PHIPA Potpourri

Orillia Family Health Organization

- December 9, 2014 -

Judith Goldstein
Legal Counsel
Information and Privacy Commissioner of Ontario

Overview of the Act

Application of the *Act*

- The *Personal Health Information Protection Act, 2004* (the *Act)* came into force on November 1, 2004

- The majority of the *Act* governs "personal health information" in the custody or control of:
  - "Health Information Custodians," or
  - "Agents" of health information custodians

Definition of Personal Health Information

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
- Relates to payments or eligibility for health care
- Identifies an individual's health care provider
- Identifies an individual's substitute decision-maker
- Is the individual's health number
- Is a plan of service under *Home Care & Community Services Act*
- 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

Overview of Consent Provisions

- A health information custodian shall not collect, use or disclose personal health information unless the:
  - Consent of the individual has been obtained; or
  - Collection, use or disclosure is permitted or required to be made without consent pursuant to the *Act*
- The *Act* sets out the requirements for a valid consent
- The *Act* also sets out the three types of consent: express, implied and assumed implied consent
- Assumed implied consent has come to be referred to as the "circle of care"

Requirements for Valid Consent

Requirements for Valid Consent

For consent to be valid, the consent must:

- Be the consent of the individual or his or her substitute decision-maker (where applicable)
- 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
- Relate to the information, and
- Not be obtained by deception or coercion

Knowledgeable Consent

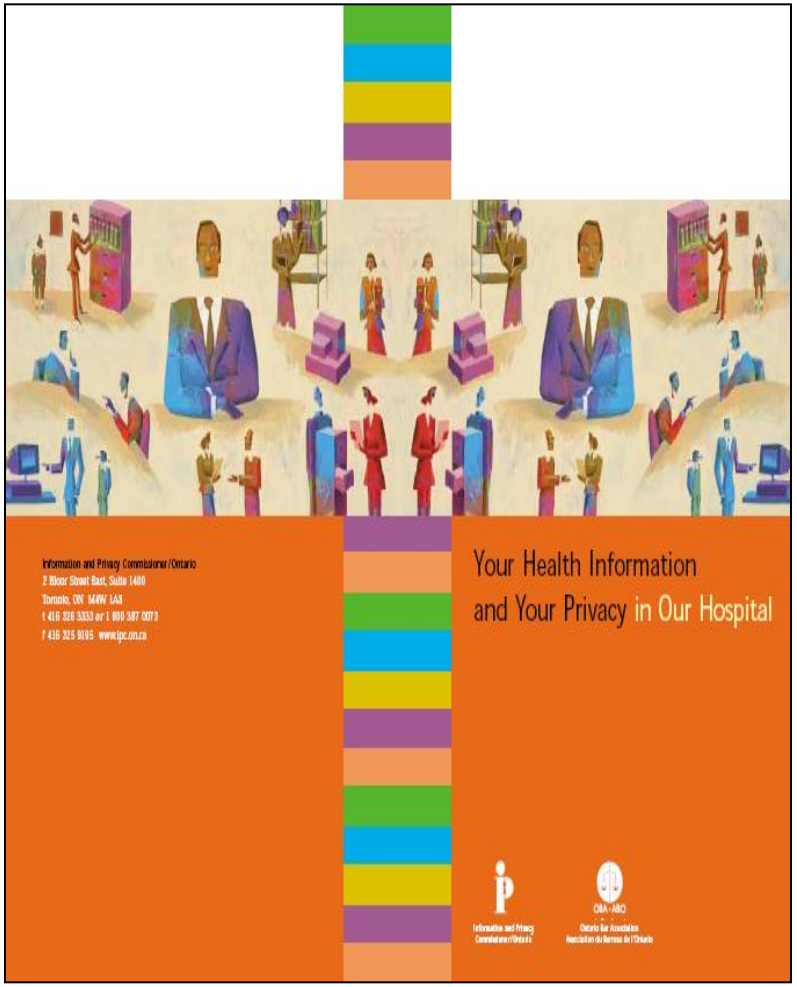
- Does not mean "informed" consent which is a higher standard used in the treatment context

- Discharging an informed consent would involve the patient reviewing his/her PHI and being informed of the material risks and benefits associated with the collection, use or disclosure of the information rather than understanding the purpose of the collection, use or disclosure.

Notice of Purposes

- May rely on a *Notice of Purposes* to support the reasonable belief that an individual knows the purpose of the collection, use, or disclosure unless it is not reasonable in the circumstances
- A *Notice of Purposes*:
  - Must be posted where it is likely to come to the attention of the individual or must be provided to the individual;
  - Must outline the purposes for which the custodian collects, uses or discloses personal health information; and
  - Should advise the individual that he or she has the right to give or withhold consent
- A *Notice of Purposes* is not required when consent may be assumed to be implied but it is a best practice

Notice of Purposes



Types of Consent

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*
- Commonly understood as a consent that has clearly and unmistakably been given orally or in writing
- Express consent is required to:
  - Disclose personal health information to a person that is not a health information custodian (subject to certain exceptions)
  - Disclose personal health information to a 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 using more than the name and address of the individual)


SEATTLE POST-INTELLIGENCER
SEATTLE POST-INTELLIGENCER
GREENBERG
INSURANCE COMPANIES
EMPLOYERS
FINANCIAL INSTITUTIONS

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 a health information custodian 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 health care purposes

Assumed Implied Consent – Circle of Care

- Certain health information custodians *may* assume implied consent to collect, use or disclose personal health information in defined circumstances

- The assumed implied consent provisions have come to be referred to as the "circle of care" provisions although "circle of care" does not appear in the *Act*

- A health information custodian may only assume implied consent if **six** conditions are satisfied

Conditions to be Satisfied to Assume Implied Consent

A health information custodian may only assume implied consent if **all** six conditions are satisfied:

1. The custodian must fall within a category of health information custodians that are entitled to rely on assumed implied consent

- Some health information custodians are not entitled to rely on assumed implied consent, such as:
  - An evaluator defined in the *Health Care Consent Act, 1996*
  - An assessor as defined in the *Substitute Decisions Act, 1992*
  - The Minister or Ministry of Health and Long-Term Care
  - The Minister or Ministry of Health Promotion
  - Canadian Blood Services

Conditions to be Satisfied to Assume Implied Consent (cont'd)

2. The personal health information must have been received from the individual, his/her substitute decision-maker or another health information custodian
   - It must not have been received from any other person such as an employer, insurer or educational institution

3. The personal health information must have been received for the purposes of providing or assisting in providing health care to the individual
   - It must not have been received for other purposes, such as providing health care to another individual

Conditions to be Satisfied to Assume Implied Consent (cont'd)

4. The purpose of the collection, use or disclosure must be for providing or assisting in providing health care to the individual to whom the information relates
   - It must not be collected, used or disclosed for any other purpose, such as research, fundraising or marketing

5. In the context of a disclosure, the disclosure must be to another health information custodian
   - Personal health information must not be disclosed to any other person regardless of the purpose of the disclosure

Conditions to be Satisfied to Assume Implied Consent (cont'd)

6. The health information custodian that receives the personal health information from the individual, his or her substitute decision-maker or another other health information custodian must not be aware that the individual has expressly withheld or withdrawn consent

Withholding and Withdrawing Consent and Express Instructions

- Individuals have the right to withhold or withdraw consent to the collection, use or disclosure of their personal health information for health care purposes
- Individuals also have the right to provide express instructions to health information custodians not to use or disclose personal health information for health care purposes without consent in the circumstances set out in sections 37(1)(a), 38(1)(a) and 50(1)(e) of the *Act*
- These provisions are referred to as the "lock-box" provisions although the term "lock-box" is not used in the *Act*

Withholding and Withdrawing Consent and Express Instructions (cont'd)

- A health information custodian is not required to comply with a lock-box request where the:
  - Use or disclosure is permitted or required to be made without consent, except as set out in section 37(1)(a), 38(1)(a) and 50(1)(e) of the *Act*
  - Effect is to prohibit or restrict the recording of personal health information by a health information custodian that is required by law or by established standards of professional or institutional practice

Other Factors to be Considered in Relying on Assumed Implied Consent

- In general, health information custodians may not:
  - Collect, use or disclose personal health information if other information will serve the purpose; or
  - Collect, use or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure
- These provisions continue to apply when health information custodians rely on assumed implied consent

Alternatives When Consent Cannot be Assumed to be Implied

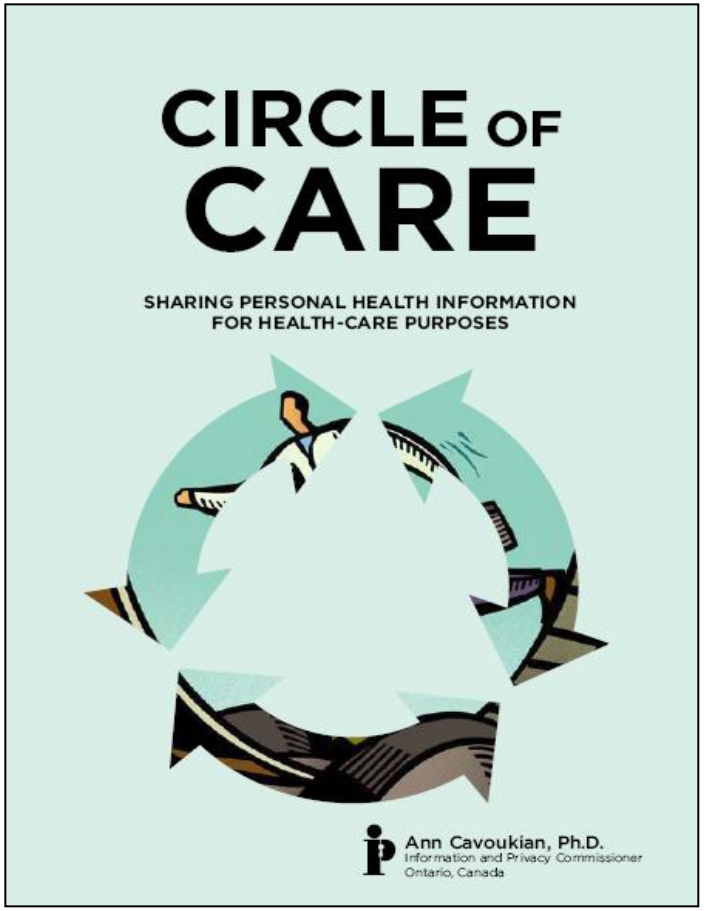
- When consent cannot be assumed to be implied, a health information custodian should consider whether:
  - The collection, use or disclosure is permitted or required by *the Act* to be made without consent
  - Consent is permitted to be implied
  - Express consent of the individual is required

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

The Perils of EMRs

- If privacy is not embedded into their design, EMRs (Electronic Medical Records) pose unique risks to the privacy of individual;
- Allow for the collection, use and disclosure of large amounts of personal health information from diverse sources;
- May attract hackers and others with malicious intent;
- Increases the risk of health care providers accessing personal health information for unauthorized purposes;
- Easier to transfer personal health information to a portable device and remove the information from a secure location.

Data Sharing Agreements

What is a Data Sharing Agreement?

- A "**data sharing agreement**" (DSA) is an agreement that sets out terms for the sharing of personal health information
- Often used to establish EMRs or electronic health records (EHRs)
- Parties to a DSA may include HICs, hospitals, and service providers
- Governs accountability for maintaining the security and privacy of the information, and clarifies ownership, custody, access, storage, copying, and transferring of data

Typical DSA Terms

They may set out:

- Ownership of PHI/Data stewardship
  - The HIC should remain the owner of the records of PHI;
- Confidentiality and privacy
  - It should reflect obligations under policies and legislation;
- Which custodians (and their agents) will have access to the EMR and to what PHI they will have access;
- How and in what circumstances will the PHI in the EMR be disclosed for research, analysis and public health surveillance purposes.

Typical DSA Terms cont.

The terms should clarify who will be responsible for:

- Responding to complaints and inquiries;
- Responding to requests for access and correction;
- Identifying, containing, investigating and remediating privacy breaches and notifying affected individuals;
- Implementing, modifying and auditing the implementation, modification and overriding of consent directives;
- Ensuring appropriate safeguards are in place;
- Auditing any time personal health information is viewed, handled or otherwise dealt with.

Typical DSA terms cont.

In reflecting PHIPA, the terms should expressly prohibit:

- Unauthorized access to and use of PHI

With a view to implementing reasonable security, as required by PHIPA, the terms should require:

- The use of protective mechanisms such as unique user names and passwords;
- That the roles and responsibilities in regard to the security of the system be set out e.g. backups of PHI, disaster recovery procedures, documentation, performance expectations, and support and maintenance obligations.

Typical DSA terms cont.

Termination of the agreement

- Set out what happens to the records after the agreement ends or when a HIC or physician withdraws;
- Remember that section 42 of PHIPA permits a custodian to transfer records of PHI to a custodian's successor, if the custodian notifies the individual to whom the information relates;
- The agreement should discuss what will happen in the event of a dispute between the parties e.g. you may want to include a clause requiring arbitration.

Helpful Resources

The following resources contain chapters that discuss DSAs:

- The IPC's *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*
  - *http://www.ipc.on.ca/images/Findings/process.pdf*
- The Canadian Medical Protective Association's *Electronic Records Handbook*
  - *https://oplfrpd5.cmpa-acpm.ca/documents/10179/24937/com_electronic_records_handbook-e.pdf*

Privacy Breaches

What is a Privacy Breach

- A **privacy breach** occurs whenever a person has contravened a provision of *PHIPA* or its regulations, including section 12(1) of *PHIPA*.
- Section 12(1) of *PHIPA* requires HICs to take steps that are reasonable in the circumstances to ensure PHI in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.
- Only those breaches where PHI is stolen, lost, or accessed by unauthorized persons result in notifications under section 12(1).

Types of Privacy Breaches

'Here's an unusual one, Wayne: Gentleman says he's lost an umbrella.'

Failure to Securely Dispose of PHI

Order HO-001

- A clinic hired a waste disposal company to shred old records of PHI, but due to a misunderstanding, the records were given to a recycling company instead of being shredded
- The recycling company sold the records to a special effects company and were used as props in a film shoot in downtown Toronto

Order HO-003

- A clinic, operated by a corporation, closed prior to the expiration of its lease
- The landlord of the property leased by the clinic discovered three shopping carts full of PHI records

Order HO-006

- Employees of a laboratory put records of PHI in boxes designated for recycling as opposed to those designated for shredding
- The boxes designated for recycling were located immediately beside the boxes designed for shredding
- The records of PHI were found scattered on the street outside of the laboratory

What the IPC Ordered

With a view to preventing further breaches, here are some of the things the IPC ordered the custodians to do:

- Appoint a staff member to facilitate compliance with the Act;
- Retain, transfer and dispose of records in a secure manner and document that secure manner;
- Health practitioners in a group practice must enter into a written agreement with the custodian that outlines the obligations of all parties in regard to the records of PHI;
- In the event of a closure of the group practice, make available to individuals a written statement describing how records will be retained or disposed of and how an individual may obtain access to or transfer their records of PHI

What the IPC Ordered cont.

When using a record storage or disposal company, ensure that agreements are in place setting out:

- The requirement to securely store records prior to disposal;
- The obligation for secure disposal, including how the records will be disposed of (i.e. in such a way that reconstruction is not foreseeable), under what conditions and by whom.
- The requirement to provide a signed attestation or certificate of destruction once secure disposal has been conducted. The document must confirm the date, time and location of the destruction as well as the name and signature of the operator who performed the secure destruction.

Unauthorized Access to PHI

Order HO-010

- A patient complained that an employee of the hospital, the former spouse of her current spouse, had inappropriately accessed her PHI records
- The hospital ordered an audit of access to the records
- The audit revealed that the patient's records were accessed by the employee on six different occasions
- The employee was not involved in providing health care to the patient

Lost or Stolen Device Containing PHI

- **Order HO-004**
  - Theft of a laptop left in a physician's vehicle containing the unencrypted PHI records of 2,900 individuals. (He was taking it home to analyze it/conduct research.)
- **Order HO-007**
  - Loss of a USB memory stick being transported by a nurse containing the unencrypted PHI records of 83,524 individuals
- **Order HO-008**
  - Theft of a laptop left in a nurse's vehicle containing the unencrypted PHI records of 20,000 individuals

Information Practices

The IPC required the custodians to create new information practices, which were to include:

- A policy prohibiting the removal of identifiable PHI from the premises to the extent possible. If it must be removed in electronic form, it must be encrypted;
- An electronic devices policy mandating that any PHI not stored on secure servers must be de-identified or encrypted;
- A policy relating to the use of secure remote access and/or Virtual Private Networks as an alternative to using laptop computers; and
- A privacy breach protocol/policy.

Encryption!

"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

Last, but not Least

In several IPC Orders, including HO-004 and HO-008, the training of staff, researchers and/or clinicians was found to be inadequate, contrary to s.15(3)(b). Accordingly, the custodians were to ensure that education was provided, in particular, in regard to:

- Risks associated with the use of laptop computers;
- How to secure the information contained on laptop computers;
- New policies of the custodian.

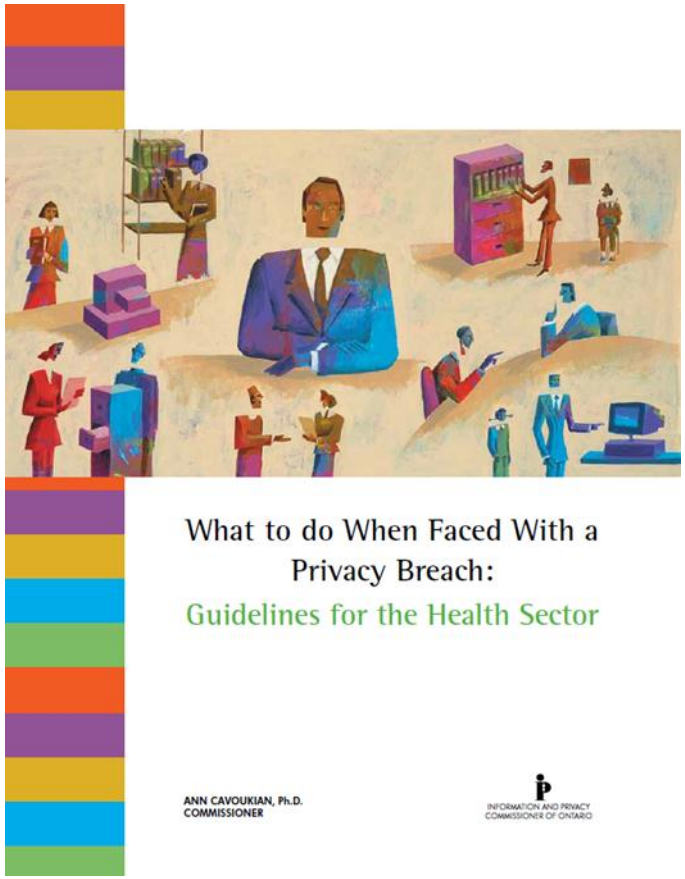
Such training is to occur on a regular and recurring basis.

What to do in the Event of a Breach

- **Containment**: Identify the scope of the potential breach and take steps to contain it
- **Notification**: Identify those individuals whose privacy was breached and notify them of the breach
  - **Note**: section 12(2) of *PHIPA* requires that a HIC notify an individual ***at the first reasonable opportunity*** if the individual's PHI is stolen, lost or accessed by unauthorized persons
- **Investigation and Remediation**
- Many organizations have in place a "**privacy breach protocol**" which sets out procedures for immediately responding to a potential breach

What to do in the Event of a Breach

For more information, see the following IPC brochure: *What to do When Faced with a Privacy Breach: Guidelines for the Health Sector*



http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=433

Questions…?

Contact us:

Information and Privacy Commissioner/Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416-326-3333

Toll Free: 1-800-387-0073

www.ipc.on.ca or

info@ipc.on.ca