THE *PERSONAL HEALTH INFORMATION PROTECTION ACT, 2004* AND PROTECTING PERSONAL HEALTH INFORMATION

Independent Diagnostic Clinics Association,
September 30, 2016

Brendan Gray, Health Law Counsel
Office of the Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

DISCLAIMER

THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES AND IS NOT LEGAL ADVICE

Outline

- Overview of the *Personal Health Information Protection Act* (the *Act* or *PHIPA*)
  - Application of the *Act*
  - Bill 119
  - Transparency of Information Practices
  - Collection, use, and disclosure and consent
  - Security of personal health information
  - Planning for, and responding to, a privacy breach
  - Causes of privacy breaches
    - Lack of clarity regarding shared systems
    - Increasing portability of personal health information
    - Unauthorized access

APPLICATION OF THE *ACT*

Application of the Act

- *PHIPA* came into force on November 1, 2004
- The majority of *PHIPA* governs "personal health information" in the custody or control of:
  - "Health Information Custodians," or
  - "Agents" of health information custodians
- However, the *Act* also has broader application
- For example it contains restrictions on the use and disclosure of personal health information by non-health information custodians that receive personal health information from health information custodians

Definition of Personal Health Information

Defined as identifying information about an individual in oral or recorded form that:

- Relates to an individual's physical or mental health
- Relates to the provision of health care to the individual
- Identifies an individual's health care provider
- Identifies an individual's substitute decision-maker
- Relates to payments or eligibility for health care
- Is the individual's health number
- Is a plan of service under the *Home Care and Community Services Act, 1994* for the individual
- Relates to the donation of body parts or bodily substances

Definition of Health Information Custodian

Health information custodians include:

- A health care practitioner who provides health care
- A person who operates a group practice of health care practitioners who provide health care
- A hospital, psychiatric facility and independent health facility
- A pharmacy, ambulance service, laboratory or specimen collection centre
- A long-term care home, care home or home for special care
- A community care access corporation
- A medical officer of health of a board of health
- Minister/Ministry of Health and Long-Term Care
- Minister/Ministry of Health Promotion

Definition of Agent

- An agent is a person that, with the authorization of a health information custodian, acts for or on behalf of the custodian in respect of personal health information

- It is irrelevant whether or not the agent:
  - is employed by the health information custodian
  - is remunerated by the health information custodian
  - has the authority to bind the health information custodian

- A health information custodian remains responsible for personal health information collected, used, disclosed, retained or disposed of by an agent

Duties Imposed on Health Information Custodians and Their Agents

- A number of duties are imposed on health information custodians and their agents under the *Act*

- These duties generally fall into four categories:
  - Collection, use and disclosure of personal health information
  - Security of personal health information
  - Responding to requests for access to and correction of records of personal health information
  - Transparency of information practices

Bill 119 – Health Information Protection Act, 2015

- The Bill was introduced on September 16, 2015
- All the provisions in the Bill relating to *PHIPA were* proclaimed into force on June 3, 2016, with the exception of Part V.1, which relates to the provincial electronic health record
- The provisions that have been proclaimed apply to all personal health information, not simply that accessible by means of the provincial electronic health record
- Regulations required by the Bill have also not been made

/Cont'd

Bill 119 – Health Information Protection Act, 2015, Cont'd

- The provisions in the Bill proclaimed into force include:
  - An amendment to the definition of "use" to clarify that viewing personal health information is a "use" under PHIPA
  - A new provision requiring health information custodians to take steps that are reasonable in the circumstances to ensure personal health information is not collected without authority
  - New provisions requiring notification of "privacy breaches" (discussed below)
  - Amendments to the provisions related to prosecution of offences under *PHIPA* (discussed below)

Bill 119 – Health Information Protection Act, 2015, Cont'd

- Custodians are required to notify the IPC where the theft, loss or unauthorized use or disclosure of personal health information meets prescribed requirements
  - While this provision has been proclaimed, no requirements have been prescribed and there is no duty to notify the IPC
  - Until requirements are prescribed, custodians are expected to continue notifying the IPC of privacy breaches as appropriate
- Custodians are also required to notify regulatory colleges, for example, where an employee is terminated, suspended or disciplined due to their handling of personal health information

/Cont'd

Bill 119 – Health Information Protection Act, 2015, Cont'd

- The requirement to commence a prosecution within six months of when the offence occurred has been removed
- There is no limitation period for commencing a prosecution
- The fines for offences have doubled from $50,000 to $100,000 for individuals and $250,000 to $500,000 for organizations

TRANSPARENCY OF INFORMATION PRACTICES

Transparency of Information Practices

➢Where a health information custodian is not a natural person, it must designate a contact person who is authorized to:

- Facilitate compliance with the *Act*.
- Ensure all agents are appropriately informed of their duties
- Respond to inquiries in relation to information practices.
- Respond to the requests of individuals for access to or correction of their records of personal health information
- Receive complaints about alleged contraventions of the *Act*

➢All custodians must have information practices that comply with the *Act*, including policies and procedures in relation to:

- When, how and the purposes for which personal health information is collected, used, disclosed, retained or disposed
- Administrative, technical and physical safeguards and practices implemented with respect to personal health information

Transparency of Information Practices, con't

- All health information custodians must have and make available a written public statement that describes:
  - The information practices of the health information custodian
  - How to contact the custodian or contact person (if applicable)
  - How an individual may obtain access or request a correction of his or her records of personal health information
  - How an individual may make a complaint to the custodian and to the Information and Privacy Commissioner/Ontario

COLLECTION, USE AND DISCLOSURE

General Provisions Related to Collection, Use and Disclosure

- Not permitted to collect, use or disclose personal health information if other information will serve the purpose

- Not permitted to collect, use or disclose more personal health information than reasonably necessary

- Not permitted to collect, use or disclose personal health information UNLESS:
  - The individual consents, or
  - The collection, use or disclosure is permitted or required by the Act to be made without consent
- The provision of personal health information to an agent of a health information custodian by the health information custodian is considered to be a use by the custodian rather than a disclosure to the agent.

Elements for Valid Consent

Consent, whether express or implied, must:

1. Be the consent of the individual or his or her substitute decision-maker (where applicable),

2. Be knowledgeable, meaning, it must be reasonable to believe that the individual knows:

   - The purpose of the collection, use or disclosure; and
   - That the individual may give or withhold consent

   Where not unreasonable, can rely on a Notice of Purposes to ensure consent is knowledgeable.

3. Relate to the information, and

4. Not be obtained by deception or coercion.

Types of Consent

- There are three types of consent under the *Act*:
  - Express consent
  - Implied consent
  - Assumed implied consent

- Assumed implied consent provisions are sometimes referred to as the "circle of care" provisions

Express Consent

- Consent may be express or implied, except when the *Act* specifies that consent must be express
- Express consent is not a defined term in the *Act*
- It is commonly understood as consent that has been clearly and unmistakably given orally or in writing
- In general, express consent is required to:
  - Disclose personal health information to a non-health information custodian
  - Disclose personal health information to another health information custodian for a purpose other than the provision of health care
  - Collect, use or disclose personal health information for marketing
  - Collect, use or disclose personal health information for fundraising (if it amounts to more than the name and address of the individual)

Implied Consent

- In all other circumstances, consent may be implied
- Implied consent is not a defined term in the *Act*
- Commonly understood as a consent that one concludes has been given based on an individual's action or inaction in particular factual circumstances
- For example, consent may be implied:
  - To *collect* or *use* personal health information for any purpose, subject to certain exceptions
  - To *disclose* personal health information to another health information custodian for the provision of health care

Assumed Implied Consent

- Sometimes referred to as "Circle of Care"

- Section 20(2) of the *Act* provides:

  (2) A health information custodian described in paragraph 1, 2, 3 or 4 of the definition of "health information custodian" in subsection 3 (1), that receives personal health information about an individual from the individual, the individual's substitute decision-maker or another health information custodian for the purpose of providing health care or assisting in the provision of health care to the individual, is entitled to assume that it has the individual's implied consent to collect, use or disclose the information for the purposes of providing health care or assisting in providing health care to the individual, unless the custodian that receives the information is aware that the individual has expressly withheld or withdrawn the consent.

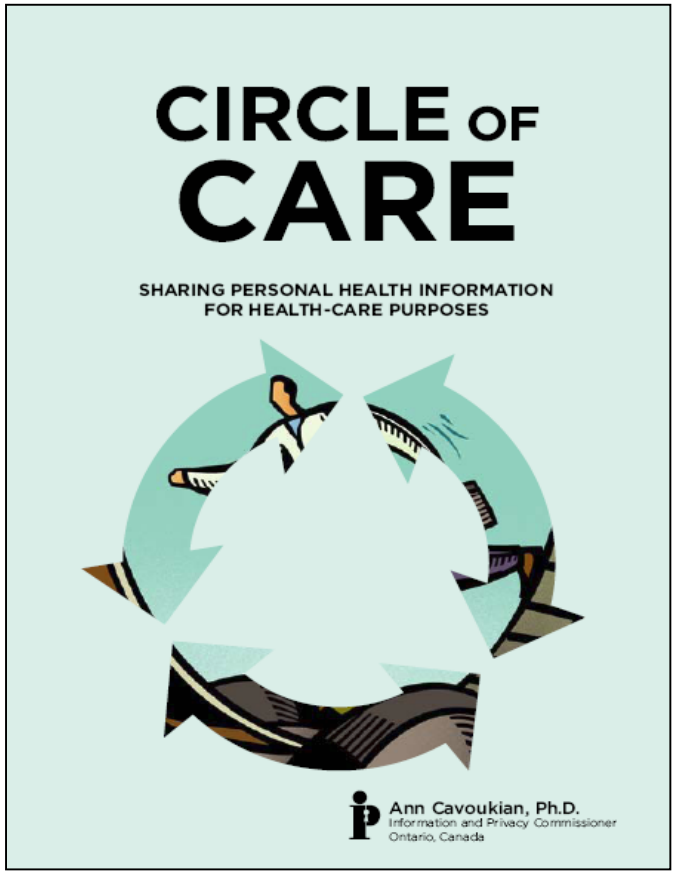
- In the context of a disclosure, the disclosure must be made to another health information custodian

Circle of Care: Sharing Personal Health Information for Health Care Purposes

The guide was published to clarify the circumstances in which consent may be *assumed* to be implied by custodians

Members of the working group who participated in publishing the guide, included:

- Information and Privacy Commissioner/ Ontario
- College of Physicians and Surgeons of Ontario
- Ontario Association of Community Care Access Centres
- Ontario Association of Non-Profit Homes and Services for Seniors
- Ontario Long Term Care Association
- Ontario Hospital Association
- Ontario Medical Association
- Ontario Ministry of Health and Long-Term Care



Available at www.ipc.on.ca

Withholding and Withdrawing Consent and Express Instructions

- The *Act* provides individuals with the right, subject to certain exceptions, to expressly:
  - Withhold or withdraw consent to the collection, use or disclosure of personal health information, including for the purpose of providing health care; and
  - Instruct that their personal health information not be used or disclosed without consent for health care purposes as set out in sections 37(1)(a), 38(1)(a) and 50(1)(e) of the Act
- These are referred to as the "lock-box" provisions, although lock-box is not a term found in the Act

Duties Arising From Withholding and Withdrawing Consent or Express Instructions

1. A custodian must comply with the decision to withhold or withdraw consent or to provide an express instruction unless:
   - The individual changes his or her mind,
   - The Act permits the collection, use or disclosure to be made without consent, except as set out in sections 37(1)(a), 38(1)(a) and 50(1)(e)
2. Compliance may be achieved through policies, procedures or manual processes and/or electronic or technological means
3. Where a custodian is prevented from disclosing personal health information to certain other custodians that is believed to be reasonably necessary for the provision of health care:
   - The disclosing health information custodian **must** notify the other health information custodian of that fact; and
   - The receiving health information custodian may explore the matter with the individual and seek consent to access the locked information

Collections, Uses and Disclosures Permitted Without Consent

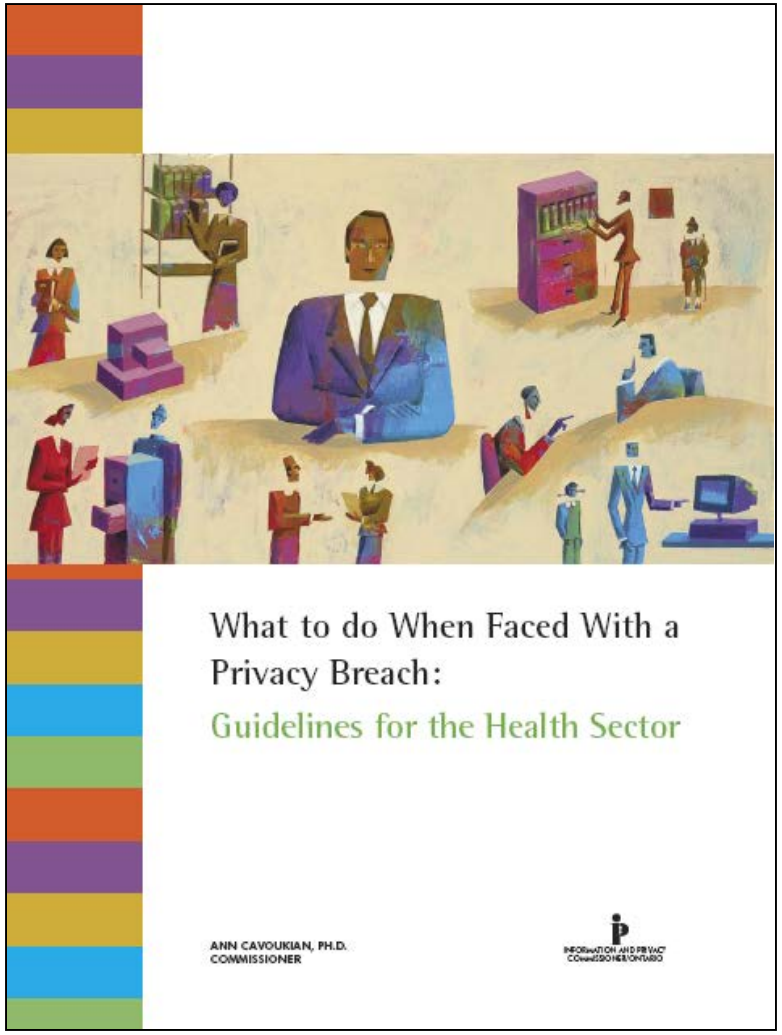
- Collections of personal health information permitted without consent are set out in section 36 of the *Act*
- Uses of personal health information permitted without consent are set out in section 37 of the *Act*
- Disclosures permitted without consent are set out in sections 38 – 48 and section 50 of the *Act*
  - Example: **Under *PHIPA,* health information custodians may disclose personal health information as permitted or required under other Acts, subject to any prescribed requirements or restrictions**. A regulation to the *Laboratory and Specimen Collection Centre Licensing Act,* requires disclosure of reportable diseases to a medical officer of health or health unit. *PHIPA* permits this disclosure as no requirements or restrictions are prescribed.

SECURITY OF PERSONAL HEALTH INFORMATION

Security of Personal Health Information

- Must ensure records of personal health information are retained, transferred and disposed of securely
- Must take reasonable steps to ensure personal health information is protected against:
  - Theft, loss and unauthorized use or disclosure
  - Unauthorized copying, modification or disposal
- Must notify individuals at the first reasonable opportunity if personal health information is stolen, lost or used or disclosed without authority

Develop and Implement a Privacy Breach Management Protocol



Responding to a Privacy Breach

STEP 1: IMMEDIATELY IMPLEMENT PRIVACY BREACH PROTOCOL

- Notify all relevant staff of the breach
- Develop and execute a plan designed to contain the breach and notify those affected
- Recommended that you contact the IPC and provide our office with details of what happened

Responding to a Privacy Breach

STEP 2: STOP AND CONTAIN THE BREACH

- Identify the scope of the breach and take the necessary steps to contain it, including:
  - Retrieve and secure any personal health information that has been disclosed
  - Ensure that no copies of the personal health information have been made or retained by the individual who was not authorized to receive the information
  - Determine whether the privacy breach would allow unauthorized access to any other personal health information and take the necessary steps, such as changing passwords, identification numbers and/or temporarily shutting your system down

Responding to a Privacy Breach

STEP 3: NOTIFY THOSE AFFECTED BY THE BREACH

- You must take the necessary steps to notify those individuals whose privacy was breached at the first reasonable opportunity
- *PHIPA* does not specify the manner in which notification must be carried out. There are numerous factors that may need to be taken into consideration when deciding on the best form of notification
- When notifying individuals affected by a breach:
  - Provide details of the breach to affected individuals, including the extent of the breach and what personal health information was involved
  - Advise of the steps you are taking to address the breach and that they are entitled to make a complaint to the IPC. If you have reported the breach to the IPC, advise them of this fact
  - Provide contact information for someone within your organization who can provide additional information and assistance

Responding to a Privacy Breach

- STEP 4: INVESTIGATION AND REMEDIATION
  - You will be expected to conduct an internal investigation, including:
    - Ensuring that the immediate requirements of containment and notification have been met.
    - Reviewing the circumstances surrounding the breach.
    - Reviewing the adequacy of your existing policies and procedures in protecting personal health information.
    - Ensuring all staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of *PHIPA*.

Potential Causes of Privacy Breaches

1. Lack of Clarity Regarding Responsibilities in Shared Systems

Challenges Posed by Shared Electronic Health Record Systems

- Health information custodians may have custody or control of personal health information they create and contribute to, or collect from, shared electronic health record systems
- No health information custodian has sole custody and control
- All participating health information custodians and their agents will have access to the personal health information
- These pose unique privacy risks and challenges for compliance with the *Personal Health Information Protection Act* (*Act*)

How to Reduce the Risk …

A governance framework and harmonized privacy policies and procedures are needed to:

- Set out the roles and responsibilities of each participating health information custodian
- Set out the expectations for all health information custodians and agents accessing personal health information
- Ensure all health information custodians are operating under common privacy standards
- Set out how the rights of individuals will be exercised

2. Increased Portability of Personal Health Information

Orders HO-004, HO-007 and HO-008

Our office has issued three orders involving personal health information on mobile and portable devices:

Order HO-004 – Theft of a laptop containing the unencrypted personal health information of 2,900 individuals

Order HO-007 – Loss of a USB containing the unencrypted personal health information of 83,524 individuals

Order HO-008 – Theft of a laptop containing the unencrypted personal health information of 20,000 individuals

How to Reduce the Risk….

- **STOP** and ask "Do I really need to store personal health information on this device?"
- **THINK** about the alternatives:
  - Would de-identified or coded information serve the purpose?
  - Could the information instead be accessed remotely through a secure connection or virtual private network?
- If you need to retain it on such a device, **PROTECT** it by:
  - Ensuring it is encrypted and protected with strong passwords
  - Retaining the least amount of personal health information
  - Developing policies and procedures, train and audit compliance

3. Unauthorized Access

Orders HO-002, HO-010 and HO-013

Our office has issued three orders involving unauthorized access:

Order HO-002

- A registered nurse accessed records of the estranged spouse of her boyfriend to whom she was not providing care
- They were accessed over six-weeks during divorce proceedings

Order HO-010

- A diagnostic imaging technologist accessed records of the current spouse of her former spouse to whom she was not providing care
- They were accessed on six occasions over nine months

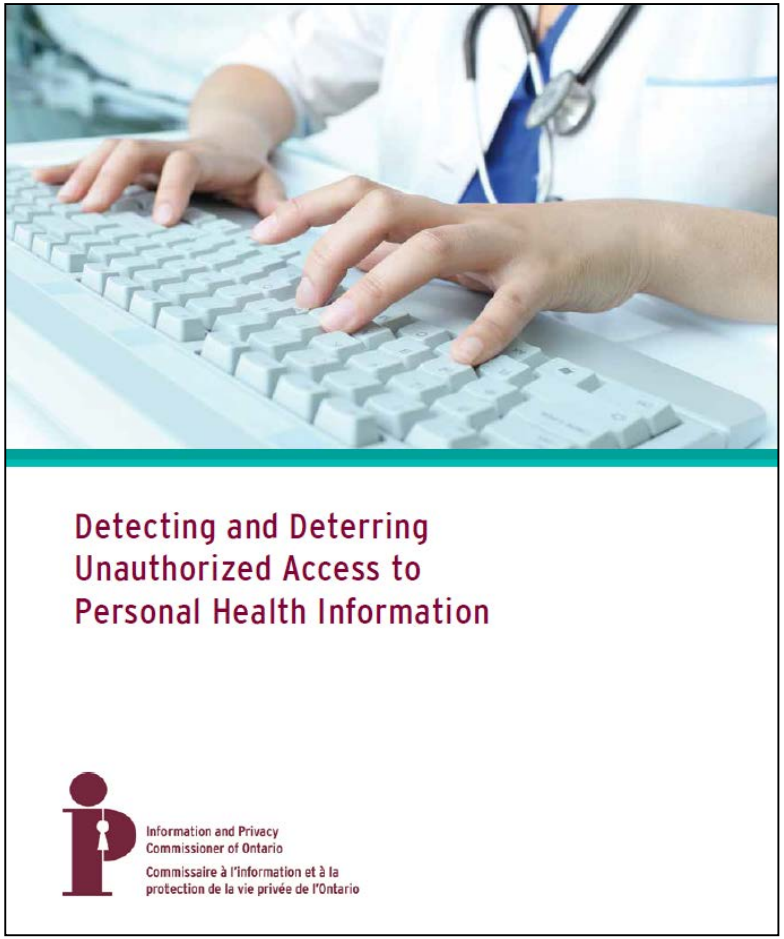
Order HO-013

- Two employees accessed records to market and sell RESPs

How to Reduce the Risk…

- Clearly articulate the purposes for which employees, staff and other agents may access personal health information
- Provide ongoing training and use multiple means of raising awareness such as:
  - Confidentiality and end-user agreements
  - Privacy notices and privacy warning flags
- Immediately terminate access pending an investigation
- Implement appropriate access controls and data minimization
- Log, audit and monitor access to personal health information
- Impose appropriate discipline for unauthorized access

Guidance Document: Detecting and Deterring Unauthorized Access



- Impact of unauthorized access
- Reducing the risk through:
  - ✓ Policies and procedures
  - ✓ Training and awareness
  - ✓ Privacy notices and warning flags
  - ✓ Confidentiality and end-user agreements
  - ✓ Access management
  - ✓ Logging, auditing and monitoring
  - ✓ Privacy breach management
  - ✓ Discipline

How to Contact Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca