REACHING OUT TO ONTARIO

Debra Grant
Director of Health Policy, IPC
&
Manuela Di Re
Director of Legal Services, IPC

Protecting Health Information

Western University, London

September 27, 2016

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

www.ipc.on.ca

Bill 119
Health Information Protection Act, 2015

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

Overview

- The Bill was introduced on September 16, 2015
- All the provisions in the Bill 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

Summary of the Provisions Proclaimed Into Force

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

Summary of the Provisions Proclaimed

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"
- Amendments to the provisions related to prosecution of offences under *PHIPA*

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

Notification and Report of Breaches

- 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

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

Prosecution of Offences

- 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

Summary of Provisions Related to Provincial Electronic Health Record Not Proclaimed

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

REACHING OUT TO ONTARIO

Summary of Provisions Related to the Provincial Electronic Health Record

- Part V.1 of the Bill has not been proclaimed and will apply to the provincial electronic health record (provincial EHR)
- It will **not apply** to local electronic medical record systems, hospital information systems or shared electronic health record systems other than the provincial EHR
- In respect of the provincial EHR, Part V.1 will:
  - Define and set out rules for collection, use and disclosure
  - Establish processes for the implementation of consent directives
  - Establish processes for individuals to access and correct their records of personal health information

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

Rules for Collection, Use and Disclosure

- In general, health information custodians can only collect personal health information from the provincial EHR:
  - To provide or assist in the provision of health care to the individual to whom the information relates, or
  - If have reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm
- If collected to provide or assist in provision of health care, it may be used or disclosed for any purpose permitted by *PHIPA*
- If collected to prevent a significant risk of serious bodily harm, it may only be used and disclosed for this purpose

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

Consent Directives and Overrides

- Individuals will have the right to implement a directive to withhold or withdraw consent to the collection, use or disclosure of their information for health care purposes
- The individual must submit the directive to a prescribed organization that is responsible for implementing the directive
- Health information custodians can override a directive:
  - With express consent
  - If there are reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm to the individual or another person, but if to the individual must also establish not reasonably possible to get timely consent

Consent Directives and Overrides

- Personal health information collected through an override may only be used or disclosed for the purpose it was collected
- Consent overrides will be audited and monitored and written notice of the override will be immediately provided to the health information custodian who collected the information
- The health information custodian must then notify the individual of the consent override and, in certain circumstances, must also notify the IPC

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

Potential Causes of Privacy Breaches

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

1. Lack of Clarity Regarding Responsibilities in Shared Systems

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

Reaching out to Ontario

Challenges Posed by Shared Electronic Health Record Systems

- Custodians may have custody or control of personal health information they create and contribute to, or collect from, shared electronic health record systems but
- No custodian has sole custody and control
- All participating custodians and their agents will have access to the personal health information
- The unique characteristics of shared electronic health record systems pose unique privacy risks and challenges for compliance with *PHIPA*

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

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

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

Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies and procedures should address:

- Privacy training
- Privacy assurance
- Logging, auditing and monitoring
- Consent management
- Privacy breach management
- Privacy complaints and inquiries management
- Access and correction
- Governance

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

2. Unauthorized Access

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

Meaning of Unauthorized Access

- Unauthorized access is when a custodian or an agent views, handles or otherwise deals with personal health information without consent and for purposes not permitted by *PHIPA*, for example:
  - When not providing or assisting in the provision of health care to the individual; and
  - When not necessary for the purposes of exercising employment, contractual or other responsibilities
- The act of viewing personal health information on its own, without any further action, is an unauthorized access

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

Examples of Unauthorized Access – Education and Quality Improvement

- There have been a number of instances where custodians or agents accessed personal health information claiming it was for:
  - Their own educational purposes
  - To improve the quality of the health care they provide
  - Other uses permitted by *PHIPA*
- Demonstrating this access is unauthorized is often difficult

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

Challenges in Establishing "Unauthorized" Access

- Demonstrating such accesses are unauthorized may be difficult where the custodian does not:
  - Have clear policies specifying the purposes for which access is and is not permitted
  - Have procedures that must be followed when accessing information for purposes other than providing care
  - Inform agents what access is permitted and is not permitted, including through training, notices, flags, agreements, etc.

Consequences of Unauthorized Access

- Review or investigation by privacy and other oversight bodies
- Prosecution for offences
- Statutory or common law actions
- Discipline by employers
- Discipline by regulatory bodies

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

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

Offences

- It is an offence to wilfully collect, use or disclose personal health information in contravention of *PHIPA*

- To date, five matters have been referred for prosecution

2011

- A nurse at North Bay Health Centre

2015

- Radiation therapists at the University Health Network

2015

- A social worker at a family health team

2016

- A registration clerk at a regional hospital

2016

- A regulated professional at a Toronto hospital

Successful Prosecutions

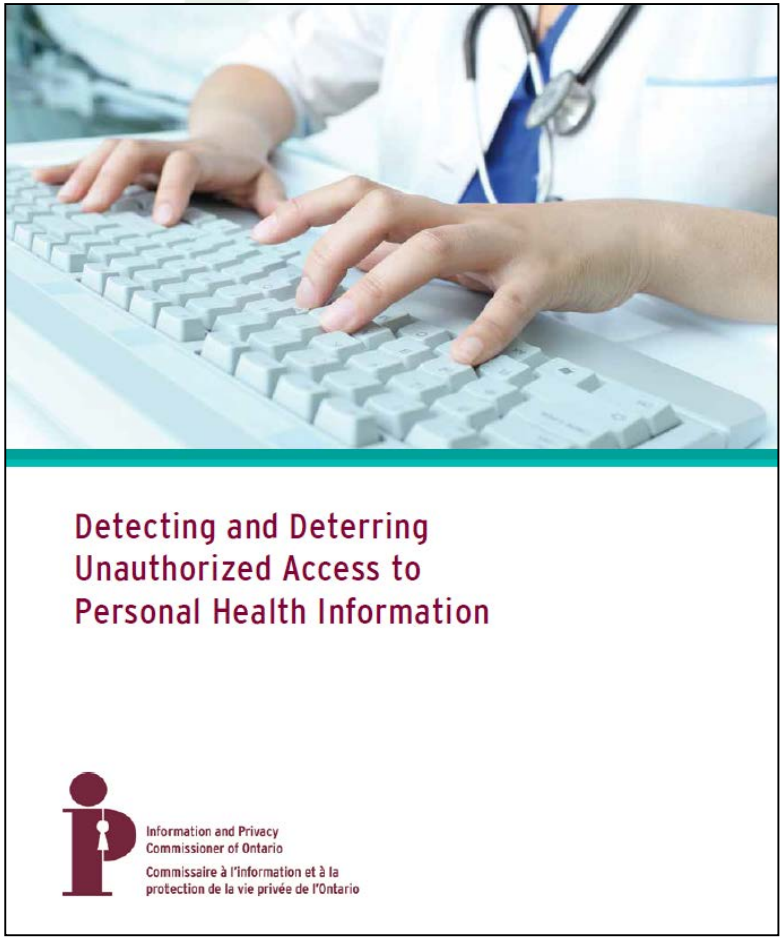
- The two radiation therapists pled guilty to wilfully collecting, using or disclosing personal health information in contravention of the *Act*, each was fined $2000
- The registration clerk pled guilty to one charge of willfully collecting, using and disclosing personal health information in contravention of the *Act* and was fined $10,000
- These are the first successful prosecutions under *PHIPA*

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

REACHING OUT TO ONTARIO

New 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

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

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
TDD/TTY: 416-325-7539
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca
Media: media@ipc.on.ca / 416-326-3965