Safeguarding PHI under the Personal Health Information Protection Act, 2004

A Presentation to the Association of Ontario Midwives

December 2, 2015

Judith Goldstein
Legal Counsel
Information and Privacy Commission

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 NOT LEGAL ADVICE.

PHIPA- What is it?

- Made in Ontario Health Privacy Legislation
- It was declared substantially similar to the federal *PIPEDA* in 2005
- Provides rules for the collection, use and disclosure of PHI
- Provides individual with a right of access and correction to their PHI with limited exceptions

Why do we need it?

- It replaced a hodgepodge of rules governing the handling of PHI in the healthcare sector.
- Beyond patient care, PHI is needed for activities such as health research and analysis and these kinds of activities are also regulated by PHIPA.
- For constitutional reasons, PIPEDA could only regulate the handling of personal information, which was being used in *the course of commercial activities*.

Application of PHIPA

It applies mainly to Health Information Custodians (HICs). Some examples of HICs are:

- Persons who operate:

  Private or public hospitals, independent health facilities, pharmacies and labs;

- Community care access corporations; and
- Health care practitioners or persons who operate a group practice of health care practitioners.

What Must HICs Do?

Take reasonable precautions to safeguard PHI including:

- Protecting against theft or loss, unauthorized use, disclosure, copying, modification or destruction; and
- Notifying an individual at the first reasonable opportunity if the information is stolen, lost or accessed by an unauthorized person.
- Ensuring records are accurate, up-to-date and complete as necessary for their purposes;
- Ensuring records are stored, transferred and disposed of in a secure manner.
- Designating or taking on the role of a contact person.

What Must Agents Do?

- If you're an agent, for example of a group practice, you don't have all the responsibilities of a health information custodian; your main responsibilities are set out in section 17.
- You may only collect, use, disclose, retain or dispose of PHI on the custodian's behalf if the custodian would be permitted to do so.
- If the collection etc. is in the course of your duties and not contrary to limits imposed by the custodian, PHIPA or another law; and
- You must notify the custodian at the first reasonable opportunity if PHI is stolen, lost or accessed by unauthorized persons.

What are Information Practices?

They are the policy of the custodian for actions in relation to PHI, including:

- When, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
- The administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information.

The information practices must comply with the *Act* and the regulations.

Information Practices *cont.*

A custodian must:

- A custodian must make available to the public a written statement that provides a general description of its information practices; and

- Inform the individual if PHI is used or disclosed without consent, in a manner outside of the scope of the information practices.


mac
WWW.DAILYMAIL.CO.UK
LOST PROPERTY
GOVERNMENT LAPTOPS
BANKING LAPTOPS
'Here's an unusual one, Wayne: Gentleman says he's lost an umbrella.'

Inadvertent Breaches

Reasonable Steps to Protect PHI?

Order HO-001 – Improper Disposal

- 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 they were used as props in a film shoot and ended up scattered on the streets of Toronto.

Lessons Learned

- Have a written agreement that outlines the obligations of all parties in regard to PHI. Require secure storage prior to disposal. Set out how records will be disposed of, under what conditions and by whom. Obtain a certificate of destruction, confirming the date, time, location of destruction and the signature of the operator who performed the secure destruction.
- Secure disposal means that reconstruction is not foreseeable i.e. cross-cut shredding or pulverization for paper records; physically damaging and discarding electronic media or, if re-using the media, using wiping utilities.

Reasonable Steps to Protect PHI?

Order HO-004

- Theft of a laptop left in a physician's vehicle containing unencrypted PHI records of 2,900 individuals. (He was taking it home to analyze it/conduct research.)

Order HO-007

- Loss of 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.

Lesson Learned

- In all of the cases on the previous slide it was found that custodians did not take steps that were reasonable in the circumstances to retain the PHI in a secure manner and to protect it against all kinds of hazards such as loss or theft.
- The IPC required the custodians to create new information practices including:
  - Prohibiting the removal of PHI from the premises to the extent possible; If it must be removed in electronic form, it must be encrypted
  - PHI not stored on secured servers must be de-identified or encrypted.
  - A privacy breach protocol/policy

Deliberate Breaches

Snooping into Medical Records

Ontario Snooping Cases

Order HO-002

- A registered nurse accessed the records of the estranged spouse of her boyfriend
- The records were accessed over a six-week period

Order HO-010

- A diagnostic imaging technologist accessed the records of the current spouse of her former spouse
- The records were accessed on six occasions over nine months

Order HO-013

- Two employees accessed records to market RESPs

Lessons Learned?

- 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 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
- Provide privacy resources for staff

An Option for Midwives

Section 14 of PHIPA permits a midwife, who is a custodian, to keep a record of PHI in an individual's home (and elsewhere even in a place that is not under the control of the midwife) if:

- the record is kept in reasonable manner;
- the individual consents;
- the midwife is permitted to keep the records in that place in accordance by-laws or guidance under the RHPA, or an Act referred to in Schedule I of the RHPA, and prescribed conditions are satisfied.

Note that PHIPA's regulation currently does not prescribe conditions in regard to storage at someone's home.

The Lock-Box

- Since PHIPA is consent-based, individuals may withhold or withdraw their consent to collect, use or disclose their PHI, for purposes that require express or implied consent.
- Lock-box requests may be implemented by technological means or a combination of policies, procedures, manual processes and technological means such as flagging electronic or paper files or sealed envelopes noting the lock.

Disclosure to Prevent Serious Harm

- A custodian or an agent of a custodian may disclose personal health information if the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

- This includes serious harm to the patient herself.

- It has also been judicially interpreted as including psychological harm.

The Lock-Box cont'd

Something to Ponder in Your Context:

- The section refers to harm to a "person or group of persons".

- The safety of a fetus would not appear to be a relevant consideration when considering whether to disclose without consent to prevent harm as a fetus is not considered to be legally a person until it has entirely emerged from its mother's body.

Access to Information

- Individuals or their substitute decision makers have a right of access to their PHI in the custody or control of HICs
- PHIPA is not a general access statute
- No general right of access to the PHI of others, even that of people's own children. a spouse's pregnant wife or prospective adoptive parents.

Access to a Child's PHI

- With some exceptions (not relevant to midwifery), a parent may consent to the disclosure of their child's PHI, where the child is less than 16 years old. [Section 23(1)2)]

- Therefore such a parent may obtain access to the PHI of their child under PHIPA.

- A "parent", for purposes of the above, must be a custodial parent, not a parent who only has a right of access to the child.

Questions?

If you have questions later, you can:

- Submit them to Info@ipc.on.ca; or
- Call: 1-800-387-0073 and ask to speak to our Communications people.
- Search our web site: www.ipc.on.ca