



## CONTACT INFORMATION

Office of the Information  
and Privacy Commissioner  
3<sup>rd</sup> Floor, 2 Canada Drive  
Sir Brian Dunfield Building  
P.O. Box 13004, Station A  
St. John's, NL A1B 3V8  
Tel: (709) 729-6309  
Fax: (709) 729-6500

Toll Free in  
Newfoundland  
and Labrador:  
1-877-729-6309

E-mail:

[commissioner@oipc.nl.ca](mailto:commissioner@oipc.nl.ca)

[www.oipc.nl.ca](http://www.oipc.nl.ca)

“Thus, at least in part, medical records contain information about the patient revealed by the patient, and information that is acquired and recorded on behalf of the patient. Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that goes to the personal integrity and autonomy of the patient.”

- Justice La Forest  
*McInerney v.  
MacDonald*, [1992]  
2 SCR 138 (SCC)

# SAFEGUARD

A QUARTERLY NEWSLETTER PUBLISHED BY THE  
OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

VOLUME 01, ISSUE 01

MAY 2017

- ◆ What is the *PHIA* and Why is it Necessary?
- ◆ What is Personal Health Information?
- ◆ Overview of Compliance Essentials
- ◆ To Whom Does *PHIA* Apply?
- ◆ The Role of the OIPC
- ◆ Collection, Use and Disclosure of Personal Health Information
- ◆ Statutory Review of the *PHIA*

## Message from the OIPC Commissioner

Welcome to the inaugural issue of *Safeguard*, a publication intended to further educate and inform those who interact with personal health information of their roles and responsibilities in relation to the *Personal Health Information Act (PHIA)*.

There is a continuing need for awareness and understanding of many aspects of the *PHIA* and we hope this newsletter will provide guidance on these matters.

Of the information we ‘share’ with government, our personal health information is among the most sensitive and sacred in terms of our privacy. To obtain care, we provide this information with the legitimate expectation that it will be held in the strictest confidence.

Those entrusted with access to personal health information must consider privacy in making every decision that may result in accessing or disclosing that information. Prior to accessing personal health information ask, what is my purpose in doing so? If there is no valid health care purpose requiring access to personal health information, do not look at it.

The *PHIA* represents the minimum privacy standards required by law. Public confidence in our health care system demands more than that. Maintaining the highest privacy standards possible in regards to personal health information is not an option, it is a necessity.

## What is the *PHIA* and Why is it Necessary?

The *PHIA*, which came into force in 2011, addresses the handling of personal health information. While the concept of patient confidentiality is not new, the responsibilities and obligations set out in the *PHIA* are specific and extensive. Simply put, the *PHIA* creates rules for the protection of personal health information in both public and private settings while supporting transparency and accountability practices. The *PHIA* strikes a balance between the protection of individuals' privacy, and the need to use personal health information for legitimate health-related, quality control and research purposes.

The *PHIA* applies to custodians involved in the delivery of health care services in both the public and the private sectors and, therefore, prevails over provincial public-sector privacy law (the *ATIPPA*, 2015) and federal private-sector privacy law (*PIPEDA*).

The *PHIA* is necessary due to the extreme sensitivity of personal health information, the increasing use of technology to create and exchange personal health information and the often large number of health care providers involved in providing care to a single individual. The need and ability to share personal health information without delay benefits patients; however, parameters must be in place to ensure that the collection, use and disclosure of personal health information respects and ensures privacy.

A complete copy of the *PHIA* can be found at:

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

## What is Personal Health Information (“PHI”)?

Personal health information is defined in section 5 of the *PHIA*. Generally, it is identifying information in oral or recorded form or about an individual that relates to:

- their physical and mental health including their status, history and family history;
- the identity of the health care provider;
- blood and organ donation;
- registration information (including MCP number or other identifier);
- payments or eligibility for insurance coverage;
- entitlement to health care benefits;
- information collected incidental to health care or payment;
- prescriptions, 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
- the identity of a representative authorized to act on the individual's behalf.

## Overview of Compliance Essentials

- ◆ **Policies and Procedures (s.13)** – Custodians must develop and implement information policies and procedures surrounding their duties and responsibilities under the *PHIA*. These policies must include procedures and practices for the protection of PHI and the privacy of the patient; the collection, storage, transfer, copying, modification, use and disposition of PHI, for limiting disclosure and access.

The policies and procedures must provide appropriate measures to address the risks associated with the storage of PHI, taking into account the manner and form in which the PHI is recorded, the location of storage and the degree of sensitivity of the PHI to be protected.

- ◆ **Employee Obligations (s.14)** - All employees, agents, contractors and volunteers of a custodian and, where the custodian operates a health care facility, those health care professionals who have the right to treat persons at the facility, **must** sign confidentiality agreements. The custodian is also responsible for ensuring that those persons are aware of the duties imposed by this *Act* and the custodian's information policies and procedures.
- ◆ **Information Security and Breach Management (s.15)** – A custodian must take reasonable steps to ensure that PHI in its custody or control is protected against theft, loss and unauthorized access, use, disclosure, copying or modification; and records containing PHI in its custody or control are retained, transferred and disposed of in a secure manner.

Patients must be notified by the custodian, at the first reasonable opportunity, of circumstances where their PHI is stolen, lost, improperly disposed of, or disclosed to or accessed by an unauthorized person unless the custodian reasonably believes that the event will not have an adverse impact upon the provision of health care to the patient or their mental, physical, economic or social well-being. Also, notification may be recommended by the Commissioner.

Where a custodian reasonably believes that there has been a material breach, as defined in the regulations, the custodian must inform the Commissioner of the breach.

- ◆ **Contact Person (s.18)** - Custodians must appoint a contact person to: facilitate compliance with the *Act*; to respond to requests for access to or correction and inquiries about the custodian's information policies and procedures; and to 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 *PHIA*. Where a custodian is an individual, the custodian may be the contact person.

## Overview of Compliance Essentials (Continued)

- ◆ **Public Statement (s.19)** – Custodians must, via a written statement, make patients aware of the existence of the custodian’s information policies and procedures along with a general description of those policies and procedures. The written statement must also identify the contact person and their contact information. Additionally, patients must be advised of how they may access or request correction of their PHI and how a complaint may be made to the Commissioner.
- ◆ **Communication with Patient (s.20)** – Where a custodian collects PHI directly from the patient or from his or her representative, the custodian must take reasonable steps to inform the individual or his or her representative of the purpose for the collection, use and disclosure of the PHI and of the identity and contact information of the contact person. Such steps may include posters or pamphlets in areas where they are likely to come to the individual's attention setting out the permissible purposes for collection, use or disclosure.
- ◆ **Information Management Providers (s.22)** – Where a custodian employs an information manager to provide information management or IT services, the custodian and information manager must sign an agreement which provides for the protection of the PHI which the information manager handles. This would include arrangements protecting the information against unauthorized access, use, disclosure, disposition, loss or modification and prescribing the purposes for which the information manager may use or disclose that information.
- ◆ **Disclosure Without Consent (s.37)** – Custodians must understand the limited circumstances under which they may disclose PHI without the consent of the patient and the ability of patients to provide express restrictions on the disclosure of their PHI.
- ◆ **Disclosure Log (s.48)** – Custodians who disclose PHI must make a note of the disclosure outlining: the name of the person to whom the custodian disclosed the information; the date and purpose of the disclosure; and a description of the information disclosed. Written notes do not have to be made where an automatic electronic log of the following information is kept: the user identification of the person that accesses the information; the date and time the information is accessed; and a description of the information that is accessed or that could have been accessed.

## To Whom Does *PHIA* Apply?

The *PHIA* applies to custodians involved in the delivery of health care services in both the public and the private sectors in Newfoundland and Labrador.

A custodian is a person who has custody or control of PHI as a result of providing health care services. Examples include:

- Regional Health Authorities;
- Department of Health and Community Services;
- 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 (e.g. chiropractor, massage therapist, etc.); or
- a Health Care Provider. This person is different from a Health Care Professional. A Provider is paid, directly or indirectly, by MCP or another insurer or person, in whole or in part, to provide health care services to an individual.

The *PHIA* specifically excludes “an employee of a custodian when acting in the course of his or her employment” from the definition of custodian. However, all employees of a custodian must be aware of the custodian’s responsibilities as employees are agents for the custodian – the custodian will be held accountable for the actions of its employees.

A custodian does not cease to be a custodian with respect to PHI until complete custody and control of the record, passes to another person who is legally authorized to hold the record (usually another custodian).

### Custodianship in clinics of Health Care Professionals?

Clinics with multiple Health Care Professionals should have agreements in place to address the ownership of patient’s PHI. This will assist in instances where a clinician decides to leave the practice. Under the *PHIA* each Professional is responsible for the PHI of their patients but the *PHIA* does not speak to ownership.

## Role of the OIPC

The *PHIA* identifies the powers, responsibilities and accountabilities of the Office of the Information and Privacy Commissioner (OIPC). These powers include oversight of the proper interpretation and application of the *Act*. Furthermore, the OIPC can investigate any alleged breach of the *Act*, inform the public about the *Act* and make recommendations to ensure compliance. Additionally, the OIPC also offers free education and resources for custodians and individuals and is available to provide training on request.

The Commissioner’s *PHIA* Reports can be found in full at:

<http://www.oipc.nl.ca/reports/commissioner>.

## Collection, Use and Disclosure of PHI

Custodians may not collect, use or disclose personal health information unless:

1. the individual consents to the collection, or
2. the collection, use or disclosure is permitted or required by the Act without consent.

The consent of a patient may be express or implied; however, consent must be express where the disclosure is to a person who is not a custodian or where the disclosure is not for the purpose of providing or assisting in providing health care.

PHI must be collected directly from the patient, except in the circumstances outlined in section 31 including:

- ◆ where the individual is unable to provide the information and the custodian collects the information from the patient's representative;
- ◆ where the custodian collects the information from a person who is not a custodian for the purpose of carrying out an approved research project;
- ◆ where the collection is permitted or required by an Act; or
- ◆ where the collection is for the purpose of assembling a family or genetic history and the information will be used for providing a health service to the individual.

Custodians may only use PHI for the limited purposes set out in the *PHIA*.

Custodians must obtain consent to disclose PHI unless disclosure without consent is permitted by the Act. Sections 37 to 46 set out the limited circumstances under which disclosure without consent may occur. These include disclosures for health care or health-related purposes, where individual is deceased, for health and safety, in respect of proceedings, required by law, for research purposes, of registration information, or for monitoring health care payments.

Custodians must make themselves familiar with the provisions of the *PHIA* such that they are aware of instances where disclosure without consent is mandatory.

Custodians may not collect, use or disclose PHI if other information will serve the purpose. Custodians must not collect, use or disclose more PHI than reasonably necessary.

Collection, use and disclosure of PHI will each be given more detailed attention in upcoming issues.



## Resource List

Breach reporting is not mandatory under the *PHIA*, however, in the past year this Office has noticed a 106% increase in the number of *PHIA* breaches reported to the OIPC. While this is not necessarily an indication that *PHIA* breaches are on the rise, it does highlight the need for on-going *PHIA* training and education. The Department of Health and Community Services offers the following tools on its website ([www.health.gov.nl.ca/health/PHIA](http://www.health.gov.nl.ca/health/PHIA)):

- ◆ Privacy Statement
- ◆ Public Awareness Materials (posters/brochures)
- ◆ Frequently Asked Questions
- ◆ Online Education Program
- ◆ Risk Management Toolkit
- ◆ Policy Development Manual

### Statutory Review of the *Personal Health Information Act (PHIA)*

Participation in the *PHIA* Review is now closed. Submissions were provided by the OIPC, all four Health Authorities, NLCHI, the Canadian Institute for Health Information, the Health Research Ethics Board, Memorial University, Workplace NL, NL Association of Social Workers, Newfoundland and Labrador Medical Association, the College of Massage Therapists of NL, Canadian Nurses Protective Society, the College of Physicians and Surgeons, Sequence Bio, and Stella's Circle.

The Review Committee was charged with completing a

review of the *PHIA* and providing a final report arising from the review to the Minister Responsible for the Department of Health and Community Services. The final report is to include detailed findings and recommendations for the Minister's consideration.

Committee Chairperson Mr. Dave Morgan has indicated that submissions are currently being reviewed and a final report will be provided in due course.

For more information regarding the Review please visit:

<http://www.phiareviewnl.ca/>

### Perfecting your Privacy Practices

The *PHIA* requires custodians to develop and implement detailed written privacy policies and procedures. When developing your privacy manual be sure to consider the safeguards you will need to put in place to protect the personal health information which you handle.

Safeguards must encompass physical (e.g. locked doors and filing cabinets), administrative (e.g. confidentiality agreements and privacy training) and technical (e.g. encryption and audits/monitoring systems) security measures.