement under *PHIA* for custodians to submit copies of their privacy policies to any entity for review or approval. *PHIA* requires that custodians who have custody or control of personal health information have policies and procedures in place to ensure compliance with *PHIA*. This means that custodians must exercise due diligence in establishing their policies and procedures in order to comply with the Act.

Privacy Training

Who needs to have a privacy training program?

PHIA does not specifically require custodians to have a privacy training program. However, *PHIA* does require that all custodians of personal health information ensure that their employees, agents, contractors and volunteers, and those health care professionals who have the right to treat persons at a health care facility that they operate comply with *PHIA*, its regulations and with the custodian's information policies and procedures. One way that a custodian can meet this requirement is to implement a program of privacy and training.

My organization only employs a few people – should I still provide privacy training?

Regardless of the size of the organization or the number of employees, a custodian must ensure that their employees, agents, contractors and volunteers, and those health care professionals who have the right to treat persons at a health care facility that they operate comply with *PHIA* and with the custodian's information policies and procedures. One way that a custodian can meet this requirement is to implement a program of privacy training.

Where can I get help preparing a privacy training program? Are there templates or examples?

Educational materials relating to *PHIA* have been prepared by the Government of Newfoundland and Labrador, and are available for anyone to use. These materials include a *PHIA* Online Training Program and a *PHIA* Facilitated Education Program, which includes train-the-trainer materials. Custodians may use these materials as a starting point for developing a privacy training program specific to their organization. The *PHIA* educational materials can be found on the Department of Health and Community Services' *PHIA* resource website at:

www.gov.nl.ca/health/PHIA

I already have a privacy training program. Do I need to change it?

Custodians should review any existing training materials to ensure that they accurately reflect the requirements set out in *PHIA* and regulations.

When should I conduct privacy training?

It is a best practice that custodians ensure that all employees, agents, contractors and volunteers, and those health care professionals who have the right to treat persons at a health care facility that they operate are made aware of their obligations under *PHIA* and with the custodian's information policies and procedures early in their engagement with the custodian. Employees should receive privacy training as

early as possible after being hired. Contractors and other service providers should be made aware of their obligations under *PHIA* and with the custodian's information policies and procedures prior to signing a contract of service.

Notice of Purposes and Record of Disclosure

Notice of Purposes

As a custodian of personal health information do I need to post a notice of purposes for collecting, using or disclosing personal health information?

Whenever a custodian collects personal health information, *PHIA* requires the custodian to take reasonable steps to inform the subject of the information of the purposes for the collection, use and disclosure of the information and of the identity of and other relevant information relating to the contact person, if the custodian has one. One way that a custodian can meet this requirement is to post a notice that sets out the purposes for collection, use or disclosure where it is likely to come to the individual's attention.

Who needs to provide a notice of purposes for collecting, using or disclosing personal health information?

All custodians that collect personal health information must take reasonable steps to inform individuals of the purposes for which their information is being collected, use and disclosed. This can be accomplished by posting a notice setting out the permissible purposes for collection, use or disclosure where it is likely to come to the individual's attention.

My organization only employs a few people – do I still need to prepare a notice of purposes?

Regardless of the size of the organization or the number of employees, a custodian must always take reasonable steps to inform the subject of the information of the purposes for the collection, use and disclosure of the information. One way that a custodian can satisfy this requirement is to post a notice setting out the permissible purpose for collection, use or disclosure where it is likely to come to affected individuals' attention.

How detailed does the notice of purposes need to be?

A custodian's notice of purposes does not need to be detailed – it can be a general statement about the reasonably foreseeable purposes for collection, use or disclosure of a person's personal health information.

How should I provide this notice of purpose? On the web? In a brochure? As a poster? Verbally?

Whenever a custodian collects personal health information, *PHIA* requires the custodian to take reasonable steps to inform the subject of the information of the purpose for the collection, use and disclosure of the information and of the identity of and other relevant information relating to the contact person, if the custodian has

one. One way that a custodian can satisfy this requirement is to post a notice setting out the permissible purposes for collection, use or disclosure where it is likely to come to the individual's attention. Custodians may also notify individuals of the purpose for the collection, use and disclosure of the information orally on a case-by–case basis, or by providing a copy of the notice of purposes to the individual in brochure form.

If a custodian chooses to rely on a posted notice of purpose, the notice should be placed in high traffic areas (e.g. a waiting room) where it is likely to come to the individuals' attention. Organizations should be aware of any specific needs of their clientele and provide the notice of purposes in alternate forms such as Braille, video, and translation into other languages if required.

I already provide a notice of purposes. Do I need to change it?

Custodians should review any existing notice materials to ensure that they accurately reflect all of the reasonably foreseeable purposes for collection, use or disclosure. Custodians should also ensure that all other requirements for public notices have been addressed, including identifying the organization's contact person (where applicable) and any other requirements that might be set out in regulations under *PHIA*.

Where can I get help preparing a notice of purposes? Are there templates or examples?

Sample notice materials have been prepared by the Government of Newfoundland and Labrador, and are available for anyone to use. Custodians may use these materials as a starting point for developing a notice of purposes specific to their organization. The sample notice materials can be found on the Department of Health and Community Services' *PHIA* resource website at:

www.gov.nl.ca/health/PHIA

When do I have to provide the notice of purposes?

Custodians need provide individuals with a notice of purposes at or before the time of collection of personal health information.

Does someone have to approve my notice of purposes?

No. *PHIA* does not require that anyone approve a custodian's notice of purposes. Custodians are responsible for creating and maintaining their own notice of purposes.

Does *PHIA* require me to file a copy of my notice of purposes with anyone?

No. There is no requirement under *PHIA* for custodians to file a copy of their notice of purposes with any body or organization. Custodians are responsible for creating and maintaining their own notice of purposes.

Sometimes I am legally obligated to disclose information. Do I need to tell people about that?

Yes. Under certain circumstances custodians are legally obligated to disclosure information without consent such as where the custodian has been provided with a search warrant, in cases of public safety (e.g., infectious diseases), and situations where a duty to report arises (e.g., child abuse). These types of situations should be addressed in your notice of purposes.

Record of Disclosure

What is a disclosure?

The term "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 (refer to section 2 of *PHIA*).

Is granting access to the information in a database considered a disclosure?

Yes. Electronic access is considered a disclosure and a record of this disclosure should be maintained.

Who needs to maintain a record of disclosure?

All custodians that disclose personal health information shall maintain a record of disclosure.

My organization only employs a few people - do I still need to maintain a record of disclosure?

Regardless of the size of the organization or the number of employees, a custodian must always maintain certain information relating to disclosures of personal health information.

What information do I have to record about disclosures of personal health information?

A custodian is required to record the name of the person to whom the custodian is disclosing the information, the date and purpose of the disclosure and a general description of the information being disclosed.

How detailed does the record of disclosure need to be?

A custodian needs to record only general information about the person to whom the custodian is disclosing the information including

- The name of the person to whom the information is being disclosed,
- The date of the disclosure,
- The purpose of the disclosure and
- A general description of the information being disclosed.

How should I maintain this record? On paper? In a file? In a database?

If the information being disclosed is in a paper format, the record of disclosure can be recorded in that same format. If a custodian maintains an electronic database

and lawfully discloses information in an electronic format, the custodian will not have to maintain a separate record of disclosure as long as the electronic database automatically keeps a log of the following information:

(a) the user identification of the person that accesses the information;
(b) the date and time the information is accessed; and
(c) a description of the information that is accessed or that could have been accessed.

Do I need to inform the people to whom I am disclosing information that a record of the disclosure is being maintained?

No. A custodian's record of disclosure is for its own internal purposes. It provides custodians with a means of ensuring that disclosures are being managed appropriately.

I already maintain a record of disclosures. Do I need to change it?

Custodians should ensure that any existing records of disclosure are in compliance with the requirements of *PHIA*.

Do I have to file a copy of my records of disclosure with someone?

No. There is no requirement under *PHIA* for custodians to file a copy of their records of disclosure with any body or organization. Custodians are responsible for creating and maintaining their own records of disclosure.

Sometimes I am legally obligated to disclose information. Do I need to record information about that?

Yes. Records of all disclosures must be maintained by custodians, except as otherwise permitted or required by law.

Circle of Care

What is the "circle of care"?

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. The health information custodians that are permitted to operate within the circle of care are set out at section 24 of *PHIA*.

PHIA defines "circle of care" as 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. For example, a person who is admitted to a hospital would have a circle of care that consisted of any of the doctors and nurses involved in providing care on the ward, as well as laboratory staff, x-ray staff and other allied health professionals and staff involved in that episode of care.

Do I need to have a patient's written consent to share information with other individuals in my organization who are working with the same patient?

Unless the patient has indicated otherwise, the health information custodians specified under *PHIA* can assume implied consent to share with individuals in their organizations involved in the provision of health care to the patient. The information shared should be the minimum amount to achieve the purpose for which it is used.

Implied consent is based on the premise that it must be reasonable to believe that an individual is aware of the purpose of the collection, use or disclosure and knows that they can either give or withhold consent. This knowledge would be provided through the health information custodian posting or making readily available a notice generally describing these purposes in a location where it is likely to come to the individual's attention or by providing the individual with such a notice.

I often informally discuss cases with a colleague of mine who is a retired healthcare professional. Can I continue to do this?

This colleague would not be considered to be in the circle of care of the individual and it would not be appropriate to share personal health information with this person. A person has to be directly involved in the delivery of care to a person in order to be considered within that person's "circle of care".

Are administrative staff members considered part of the circle of care?

Administrative staff members are not directly involved in the provision of health care to the patient but, depending on their role, may have a responsibility in the circle of care as defined in *PHIA*. There may also be circumstances where administrative staff members use personal health information for other "uses", as permitted under *PHIA*.

An example of such a use would be for the registration of a patient, or for billing purposes. Such a use would be limited to the minimum amount of information necessary for the purpose.

What is the responsibility of a health information custodian who works for a non-health information custodian?

A health care practitioner who has custody or control over personal health information but who contracts with, is employed by or volunteers for an organization that is not defined as a health information custodian under *PHIA*, is not an agent. In such a circumstance, the health care practitioner themselves would fall within the definition of a health information custodian under *PHIA* and must ensure compliance.

Examples of health information custodians who work for non-health information custodians include:

- A nurse employed by a school board to provide health care services to students;

- A doctor employed by a mining company in order to treat work-related injuries;

- A registered massage therapist providing health care services to clients of a spa; and

- A nurse employed in-house by a manufacturing firm in a health care capacity.

I engage in non-traditional healthcare practices in which family members are considered an important part of the healing process. Are these family members considered part of the circle of care?

PHIA permits persons who are involved in the provision of health care to the individual to be involved in the circle of care. In some circumstances, for instance when an individual is being discharged from hospital, unless the patient indicates otherwise, a family member providing health care at home may be in the circle of care. *PHIA* also allows the disclosure of personal health information with consent. As such, depending on the circumstances, you may need to obtain consent for sharing of information.

Another physician has requested information on a patient. Can I disclose my patient's information with them?

Before relying on implied consent you must determine if the receiving physician is in the patient's circle of care. Is the receiving physician involved in the current episode of care? If so, you may disclose the information relying on implied consent as the receiving physician will be considered to be within the circle of care.

Where can I get more information on the circle of care?

Further materials on the circle of care have been prepared by the Government of Newfoundland and Labrador, and are available for anyone to use. The materials can be found in the *PHIA* Policy Development Manual on the Department of Health and Community Services' *PHIA* resource website at:

www.gov.nl.ca/health/PHIA

Privacy Breaches

What is a privacy breach?

A privacy breach is any collection, use or disclosure of personal health information that is not authorized under *PHIA*. Privacy breaches occur when personal health information is:

- stolen;
- lost;
- disposed of, except as permitted by *PHIA* or the regulations; or
- disclosed to or accessed by an unauthorized person.

What is an example of a privacy breach?

An example of a privacy breach under *PHIA* would be where a custodian discloses an individual's personal health information to someone who is not a custodian without first obtaining the individual's express consent.

Who needs to create a process for managing privacy breaches?

All custodians of personal health information should have a process in place to manage privacy breaches.

My organization only employs four people. Do I still need to create a process for managing privacy breaches?

Yes. All custodians of personal health information should have a process in place to manage privacy breaches.

What considerations should go into creating a process for managing privacy breaches? Where can I get advice on how to create a process for managing privacy breaches?

Custodians of personal health information should have a process in place for:

(1) Containing a breach,
(2) Implementing a pre-determined breach protocol,
(3) Notifying affected individuals and the Office of the Information and Privacy Commissioner (if applicable), and
(4) Investigating and preventing similar breaches in the future.

Privacy breach guidelines have been prepared by the Government of Newfoundland and Labrador, and are available for anyone to use. The privacy breach guidelines can be found in the *PHIA* Risk Management Toolkit on the Department of Health and Community Services' *PHIA* resource website at:

www.gov.nl.ca/health/PHIA

I already have a process for managing privacy breaches. Do I need to change it?

If custodians have a process for managing privacy breaches, they should review it to make sure it meets the requirements set out under *PHIA*. For example, custodians are required to notify the Office of the Information and Privacy Commissioner when a material breach of *PHIA* occurs.

Do I have to file a copy of my process for managing a privacy breach with someone?

No. Custodians should have a process for managing privacy breaches in place, but they do not need to submit their process to anyone for approval. Custodians may contact the Office of the Information and Privacy Commissioner to obtain feedback on their process for managing privacy breaches.

Do I have to report privacy breaches to someone? Is there a form for doing this?

Custodians are required to notify the individual who is the subject of the information at the first reasonable opportunity where personal health information is:

- stolen;
- lost;
- disposed of, except as permitted by *PHIA* or the regulations; or
- disclosed to or accessed by an unauthorized person.

Custodians are not obligated to notify affected individuals where it is reasonable to believe that the privacy breach will not have an adverse impact on:

> (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.

In addition, Custodians are required to report material breaches to the Office of the Information and Privacy Commissioner. A from for reporting privacy a breach to the Office of the Information and Privacy Commissioner has been prepared by the Government of Newfoundland and Labrador, and is available for anyone to use. The breach reporting form can be found in the *PHIA* Risk Management Toolkit on the Department of Health and Community Services' *PHIA* resource website at:

www.gov.nl.ca/health/PHIA

Do I have to maintain an internal record of privacy breaches?

Custodians are required to take steps that are reasonable in the circumstances to ensure that the personal health information in their custody or control is protected appropriately. As a best practice, maintaining an internal record of all privacy breaches that occur is recommended.

Sometimes I am legally obligated to disclose information. Could this be considered a privacy breach?

Disclosing personal health information in a way that is either permitted or required by law, such as disclosing information about infectious diseases to public health officials, does not constitute a privacy breach.

A patient made a limited consent request that restricts me from sharing information with someone. I accidentally forgot about it and share their information with that person. Is this a privacy breach?

Yes. Disclosing an individual's personal health information in a way that is contrary to their instructions represents a privacy breach, unless the disclosure is otherwise permitted or required by law.