OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

PHIA Toolkit for Small Custodians

March 31, 2023

HEALTH INFORMATION
A PRIVATE MATTER

Table of Contents

INTRODUCTION 1

WHO IS THE CUSTODIAN? 2

WHO IS THE AGENT? 2

WHO IS THE INFORMATION MANAGER? 3

WHO IS THE CONTACT PERSON? 3

CUSTODIAN'S OBLIGATIONS UNDER *PHIA* 4

SECURITY OF INFORMATION 7

PRIVACY BREACH 9

COLLECTION, USE AND DISCLOSURE IN ACCORDANCE WITH *PHIA* 9

ACCESS TO PERSONAL HEALTH INFORMATION 12

CORRECTION OF PERSONAL HEALTH INFORMATION 13

ADDITIONAL RSOURCES 15

APPENDIX "A"

This guide is for informational purposes only and does not constitute legal advice. Please refer to the *Personal Health Information Act* (*PHIA)* for a complete understanding of your obligations. Should you wish to discuss *PHIA* and/or require assistance in identifying sections of the Act that may be applicable to a particular situation, please contact the Department of Health and Community Services or the Office of the Information and Privacy Commissioner.

INTRODUCTION

The *Personal Health Information Act (PHIA)* is Newfoundland and Labrador's legislation that governs personal health information. The purpose of *PHIA* is to establish strong and effective mechanisms to protect personal health information (PHI), establish rules for the collection, use, disclosure, security, and management of PHI, and provide individuals with the right to access their PHI or request the correction of PHI.

Target Audience

This toolkit is intended as a guide to help small custodians, such as individual health care professionals/practitioners and private long term care facilities, understand and comply with their obligations under *PHIA.*

Using this Tool Kit

This tool kit will help you:

- familiarize yourself with *PHIA* terminology;
- identify custodians, agents, information managers, etc. and understand the roles and responsibilities of each;
- help you understand and fulfill your obligations under *PHIA*; and
- identify additional resources to help you navigate *PHIA.*

Who Must Comply with *PHIA*?

PHIA applies to custodians who have 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 section 2(1)(o)). *PHIA* outlines obligations for all custodians, regardless of the size of their organization. As such, it is important to identify who is the custodian.

Custodians include (section 4 of *PHIA* provides a full list):

- Regional Health Authorities
- Health care professionals (section 2(1)(j)):
    - Chiropractors
    - Dentists
    - Optometrists
    - Registered Nurses/Licensed Practical Nurse
    - Massage Therapists
    - Physiotherapists

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

  - Psychologists
  - Social Workers
  - Pharmacists
  - Occupational Therapists
  - Dietitians
- Health care providers (section 2(1)(k))
  - A health care provider is defined as a person, other than a health care professional, who is paid by MCP or another insurer or person that provides health care services to an individual. For example, a home support agency.
- Operators of a health care facility (section 2(1)(i))

WHO IS THE CUSTODIAN?

Use the template in Appendix A to write your answer.

Custodian

For smaller entities, the custodian is usually the individual who is responsible for making decisions and overseeing operations. Health professionals working within a group setting should clarify who is a custodian through an information management agreement and/or consult their legal counsel.

Examples:

- If you are a physician in private practice, regardless of the ownership of the practice, you are typically the custodian.
- If you are the pharmacist in charge of a pharmacy, regardless of whether you own it or not, you are the custodian.
- If you are a chiropractor, physiotherapist, psychologist, dentist, etc. in private practice, you are typically the custodian, unless you are employed by another custodian.
- If you own a private long term care home, you are a custodian.

If identifying the custodian is not immediately obvious, a more thorough analysis may be required. You may contact our office for further guidance or seek legal advice.

WHO IS THE AGENT?

Use the template in Appendix A to write your answer.

Agent(s)

In relation to a custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of

the custodian, and not the agent's purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian.

Examples:

- medical office assistant(s);
- office manager(s);
- reception/front desk staff;
- volunteers;
- locum physicians;
- trainees and students.

Agents must sign an oath/affirmation of confidentiality acknowledging they are bound by *PHIA* and are aware of the consequences of a breach. It is strongly recommended they take the *PHIA* Facilitated Education Program.

WHO IS THE INFORMATION MANAGER?

List your information manager(s) on the template in Appendix A.

Information Manager

An information manager is a person or body, other than an employee of a custodian acting in the course of their employment that:

- Processes, retrieves, stores or disposes of personal health information for a custodian or
- Provides information management or information technology services to a custodian.

For further information regarding the information manager, please refer to section 22 of *PHIA.*

You must have a written agreement with your information manager that provides for the protection of the personal health information against unauthorized access, use, disclosure, disposition, loss or modification in accordance with *PHIA* and its regulations.

The requirements for written agreements with information managers are quite extensive. The Department of Health and Community Services *PHIA* Policy Development Manual discusses Information Management Agreement Principles. You may wish to consider consulting with a lawyer or privacy professional to assist in drafting the document to ensure compliance with *PHIA* and its regulations.

If you already have an agreement in place with your information manager, you may consider having a lawyer review it to ensure it meets all the requirements.

Information Manager(s) must sign an oath/affirmation of confidentiality acknowledging they are bound by *PHIA* and are aware of the consequences of a breach. It is strongly recommended they take the *PHIA* Facilitated Education Program.

WHO IS THE CONTACT PERSON?

Identify your contact person on the template in Appendix A.

Contact Person

A custodian must identify a contact person. If a contact person is not identified, the custodian themselves is automatically the contact person.

Subsection 18(3) of *PHIA* outlines the obligations of the designated contact person, who must:

- facilitate the custodian's compliance with *PHIA* and regulations;
- 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 *PHIA* and the regulations;
- respond to inquiries from the public in respect of the custodian's information policies and procedures;
- 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 custody of the custodian.

CUSTODIAN'S OBLIGATIONS UNDER *PHIA*?

Custodians are obligated to comply with *PHIA*. There is no mechanism to "opt out" of the Act and its regulations. Agents also have obligations under the *Act*. It is incumbent on custodians to properly manage their relationship with their agents, including information managers, to ensure compliance with *PHIA*.

Practices to Protect Personal Health Information

The following sections briefly outline custodian obligations under *PHIA.* To review the full sections please refer to the *Act*. It is strongly recommended custodians take the time to review their obligations.

Oath or Affirmation of Confidentiality

An 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.

An 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.

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.

The Department of Health and Community Service's *PHIA* Policy Development Manuel has a section on Oath or Affirmation of Confidentiality to assist custodians.

PERSONAL HEALTH INFORMATION ACT
Section Title and Custodian Responsibility

Section 13 - Information practices, policies and procedures

A custodian that has custody or control of personal health information must establish and implement information policies and procedures ensuring compliance with *PHIA* and its regulations. These policies and procedures must:

- 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 the information;
- restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian to only that information that the employee, agent, contractor or volunteer requires to carry out the purpose for which the information was collected or will be used;
- restrict access to an individual's personal health information by a health care professional who has the right to treat personas at a health care facility operated by the custodian to only that information that the health care professional requires to carry out the purpose for which the information was collected or will be used;
- 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;
- provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information.

The Department of Health and Community Services also provides resources for policy and procedure development, located on their PHIA Resource page at https://www.gov.nl.ca/hcs/phia/.

Section 14 - Obligations of Employees, etc.

A custodian is responsible for ensuring *PHIA* compliance among staff, agent(s), the information manager, contractors, volunteers, etc. and that all take an oath of confidentiality acknowledging they are bound by *PHIA* and are aware of the consequences of a breach. It is strongly recommended they take the *PHIA* Facilitated Education Program.

Section 16 - Accuracy of Information

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

- 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;
- clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, completeness or up-to-date character of the information; and
- make a reasonable effort to ensure that the person to whom a disclosure is made is the person intended and authorized to receive the information.

Section 18 - Contact Person

A custodian who is an individual may designate a contact person. Where no contact person is designated, the custodian shall be considered to be the contact person.

A custodian that is not an individual, such as an organization, shall designate one or more contact persons.

A contact person shall:

- facilitate the custodian's compliance with *PHIA* and the regulations;
- 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 *PHIA* and the regulations;
- respond to inquires from the public in respect of the custodian's information policies and procedures;
- 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.

Note: Where the contact person is a person other than the custodian:

- a collection, use or disclosure of personal health information by the contact person is considered to be a collection, use or disclosure by the custodian;
- a disclosure of personal health information to the contact person is considered to be disclosure to the custodian.

Section 19 - Written Public Statement

A custodian must make available to those who are or who are likely to be affected by the custodian's activities a written statement that:

- provides a general description of the custodian's information policies and procedures;
- identifies the contact person and provides access information, or where no contact person has been designated, sets out the name and access information of the custodian;
- describes how an individual may obtain access to or request correction of a record of personal health information about the individual that is in the custody or control of the custodian;
- describes how a complaint may be made to the commissioner.

Section 20 – Duty of Custodian to Inform or Notify.

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

- of the purpose for the collection, use and disclosure of the information;
- of the identity and other relevant information relating to the contact person;
- of other information prescribed in the regulations, i.e. material breach.

SECURITY OF INFORMATION

Custodians must ensure they are adequately protecting patients' personal health information at all times. A custodian must take reasonable steps to ensure that:

- personal health information in its custody or control is protected against theft, loss and unauthorized access, use or disclosure;
- records containing personal health information in its custody or control are protected against unauthorized copying or modification;.
- records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner.

Safeguards must be proportionate to the sensitivity of the information. This requires knowing what PHI is in your custody or control and then determining how best to protect it, paying particular attention to PHI that is sensitive in nature.

It is important to remember that there is no "one-size-fits-all solution" for meeting your obligations under *PHIA* and the threshold for what is an adequate safeguard may differ between custodians.

For example, a psychologist may have more sensitive PHI in their custody or control than a dentist, and therefore stronger safeguards may be necessary.

Let's take a closer look at some security concepts in action.

Use the template in Appendix A to evaluate and document your office's compliance.

- **Administrative policies** include written policies outlining the custodian's instructions in respect of collecting, using and disclosing PHI and the rules to effectively safeguard PHI; breach reporting procedures and ongoing privacy and security training for employees.
- **Technical and physical safeguards** include the following.
  - Access controls restricting the PHI that employees can access. Access controls can often be administered through your electronic medical record system (EMR) and can help limit snooping and other unauthorized access to PHI. It is particularly important to limit access to sensitive PHI. Consider that different agents may require different levels of access to PHI. For example, consider whether it is appropriate for your reception staff to have full access to all patient medical records.
  - Locks on doors and filing cabinets, and rooms with restricted access.
  - Regular monitoring or auditing of your record system, either EMR system or other, to detect potentially unauthorized accesses by employees (snooping).
  - Refer to the Office of the Information and Privacy Commissioner's guidance on Use of Email for Communicating Personal Health Information.
  - Encryption of servers, workstations, mobile devices and other data carriers used to access and store PHI.
  - Adequate methods of authentication, including two-factor authentication for accessing EMR systems.
- **Physical security** might include a monitored alarm system, or electronic "fob"/access cards for gaining access to the premise
- **Confidentiality** might include sound-proofing between exam rooms to limit eavesdropping, or a confidential area at reception where patients can speak privately with staff without fear that their personal health information will be overheard by other patients. Training should include locking screens when leaving a workstation and making sure paper patient files are not left in sight of patients or colleagues without a need to know.

PRIVACY BREACH

A security breach means that personal health information was inappropriately disclosed, accessed by an unauthorized individual, or was stolen, lost, or disposed of contrary to *PHIA*. Breaches can be caused by many types of incidents including malware, an employee who purposely or accidentally discloses patient PHI, and lost, stolen or misplaced laptops or other mobile devices, or physical records.

PHIA has mandatory breach notification provisions. Custodians should take the time to carefully review section 15 and the provisions noted below and be sure they understand their obligations in respect of security breaches.

When a breach of personal health information under the custody or control of a custodian has occurred, the custodian must notify the individual who is the subject of the information at the first reasonable opportunity.

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:

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

Even though the custodian may not need to notify the individual as noted above, the Information and Privacy Commissioner may recommend that the custodian, at the first reasonable opportunity, notify the individual who is the subject of the information.

If a material breach has occurred involving the unauthorized collection, use, or disclosure of personal health information, the custodian must inform the Commissioner of the breach.

Under section 5 of the *PHIA* Regulations, when determining whether there has been a material breach for the purpose of subsection 15(4) of *PHIA*, a custodian must consider the following:

- the sensitivity of the personal health information involved;
- the number of people whose personal health information was involved;
- whether the custodian reasonably believes that the personal health information involved has been or will be misused; and
- whether the cause of the breach or the pattern of breaches indicates a systemic problem.

COLLECTION, USE AND DISCLOSURE IN ACCORDANCE WITH *PHIA*

As per section 29, a custodian shall 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 lawful purposes; or
- the collection is permitted or required by *PHIA*.

Collection, use and disclosure under *PHIA* is further discussed in sections 29-50.

"Collect" means to gather, acquire, receive or obtain the information by any means from any source and *"collection"* has a corresponding meaning.

"Disclose" means to make the personal health information in the custody or control of a custodian or other person available or release it but does not include a use of the information and *"disclosure"* has a corresponding meaning.

"Use" means to handle or deal with the personal health information in the custody or control of a custodian or to apply the information for a purpose and includes reproducing the information but does not include disclosing the information.

Scope of Collection

A custodian must not collect more personal health information than is reasonably necessary to meet the purpose of the collection (section 32). Think of it as a "need to know" principle.

The "need to know" principle must extend to agents, employees, contractors or volunteers of the custodian or health care professionals who have the right to treat persons at a health care facility operated by a custodian. Access to personal health information should only be to information required to carry out the purpose for which the information was collected or will be used.

The custodian is responsible for ensuring their agents, employees, contractors or volunteers understand and comply.

It might be a good idea to start by considering what information you are collecting from your patients and evaluate whether you need the information to provide health care to that individual.

Below are some examples to help you evaluate your practices in respect of collection and disclosure.

Am I Collecting too much Information?

Jenny is a new patient of Dr. Grant. At her first appointment, Jenny is asking to fill out a health questionnaire and provide some basic information. While most of the questions make sense (allergies to medications, chronic health conditions, etc.) Jenny wonders why Dr. Grant needs her partner's name and phone number, or why she is being asked to provide her employer's name and address.

At face value, it is not clear how this information relates to the provision of health care, and therefore collecting it may be contrary to *PHIA.*

If you determine you do need to collect this information for the provision of health care to Jenny, then be clear about **WHY** you are collecting it.

For example, if you are collecting the partner's name and phone number as an emergency contact, then consider having an "emergency contact" space on the form and let the patient decide who to choose.

IF YOU DON'T NEED THE INFORMATION, DON'T COLLECT IT!

Consent

PHIA is **consent-based legislation** and generally requires that custodians obtain consent to collect, use, or disclose personal health information. Depending on the circumstances, consent may be implied or express (section 24). A custodian must follow the rules of consent found in sections 23-28.

Consent must meet certain requirements for the purposes of providing health care. The consent:

- must be the consent of the individual;
- must be knowledgeable; and
- must not be obtained through deception or coercion.

Consent is considered "knowledgeable" when the individual knows:

- the purpose of the collection, use or disclosure of the personal health information;
- that they may give or withhold consent;
- that the information may be only collected, used or disclosed without their consent in accordance with *PHIA*.

Am I Disclosing too Much Information?

You are Steve's psychiatrist, and his family doctor has requested a status update. In response, you ask your medical office assistant to send over a copy of Steve's complete medical records to his family doctor.

Disclosing Steve's **complete** medical file to his family doctor may be contrary to *PHIA* as it is unclear why his family doctor would require this level of detailed and sensitive personal health information.

In this example, it might be more appropriate to send the family doctor a high-level summary including your diagnosis and any medications you have prescribed. This disclosure is likely reasonable in the circumstances.

If Steve's family doctor insists on receiving additional information beyond this, then it may be appropriate to inquire about why the family doctor needs this information, **before** disclosing Steve's sensitive personal health information.

As well, remember to ensure that Steve consents to the disclosure, or that you have the authority to disclose the information without consent.

Documenting Consent

It is recommended that custodians always document patient consent. For example, if consent was obtained verbally, it should be noted on the patient's file. Without documentation, custodians cannot substantiate that an individual's consent was obtained. As well, this practice promotes transparency and accountability in the provision of health care.

Note**:** *PHIA* allows for the disclosure of PHI **without** patient consent in certain circumstances. Sections 37-47 outline the circumstances in which a custodian may disclose PHI without consent.

ACCESS TO PERSONAL HEALTH INFORMATION

Access to Personal Health Information

Under section 52(1) an individual has a right to access a record containing their personal health information that is in the custody or under the control of a custodian. This access can extend to a representative of the individual as per section 7. Custodians should note that while *PHIA* establishes a formal framework for access requests, as per section 59, nothing in the Act prevents informal access.

A custodian can require a request for access to be in writing, unless the individual has limited ability to read or write English, or has a disability or condition that impairs their ability to make the request in writing.

The request needs to have enough detail to help the custodian identify and locate the record; if the request doesn't provide enough information, the custodian must offer to assist the individual in making the request.

A custodian may require an individual to provide the information confirming their identity, which can assist in locating the correct record, such as:

- name;
- birth date;
- MCP or other unique identifier(s);
- address; or
- sufficient information to allow for record retrieval with reasonable effort.

Timely Response

As per section 55 custodians must respond within 60 days of receiving a request to access PHI. The deadline may be extended by an additional 30 days where:

- meeting the deadline would unreasonably interfere with the operations of the custodian, or
- the information consists of numerous records or locating the information that is the subject of the request cannot be completed within the originally prescribed time limit.

Should a custodian extend the original timeframe by an additional 30 days, the custodian must give the individual written notice of the extension, including the reasons for the extension. A custodian must respond to the individual's request as soon as possible and no later than the expiration of the extended time limit.

Custodian's Response

Access: Where the custodian grants access, the custodian must make the record available to the individual for review and, upon request, provide a copy of the record to the individual and an explanation, where necessary, of any information contained in the record. While custodians are allowed to charge a fee, the fee can be waived by the custodian and cannot exceed the limit established by the Minister. OIPC discussed the matter of fees in Report AH-2012-001.

Record does not Exist: The custodian must give written notice to the individual stating that, after reasonable efforts, it has been concluded that the record does not exist or cannot be found.

Access Refused: Section 58 of *PHIA* discusses why a custodian would refuse access to personal health information. Where the custodian refuses access to the record, in whole or in part, the custodian must provide written notice to the individual stating that access to the record, in whole or in part, is refused, along with reasons for the refusal, and that the individual may appeal the refusal to the Trial Division under Part VII of *PHIA* or request a review by the commissioner as per Part VI of *PHIA.*

Failure to Respond

Should a custodian fail to respond to an access to personal health information request within the legislated timeframe they will 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 by the Commissioner.

CORRECTION OF PERSONAL HEALTH INFORMATION

When an individual, who has been granted access to their PHI, identifies incorrect PHI within their record, the individual is able to request a correction as per section 60(1) of *PHIA*. This request can be submitted in writing or verbally at no charge to the individual. It is the responsibility of the custodian to take reasonable steps to confirm the individual's identity in order to process a request to correct PHI.

Timely Response

As per section 62, a custodian must respond to a PHI correction request no more than 30 days (as defined under the Interpretation Act, section 22(k)) after receiving it. However, a custodian may extend the time limit by an additional 30 days where:

- meeting the original due date would unreasonably interfere with the operations of the custodian, or
- the information that is the subject of the request for correction is located in numerous records so that the request cannot be completed within the original 30 days.

Should a custodian extend the original response time by 30 days, the custodian must give the requestor written notice of the extension along with reasons for the extension. A custodian must respond to the individual's request as soon as possible and no later than the expiration of the extended time limit.

The custodian must grant the request for correction where the individual has demonstrated that the record is incomplete or inaccurate for the purposes of the information and gives the custodian the information necessary to make the correction.

Making the Correction

When a request for correction is granted, the custodian must make the correction and provide written notification to the individual that it has been made as per section 63 of *PHIA*. The custodian must also provide written notice of the requested correction, to the extent reasonably possible, to those to whom the custodian has disclosed the information within the 12 month period immediately preceding the request (for example, WorkplaceNL or a health care professional to whom a referral was made), unless the custodian reasonably believes that the correction will not impact the ongoing provision of health care or other benefits.

Refusal

A custodian may refuse a request to correct personal health information if the record was not originally created by the custodian and the custodian does not have sufficient knowledge, expertise and authority to correct the information. The OIPC discussed the refusal to correction personal health information in Report AH-2020-001.

A custodian may also refuse a request for correction where the information consists of a professional opinion or observation the 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.

When a custodian refuses a request to correct PHI, the custodian must annotate the personal health information with the correction that was requested and not made. Where practical, the custodian shall notify those to whom the custodian has disclosed the information within the 12 month period immediately preceding the request for correction of the annotation, unless the custodian reasonably believes that the correction will not impact the ongoing provision of

health care or other benefits. The OIPC discussed section 63(2)(a) of *PHIA* in Report AH-2014-001.

Recourse

When a request to correct PHI is refused, the custodian must provide the requestor with a written notice outlining the correction that the custodian refused to make, the reasons for the refusal and the right of the individual to appeal the refusal to the Trial Division or request a review by the Information and Privacy Commissioner.

Custodians that receive a request for access to or correction of an individual's personal health information and are unsure what to do may contact the Office of the Information and Privacy Commissioner for guidance.

ADDITIONAL RESOURCES

Resources from the Office of the Information and Privacy Commissioner

Office of the Information and Privacy Commissioner

https://www.oipc.nl.ca/custodians

- *PHIA* Compliance Checklist for Custodians
- Use of Email for Communicating Personal Health Information
- Use of Personal Health Information for Research Purposes
- Yes You Can

Resources from the Department of Health and Community Services

https://www.gov.nl.ca/hcs/phia/

- Personal Health Information Act
- Personal Health Information Regulations
- *PHIA* Privacy Statement
- *PHIA* FAQs
- *PHIA* Overview
- *PHIA* Online Education Program
- *PHIA* Policy Development Manual

Resources from the Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada

Appendix “A”

PHIA Small Custodian Policy and Procedures Template

PHIA Small Custodian Policy and Procedures Template

This template is intended to help you develop and/or evaluate your organization's compliance with the *Personal Health Information Act* (*PHIA*). If used correctly and completed in sufficient detail, this document can serve as a basis for your organization's privacy and access policy and procedures. *PHIA* governs the collection, use, disclosure, security, and management of personal health information (PHI), and provides individuals with the right to access their PHI or request the correction of inaccuracies.

Information practices: This policy and associated procedures outline the circumstances in which the custodian will collect, store, transfer, copy, modify, use, and dispose of the PHI of individuals.

Principles to consider include the following:

- the custodian must manage personal information in a privacy-protective manner in compliance with *PHIA*;
- an individual has the right to protection of their PHI that is held by the custodian and has the right to access it and to request corrections;
- the custodian must be transparent in how it protects the PHI that it holds;
- the custodian is obligated to notify an individual if there is a breach of their PHI unless section 15(6) or 15(7) indicate otherwise; and
- the custodian must continually evaluate its information practices to ensure compliance with *PHIA*.

Your Structure and Operations

Who is the Custodian?	Things to Consider...
	If identifying the custodian is not immediately obvious to you, a more thorough evaluation may be required. See section 4 of *PHIA*, or contact our office for further guidance on making this determination.
Who is your Agent(s)?	**Things to Consider...**
	These include all your employees, contractors, and volunteers. An agent is any person that you have expressly authorized to collect, use, disclose, or access PHI for you or on your behalf.

Who is your Information Manager(s)?	Things to Consider…
	Some custodians may not have one, others may have more than one. See section 22 of *PHIA*. You must have a written agreement in place with your information manager(s) and meet the requirements under *PHIA*. You may want to attach a copy of any agreements to the end of this document for ease of reference.
Who is your Contact person?	**Things to Consider…**
	You must designate a "contact person". **If you do not make a designation, the custodian (if a natural person and not a corporation) is deemed to be the contact person.** Ensure your contact person knows and understands their obligations outlined in section 18. Your contact person is responsible for several duties. Do you have a written procedure for: • custodian's compliance with *PHIA*; • ensuring that all of the custodian's employees, contractors, agents, and volunteers are appropriately informed of their duties under *PHIA*; • receiving and managing inquiries/complaints from the public about your information practices/policies; and • responding to requests for access or correction of PHI?

Custodian's Obligations Under *PHIA*

<table>
<tr><th>Collection, Use, and Disclosure</th><th>Things to Consider...</th></tr>
<tr><td>What PHI do you normally collect and why?

When describing the PHI in this section, you may wish to categorize the information. For example, I collect PHI from individuals only as necessary to provide them with health care. I collect health insurance information for billing purposes.</td><td rowspan="3">Collection, use, and disclosure must only be in accordance with PHIA (ss.29-50).

You must limit the amount of PHI collected, used, and disclosed to the minimum amount reasonably necessary to achieve the purpose for the collection, use, and disclosure of PHI.

Evaluate what PHI you regularly collect, use, and disclose.

Review forms, questionnaires, etc. Consider the circumstances when you regularly use and disclose patient PHI (e.g. referrals to another custodian, patient changing doctors, etc.).

Do you have reasonable administrative security measures in place? How about procedures and/or limitations on faxing or emailing PHI? Do you use an Electronic Medical Records (EMR) system? Did you have a Privacy Impact Assessment on any system or process that you use? Have you implemented voice mail rules or established a social media policy for staff?</td></tr>
<tr><td>What PHI do you normally use and why?

For example, I use a patient's PHI when providing them with health care and for communicating with my office staff (agents) for follow-up as necessary to provide the patient with ongoing health care.</td></tr>
<tr><td>What PHI do you normally disclose and why?

For example, I disclose billing information to receive payment; I disclose PHI to police officers or social workers conducting investigations; I disclose PHI to another custodian or care provider only as necessary to facilitate the ongoing care of my patient.</td></tr>
<tr><th>Consent</th><th>Things to Consider...</th></tr>
<tr><td>How does your organization typically obtain knowledgeable consent from patients?</td><td>Generally, patients should be kept informed in respect of the collection, use, or disclosure of the PHI to allow them to make informed decisions about their care.

How well do you inform your patients of their rights under PHIA? Do you inform them of the purpose of collection? Advise them of how to access their own information, including fees? Advise them of their right to correction?</td></tr>
</table>

	Do you have a *PHIA* public written statement posted in your office or on your web site? Does it include a description of your policies, contact person information, information on how to access their PHI, or how to complain?

Custodian's Information Practices (ss.13-22)

Technical, Administrative, and Physical Safeguards	Things to consider...
Detail your organization's administrative and technical safeguards.	Evaluate whether your safeguards are adequate to protect PHI under your custody and control Some examples include: • limits on faxing/emailing PHI; • preprogrammed fax machine (if used)--are the preprogrammed numbers continually updated?; • have you completed a Privacy Impact Assessment? Please read our guidance piece on Privacy Impact Assessments on our website; • updating the Privacy Impact Assessment; • voicemail rules; • social media policy and awareness; • a policy regarding the safe and appropriate usage of the custodian's systems and the PHI contained in the systems; • ongoing training of employees and agents regarding information and security and privacy practices; • a controlled termination of employment process to ensure that any outgoing employees no longer have access to any records, electronic systems, or to the premises; the employee's accesses should be removed prior to termination; • access controls for paper and electronic records; • logging and auditing of your EMR to detect unauthorized activity by employees (e.g. snooping, unauthorized alteration of data, etc.);

	• using a secure method of transmission for sending/receiving documents (e.g. secure file transfer); • encryption of servers and other data carriers; and • proper authentication, including two-factor authentication for EMR systems.
Physical Safeguards	**Things to consider…**
Detail the security measures your organization has in place.	Some examples include: • lock on doors, filing cabinets, and restricted areas; • a monitored alarm system; • electronic "fob"/access cards for gaining access to the premises; and • computer screens not visible to clients.
Confidentiality	**Things to consider…**
Detail how your organization keeps PHI confidential.	Some examples include: • locked filing cabinets; • restricted access; • privacy screens on monitors; • caution about overhearing information; • sound proofing between exam rooms to limit eavesdropping or a confidential area at reception where patients can speak privately about their medical concerns; • ensuring computer screens are locked automatically when inactive for some time and training employees to lock screens when leaving their workstation; and • training staff to ensure paper records are not left unattended in rooms with patients.
Security Breaches	**Things to consider…**
Detail your organization's procedure for managing a security breach.	***PHIA*** **has mandatory breach notification provisions so it is important you take the time to understand your obligations under section 15.** Your organization should have clear breach reporting protocols so your employees/agents know what constitutes a breach/material

	breach, who they should report it to, and that they must do so at the first reasonable opportunity. Your procedures should outline measures to identify and contain security breaches, as well as the notification of individuals affected by real or suspected security breaches. It should identify roles and responsibilities to effectively respond to breaches quickly and in a coordinated manner. You may wish to designate your contact person as the person responsible to receive breach reports and for managing the breach process to ensure *PHIA*'s mandatory breach reporting requirements are met.
Request for Access and Correction of PHI	**Things to consider…**
What is your organization's process for managing access requests or requests to correct PHI?	Under section 52(1) an individual has a right to access a record containing their PHI that is in the custody or under the control of a custodian. Your policy should set out criteria and the procedures for responding to applications for access to PHI you hold. It applies to individuals making application for their own PHI. Your written procedures for managing access/correction requests under section 52 and section 60 should include: • statutory timelines for responding to access requests; • time extensions; • contents of the response; • how access is to be granted; • refusing access; • fees; • notifying applicants if their PHI is in the custody or control of another custodian; • managing requests for correction of an individual's PHI; and • keeping a record or log of all disclosures of PHI.