PHIA:
The *Personal Health Information Act*

Department of Health and Community Services
June, 2011
The **Personal Health Information Act**

**Objectives of presentation:**

1. Introduce the *Personal Health Information Act (PHIA)*

2. Provide an overview of resources available to those subject to *PHIA*
Why do we need PHIA?

Privacy in the health care sector is critical:

- Extreme sensitivity of personal health information
- Historically, a patchwork of rules across the health sector
- Increasing use of technology, including computerized patient records
- Increasing electronic exchanges of personal health information
- Multiple providers involved in providing care to an individual
Why do we need PHIA?

Personal health information is **unique**:

- **Highly sensitive** and personal in nature
- Must be **shared without delay** among a range of health care providers for individuals’ benefit
- Widely used and disclosed for **secondary purposes** that are in the public interest (e.g., research, planning, fraud investigation, quality assurance, etc.)
The Personal Health Information Act became law on April 1\textsuperscript{st}, 2011
What is PHIA?

The **Personal Health Information Act (PHIA):**

- **PHIA** is new health-sector specific provincial privacy law
- Applies to “personal health information” (PHI)
- Governs the actions of “custodians” of personal health information
Why do we need PHIA?

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)
  • Criminal investigations
An overview of **PHIA**

**Application – Who?**

- *PHIA* applies to "**custodians**" of personal health information
- Custodians are identified in the Act
- Examples of custodians under *PHIA*:
  - Regional Health Authorities
  - *Department of Health and Community Services*
  - *Workplace Health, Safety and Compensation Commission*
  - Regulated health professionals: Physicians, pharmacists, dentists, optometrists, etc.
  - Health care providers (unregulated)
  - Others deemed to be custodians via regulations in future
An overview of **PHIA**

**Application – What?**

- **PHIA** establishes a comprehensive set of rules for the collection, use and disclosure of “**personal health information**”

  - “**Personal health information**” is defined in the Act
  - The definition is broad
  - Includes identifiable information about physical and mental health, family history, organ donation, insurance coverage, prescriptions
  - Includes information both in oral and recorded form
An overview of PHIA

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

- Ultimately, PHIA will take the place of 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 may not collect, use or disclose more personal health information than reasonably necessary (general limiting principle)
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 (with limited exceptions)

• Custodians must notify the Privacy Commissioner in the event of a material breach
Security obligations:

- Custodians must implement physical, administrative and technical safeguards to ensure that the PHI in their custody or control is safeguarded:

  **Physical safeguards Include:**
  - Securing physical premises appropriately
  - Retaining records of PHI in a secure area

  **Administrative safeguards Include:**
  - 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 safeguards Include:**
  - Instituting strong authentication measures
  - Implementing encryption where appropriate
  - Implementing detailed audit monitoring systems
Consent:

- The default position of PHIA is that consent is required for the collection, use, disclosure of personal health information

- The requirement to obtain consent is subject to certain specific exceptions set out in the Act

- Where consent is required, consent must:
  - be a consent of the individual
  - be knowledgeable
  - relate to the information
  - not be obtained through deception or coercion

- Generally, consent may be either express or implied, subject to certain restrictions
An overview of *PHIA*

Express consent:

- **Express consent**: consent that 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 may be **exceptions** set out in the Act – where no consent is required.
An overview of PHIA

Implied consent:

- **Implied consent**: consent that may be *reasonably* inferred from signs, actions or facts, or by inaction or silence.

- Certain custodians may assume implied consent, but only when disclosing PHI to custodians or other persons *for the purpose of providing health care* – i.e., within the “circle of care”.

- 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.
Withdrawal of consent – “lock box”:

- Where consent is required for a collection, use or disclosure, consent may be withdrawn – applies to situations involving both express and implied consent

- Withdrawal of consent does not prevent custodians from using or disclosing PHI where uses or disclosures without consent are authorized by PHIA

- Balancing provisions:
  - **Notification** – if a disclosing custodian believes that all information necessary for the provision of health care has not been disclosed, the custodian must notify the recipient of that fact
  - **Override** – a custodian may disclose if disclosure is necessary to prevent significant risk of serious bodily harm to a person or a group of persons
An overview of PHIA

Access and correction

• An individual has the right to access their personal health information – with exceptions: if harm to the individual or another person might result; where a legal investigation is underway; 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
An overview of PHIA

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.

• If the matter involves access to or correction of a record of personal health information, an individual may make an appeal directly to the Supreme Court, Trial Division or following a review by the OIPC
An overview of PHIA

PHIA – Compliance essentials for custodians include:

- 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

Resources for custodians:

Now available on the Department’s website -

- PHIA FAQs
- PHIA Online Education Program
- PHIA Risk Management Toolkit
- PHIA Policy Development Manual

www.health.gov.nl.ca/health/PHIA
Resources for Custodians

PHIA FAQs

- Frequently asked questions about the Act
- Great place to start when learning about PHIA or when there is a question
- Useful reference tool
- Assistance for custodians in understanding the requirements of PHIA
- Help for residents of the province in understanding their rights under PHIA
Resources for Custodians

PHIA Online Education Program

- An introduction to PHIA
- Three versions of the course – for custodians, for those who work with PHI and for other employees / persons who don’t work with PHI.
- May be taken by custodians to familiarize themselves with the Act
- Custodians can have employees, contractors, etc., take the course
- Can complete course over several sessions
- Certificate awarded on completion
- Accredited by College of Family Physicians of Canada and by the NL Pharmacy Board
**PHIA Risk Management Toolkit**

- Assistance for custodians in understanding their legal obligations under *PHIA*
- Assist custodians in assessing their current state of compliance with *PHIA*
- Identify and mitigate risks / gaps in security measures
- The Risk Management Toolkit contains several tools, including:
  - Privacy checklist
  - Short-form PIA
  - Long-form PIA
  - Privacy Audit
  - Privacy Breach Guidelines
PHIA Policy Development Manual

- Assistance for custodians in establishing information policies and procedures as required under PHIA
- Arranges the legal requirements of the Act into a policy development framework
- Provides users with sample language for policies and procedures
- Custodians must adapt the sample language to their specific activities / lines of business
Brian Bennett, B.A., LL.B., CIPP/C
Privacy Manager,
Department of Health and Community Services,
Division of Legislative and Regulatory Affairs

West Block, Confederation Building
P.O. Box 8700
St. John’s, NL  A1B 4J6

T. (709) 729-7007
F. (709) 729-5824
E. BrianDBennett@gov.nl.ca