OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NEWFOUNDLAND AND LABRADOR

PHIA: Personal Health Information Act Overview

NL Pharmacy Board – November 23, 2023

PHIA

- Came into force in 2011; contains rules for collection, use and disclosure of personal health information (PHI)
- Similar to but expands on the older concept of patient confidentiality
- *PHIA* is more specific

Purpose/Objectives of *PHIA*

- *PHIA* creates consistent rules for the protection of PHI in both public and private settings.
- Supports transparency and accountability practices.
- *PHIA* strikes a balance between:
  - Protecting individuals' privacy, and
  - Using PHI for legitimate health-related purposes – for example: delivering primary health care, planning and monitoring of the health system, public health and safety, health research, and criminal investigations.

Application – Who?

- Custodian (section 4) means a person who has custody or control of PHI as a result of or in connection with the performance of the person's powers or duties or the work described in that paragraph. For example:
  - NL Health Services;
  - A person who operates a health care facility, a licensed pharmacy, an ambulance service etc;
  - With respect to MUN – the Faculty of Medicine, School of Nursing, School of Pharmacy etc.

Application – Who? (continued)

- A health care professional - when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual

- A health care provider – a person, other than a health care professional, who is paid by MCP, another insurer or person, whether directly or indirectly or in whole or in part, to provide health care services to an individual

- Note: Some health care professionals, such as social workers, are either custodians themselves or employed by a custodian. Decisions about who is a custodian could have a major impact on individual staff.

Who is NOT a Custodian?

- Health care professionals employed by custodians
- A person that collects or uses an MCP number for a purpose other than the provision of health care
- An information manager (see sections 2(1)(l); 22)
- Full list in section 4(2)
- NOTE: all employees of custodians and agents must be aware of responsibilities – the custodian will be held accountable for the actions of their employees and agents.

Health Care Defined

- Health care means an observation, examination, assessment, care, service or procedure in relation to an individual that is carried out, provided or undertaken for one of the following health-related purposes:
  - The diagnosis, treatment or maintenance of an individual's physical or mental condition,
  - The prevention of disease or injury,
  - The promotion of health,
  - Rehabilitation,
  - Palliative care,
  - The taking of a donation of blood, blood products, bodily parts or other bodily substances from an individual,
  - The compounding dispensing or selling of a drug, health care aid, device, product, equipment or other item to an individual or for the use of an individual, under a prescription, or
  - A program or service designated as a health care service in the regulations.

Personal Health Information

- Defined in section 5
- Identifying information **in oral or recorded form** about an individual that relates to:
  - Physical and mental health, including their status, history and family history,
  - Identity of the health care provider,
  - Blood and organ donation,
  - Registration information (incl. MCP# or other identifier), payments or eligibility for insurance coverage,
  - 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,
  - Identity of a representative authorized to act on their behalf.

PHI in Other Records

PHIA section 5 establishes:

5. *(4) Notwithstanding subsection (3), personal health information does not include identifying information contained in a record that is in the custody or under the control of a custodian where*

(a) the identifying information contained in the record relates primarily to an employee or agent of the custodian; and

(b) the record is created or maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employee or agent.

Where Does *PHIA* Apply?

- *PHIA* applies to custodians of personal health information in both public and private sectors in Newfoundland and Labrador
- *ATIPPA* – provincial public-sector privacy law
- *PIPEDA* – federal private –sector privacy law
- *PHIA* replaces both *ATIPPA* and *PIPEDA* in respect of personal health information
  - It has been declared substantially similar to *PIPEDA* by Industry Canada.
  - This status will be impacted if proposed amendments to *PIPEDA* are proclaimed.

PHIA Compliance Essentials for Custodians

- A contact person must be designated (s.18).
- Confidentiality agreements for all employees, agents, contractors and volunteers (s.14).
- Agreements with “information managers” (s.22).
- Detailed privacy and security policies and procedures (ss.13,15).
- Privacy and security training program (s.14).
- Written statement of information practices, available to the public (s.19).
- Notice of purposes for which personal health information is collected, used and disclosed for posting or providing to clients (ensures that consent is knowledgeable) (s.20).
- Records/logs of disclosures (s.48).
- Process for managing limited consent/lock box requests (s.37).
- Privacy breach management protocol (s.14).
- OIPC has guidance on our website www.oipc.nl.ca/pdfs/PHIAComplianceChecklist.pdf

Custodian's Obligations Under *PHIA*

- Custodians are obligated to comply with *PHIA*. There is no mechanism to "opt out" of the Act.

- Section 13 - Information practices, policies and procedures
  - A custodian must establish and implement information policies and procedures ensuring compliance with *PHIA* and its regulations.

  - The Department of Health and Community Services has resources for policy and procedure development located on their *PHIA* Resource page at www.gov.nl.ca/hcs/phia/

Custodian's Obligations Under *PHIA* (continued)

- Section 14 - Obligations of Employees, etc.
  - A custodian is responsible for ensuring *PHIA* compliance among staff, agent(s), the information manager, contractors, volunteers, etc.
  - Custodians should develop a standard form oath or affirmation for individuals to sign.
- Section 16 - Accuracy of Information
  - Before using or disclosing PHI in its custody or control, a custodian shall: take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary 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.

Custodian's Obligations Under *PHIA* (continued)

- 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.

- Section 20 – Duty of Custodian to Inform or Notify.
  - Where a custodian collects personal health information directly from the individual, the custodian shall take reasonable steps to inform the individual of the purpose for the collection, use and disclosure of the information

Security Obligations

- Custodians must take steps that are reasonable in the circumstances to ensure that:
    - personal health information is protected against theft, loss and unauthorized access, use or disclosure;
    - records are protected against unauthorized copying or modification; and,
    - records are retained, transferred and disposed of in a secure manner.

- Custodians must notify individuals if their personal health information is lost, stolen, disposed of or disclosed in an unauthorized manner, unless there will be no adverse impact on their health care or well-being.

- Custodians must notify the Privacy Commissioner in the event of a material breach.

Safeguards

Physical:
-Securing physical premises appropriately.
-Retaining records of PHI in a secure area.

Administrative:
-Requiring employees and agents to sign confidentiality agreements.
-Requiring agents to attend privacy and security training.
-Developing, monitoring and enforcing privacy and security policies.
-Conducting privacy impact assessments on information systems, technologies or programs that involve personal health information.

Technical:
-Instituting strong authentication measures.
-Implementing encryption where appropriate.
-Implementing detailed audit monitoring systems.

Access and Correction

- An individual has the right to access their personal health information. There are limited exceptions, which include:
  - harm to the individual or another person might result;
  - where a legal investigation is underway;
  - it is a frivolous or vexatious request; etc.

- *PHIA* identifies the process and timelines for accessing personal health information files and requesting corrections or annotations. (Part V starting at section 51)

- *PHIA* identifies the responsibilities of custodians regarding access and correction.

Consent, Collection, Use Disclosure: Key Sections

- Consent – Sections 23-28
- Collection – Sections 29-32
- Use – Sections 33-35
- Disclosure – Sections 36-50

Collection, Use and Disclosure of PHI

- Custodians may not collect, use or disclose PHI unless:
  - The individual consents, or
  - It is permitted or required by the Act without consent.
- 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 (general limiting principle).

Consent

- Where consent is required, consent must:
  1. Be the consent of the individual the info is about
  2. Be knowledgeable, which means:
     1. They know the identified purpose;
     2. They know they can say no; and
     3. They know *PHIA* will be followed.
  3. Not be obtained through deception or coercion
- Within the “circle of care” a custodian is entitled to assume that they have the individual’s continuing implied consent as long as they are providing health care to that individual, unless specifically withdrawn.

Express Consent

- Express consent is obtained as a result of an individual positively indicating, either verbally or in writing, that they agree to a stated purpose.
- Under *PHIA*, consent must be express and cannot be implied when:
  1. A custodian discloses to a custodian for a purpose other than providing health care.
  2. A custodian discloses to a non-custodian for a purpose other than providing health care.
- There are exceptions set out in the Act where no consent is required.

Implied Consent

- Implied consent is consent that may be reasonably inferred from signs, actions or facts, or by inaction or silence.
- As with express consent, implied consent requires that individual's be notified at the point of collection of the intended uses and disclosures of their PHI:
  - Verbal notification, discussion
  - Pamphlets, posters
- Implied consent ends if individual expressly withdraws consent.

Disclosure Without Consent

- Section 37 – disclosure without consent for *health care* purposes:
  - A custodian may disclose to another custodian:
    - where it is not possible to obtain consent of the individual in a timely manner; or
    - the individual has been certified as an involuntary patient
  - A custodian may disclosure to a non-custodian:
    - for the purposes of contacting a relative, friend or potential substitute decision-maker of the individual where the individuals is injured, incapacitated or ill and unable to give consent

Disclosure Without Consent (continued)

- Section 39 - disclosure without consent for *health related* purposes
- Section 38 – where individual is deceased
- Section 40 – disclosure related to health and safety
  - Where the custodian reasonably believe the disclosure is required
    - to prevent or reduce a risk of serious harm to the mental or physical health of safety of the individual the information is about or another individual; or
    - for public health or safety

Disclosure for Enforcement

- Section 42(1) of *PHIA* is a mandatory disclosure provision
- When disclosing PHIA, the custodian should confirm that:
    - there is an inspection or investigation;
    - the disclosure of the personal health information is for the purpose of facilitating the inspection or investigation; and
    - the inspection or investigation is authorized by *PHIA*, the *Child, Youth and Families Act* (formerly *Child, Youth and Family Services Act*) or another Act or Act of Canada.

Disclosure for Enforcement (continued)

- Section 42(2) is not a mandatory disclosure and allows one custodian to disclose PHI without consent to another custodian in certain circumstances.
- The custodian disclosing the information should have a reasonable expectation that disclosure will:
    - detect or prevent fraud; or
    - limit abuse in the use of health care; or
    - prevent the commission of an offence under an Act of the province or Canada.

Maintaining Disclosure Info

- Section 48 requires custodians to make note of certain disclosure information:
  - (a) the name of the person to whom the custodian discloses the information;
  - (b) the date and purpose of the disclosure; and
  - (c) a description of the information disclosed.

- The above is not required if the custodians discloses PHI by permitting access to the information through an electronic system that automatically keeps an electronic 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.

NOTE: This is one reason why auditing is a key consideration for electronic systems in health care

OIPC Oversight

- The OIPC can investigate any alleged breach of the Act. This includes complaints about access requests, privacy breaches or correction requests.
- The OIPC can also inform the public about the Act and make recommendations to ensure compliance.
- For matters involving access to or correction of a record, an individual may make an appeal directly to the Supreme Court, Trial Division or following a review by the OIPC.

Breaches

- Under *PHIA*, only material breaches must be reported to OIPC. Considerations for material breaches are outlined in section 5 of the PHIA Regulations:

  (a) the sensitivity of the personal health information involved;

  (b) the number of people whose personal health information was involved;

  (c) whether the custodian reasonably believes that the personal health information involved has been or will be misused; and

  (d) whether the cause of the breach or the pattern of breaches indicates a systemic problem.

NOTE: All four considerations need not be present; these are simply there to guide custodians in their assessment; Custodians may choose to report breaches even when not required by statute (see resources on our website).

Notifying the Individual

- The *Act* requires custodians to notify an individual when their personal health information has been stolen, lost, disposed of improperly or disclosed to, or accessed by an unauthorized person.
- OIPC may also recommend notification (see, for example, P-2018-006).
- Notification is not required where the custodian "reasonably" believes the situation will not have an adverse effect on the provision of health care to the impacted individual or the mental, physical, economic or social well-being of the individual.

Intentional Violation of Privacy

- While mistakes happen, intentional violations of privacy should not. Every individual must take care not to violate another person's privacy.
- 88 of *PHIA* establishes what is considered an offence; Individuals and/or custodians may be prosecuted.
- **Willful** privacy breach may result in a fine of up to $10,000 or imprisonment of up to 6 months, or both.

Privacy Impact Assessments (PIA's)

- OIPC has PIA guidance designed for public bodies on our website. Many of the principles are the same for personal information as personal health information
- A PIA is a systematic process that identifies and evaluates, from the perspective of all stakeholders, the potential effects on privacy of a project, initiative, or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts (Roger Clarke, "Privacy impact assessment: Its origins and development").

PIA's (continued)

- Some Key Questions:
  - Has the custodian identified and appropriately assessed risks to individuals, not just the organization?
  - Once risks were identified, if there are a number of moderate to high risks, did the custodian consider:
    - Is the measure demonstrably necessary to meet a specific need?
    - Is the loss of privacy proportional to the need?
    - Is there a less privacy-invasive way of achieving the same end?

PHIA Toolkit for Small Custodians

- Intended as a guide to help small custodians understand and comply with their obligations under *PHIA*. The 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*.

Resources

Available on the Department of Health and Community Services' website:

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

www.health.gov.nl.ca/health/PHIA

Resources

Available on the OIPC's website:

- *PHIA* Toolkit for Small Custodians
- *PHIA* Compliance Checklist for Custodians
- Best Practices for Information Management Agreements
- Use of Email for Communicating Personal Health Information
- Privacy Breach Incident Form (for Custodians reporting a breach)

Contact Information:

(709)729-6309 (t)

commissioner@oipc.nl.ca

Questions