OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NEWFOUNDLAND AND LABRADOR

PHIA: The *Personal Health Information Act*

Medical Administration Specialists

Janet O'Reilly – Access and Privacy Analyst

January 18, 2016

The Personal Health Information Act

- This Act came into force in 2011, *PHIA* contains rules surrounding the handling of personal health information.
- Similar to the older concept of patient confidentiality.
- The rules under *PHIA* are more specific.

Purpose/Objectives of *PHIA*

- *PHIA* creates consistent rules for the protection of personal health information in both public and private settings.
- Supports transparency and accountability practices.

- *PHIA* strikes a balance between:
  1. protecting individuals' privacy, and
  2. using personal health information for legitimate health-related purposes – for example: delivering primary health care, planning and monitoring of the health system, public health and safety, health research (Research Ethics Board), and criminal investigations.

Application – Who?

- Custodian means a person who has custody or control of **personal health information** as a result of **providing health care services**.

- Examples of custodians under *PHLA*:
  - 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;
  - 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.

Application – Who?

- The rules of *PHIA* apply to custodians but all employees of custodians must be aware of the responsibilities as they are agents for the custodian – the custodian will be held accountable for the actions of their employees.

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.

Application – What?

- Personal Health Information - **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.

Application – Where?

- *PHIA* applies to custodians involved in the delivery of health care services in both the public and the 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.

Collection, Use and Disclosure of PHI

- Custodians may not collect, use or disclose personal health information unless:
    1. The individual consents, or
    2. The collection, use or disclosure is permitted or required by the Act without consent.

- Custodians may not collect, use or disclose personal health information if other information will serve the purpose.

- Custodians must not collect, use or disclose more personal health information than reasonably necessary (general limiting principle).

Consent

- The default position of *PHLA* is that consent is required for the collection, use, disclosure of personal health information.
- Where consent is required, consent must:
    1. Be the consent of the individual the info is about.
    2. Be knowledgeable, which means:
        - they know the purpose of the collection/use/disclosure.
        - they know they can say no, and
        - they know the *PHLA* 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 individuals be notified at the point of collection of the intended uses and disclosures of their personal health information:
    - Verbal notification, discussion
    - Pamphlets, posters

- Implied consent ends if individual expressly withdraws consent.

Permitted Uses without Consent

- When it is consistent with the purpose for which it was collected or reasonably necessary for that purpose.
- Where an Act permits or requires disclosure, for that purpose.
- For planning, delivering, evaluation, monitoring of health services or preventing fraud.
- For risk management or quality of care.
- In a proceeding or contemplated proceeding.
- For cost recovery or obtaining payment.
- To prevent or reduce serious risk of harm.

Permitted Disclosures without Consent

- When it is necessary for the provision of health care and its not possible to obtain consent or they are an involuntary patient.
- For the purpose of contacting a relative or friend when they are injured, incapacitated or ill and unable to consent.
- Reasonably believes it is necessary to prevent or reduce risk of serious harm.
- When required to under an Act.
- For determining or verifying entitlement to services.
- For determining or providing payment.
- For delivering, evaluating or monitoring a program of the custodian.
- To an information manager (with an agreement), an auditor, a statistical agency, an approved researcher.
- To a successor custodian with confidentiality agreement.

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.

Physical, Administrative and Technical 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;

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

Oversight by Privacy Commissioner

- *PHIA* identifies the powers, responsibilities and accountabilities of the Office of the Information and Privacy Commissioner (OIPC).

- The OIPC can investigate any alleged breach of the Act, 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.

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 (s.13, s.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).

Resources for Custodians

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

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

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

Contact Information

Office of the Information and
Privacy Commissioner
P.O. Box 13004, Station A
2 Canada Drive
St. John's, NL
A1B 3V8

(709)729-6309 (t)
(709) 729-6500 (f)
commissioner@oipc.nl.ca
www.oipc.nl.ca

Questions