PROTECTING HEALTH INFORMATION IN AN ELECTRONIC ENVIRONMENT

Ontario Bar Association
Health Law Section

Brian Beamish

Information and Privacy Commissioner

June 15, 2015

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

The Promise of Electronic Records

- Facilitate more efficient and effective health care and improve the quality of care provided
- Accessible by all health care providers involved in the care of an individual, regardless of location
- More complete than paper records - not spread over a wide range of health care providers
- Easier to read and locate
- Can enhance privacy, i.e. through access controls, audit logs and strong encryption

The Peril of Electronic Records

- If privacy is not built into their design and implementation, electronic records pose unique risks to privacy
- Easier to transfer or remove personal health information from a secure location
- May attract hackers and others with malicious intent
- Increases the risk of authorized individuals accessing information for unauthorized purposes

Consequences of Inadequate Attention to Privacy

- Discrimination, stigmatization and psychological or economic harm to individuals based on their health information
- Individuals being deterred from seeking testing or treatment
- Withholding or falsifying information provided to health care providers
- Loss of trust or confidence in the health system
- Costs and lost time in dealing with privacy breaches
- Legal liabilities and ensuing proceedings

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

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

Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies and procedures should address:

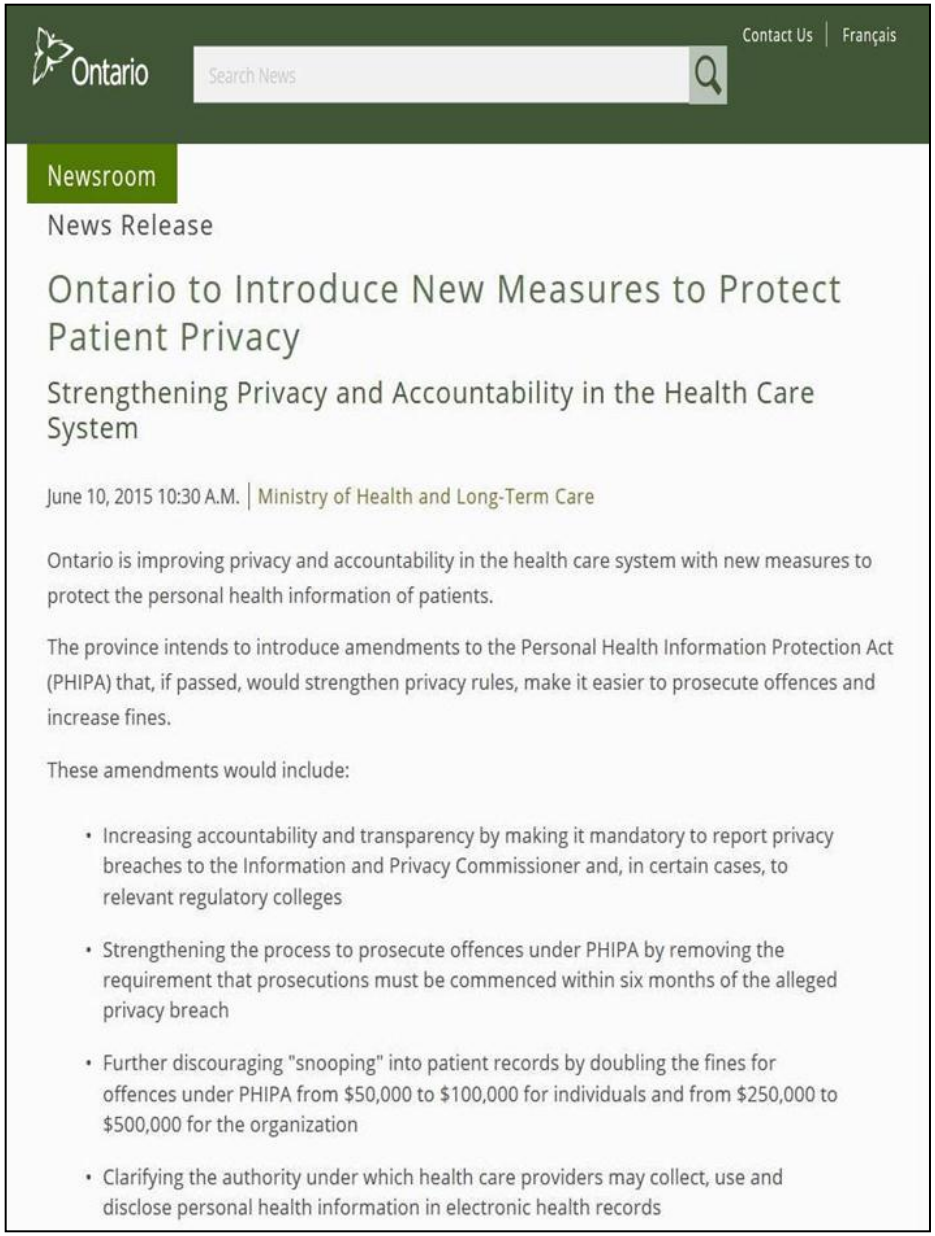
- Privacy training
- Privacy assurance (i.e. privacy readiness assessments)
- Logging, auditing and monitoring
- Consent management
- Privacy breach management
- Privacy complaints and inquiries management
- Access and correction

Recommendation in Support of *ePHIPA* from Our 2014 Annual Report

Recommendation

EHRs have the potential to improve treatment, enhance safety, and facilitate the coordination of services, resulting in a more efficient and effective health-care system. Over the coming years, Ontario's health-care system will need to adapt to rapid changes in technology, including EHRs. Consequently, there is a growing need for a legislative framework to address PHI in an increasingly digital and interconnected world.

While *PHIPA* has served Ontario admirably over the last decade, it does not adequately address the rights of individuals and the duties of HICs in an EHR environment. The IPC recommends that the government re-introduce the *Electronic Personal Health Information Protection Act*. This legislation will amend *PHIPA* to clarify how the privacy of patients and the confidentiality of their PHI will continue to be protected as the health-care sector transitions to electronic systems.



Ontario

Search News

Contact Us | Français

Newsroom

News Release

Ontario to Introduce New Measures to Protect Patient Privacy

Strengthening Privacy and Accountability in the Health Care System

June 10, 2015 10:30 A.M. | Ministry of Health and Long-Term Care

Ontario is improving privacy and accountability in the health care system with new measures to protect the personal health information of patients.

The province intends to introduce amendments to the Personal Health Information Protection Act (PHIPA) that, if passed, would strengthen privacy rules, make it easier to prosecute offences and increase fines.

These amendments would include:

- Increasing accountability and transparency by making it mandatory to report privacy breaches to the Information and Privacy Commissioner and, in certain cases, to relevant regulatory colleges
- Strengthening the process to prosecute offences under PHIPA by removing the requirement that prosecutions must be commenced within six months of the alleged privacy breach
- Further discouraging "snooping" into patient records by doubling the fines for offences under PHIPA from $50,000 to $100,000 for individuals and from $250,000 to $500,000 for the organization
- Clarifying the authority under which health care providers may collect, use and disclose personal health information in electronic health records

"No matter where people receive care, they deserve to know that they are protected by a health care system that is accountable and keeps their personal health information private. By increasing fines and requiring that privacy breaches are reported to the Information and Privacy Commissioner, we can help strengthen patient privacy and improve our health care system. If passed, these changes will strengthen Ontario's position as the nation-wide leader in protecting patient privacy."

Dr. Eric Hoskins

Minister of Health and Long-Term Care

Unauthorized Access

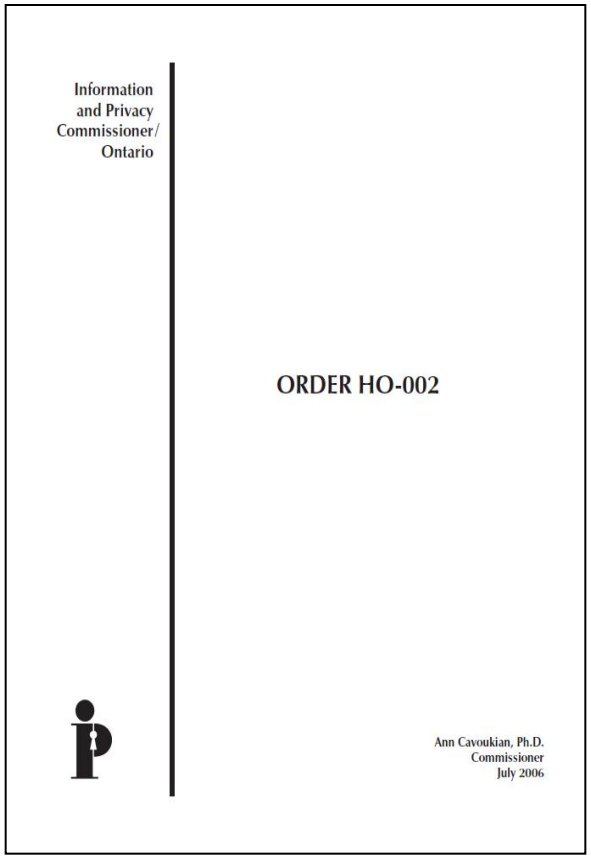
Meaning of "Unauthorized Access"

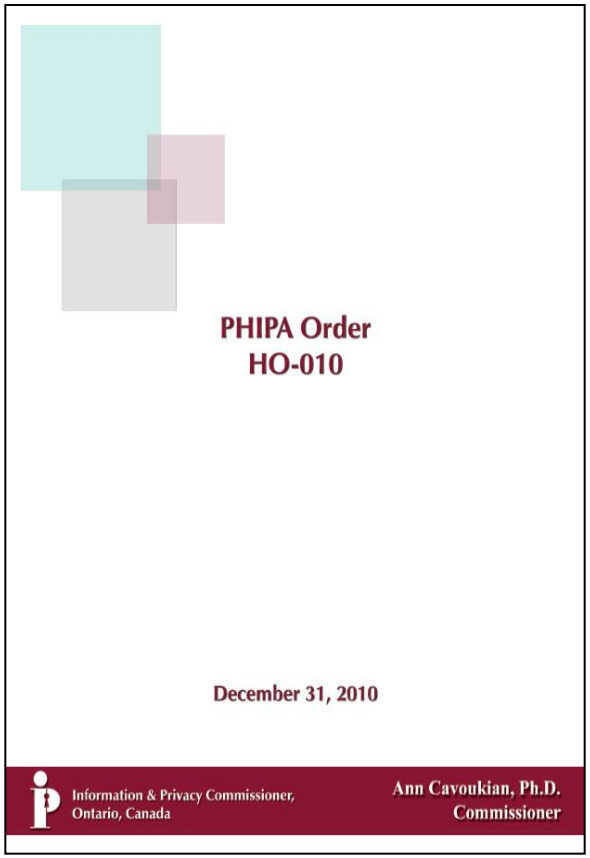
- Accessing PHI without consent and for purposes not permitted by *PHIPA*, for example:
  - When not providing or assisting in the provision of health care to the individual; and
  - When not necessary for the purposes of exercising employment, contractual or other responsibilities
- "Snooping" includes "only" viewing PHI

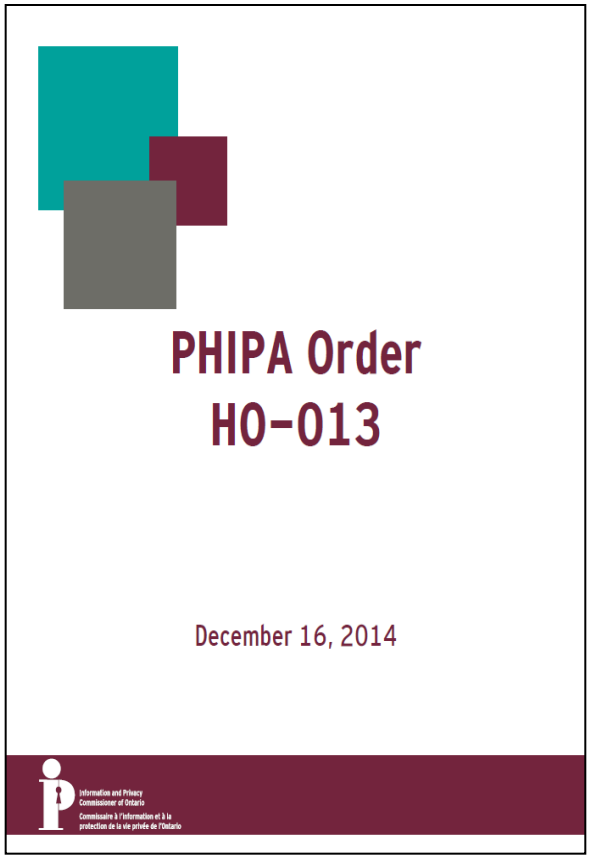
Sanctions for Unauthorized Access

- Discipline by employers
- Discipline by regulatory bodies
- Investigation by privacy oversight bodies
- Prosecution for offences
- Statutory or common law actions

Orders Issued by the IPC







Examples from Other Jurisdictions—Alberta

Investigation Report H2011-IR-004

- Physician used Alberta Netcare to view the records of a partner's former spouse and the mother and girlfriend of the partner's former spouse
- Records viewed on 21 occasions over a 15 month period
- Accessed for a divorce and custody dispute
- Accounts of colleagues who failed to log out of Alberta Netcare used
- Employer reprimand, college suspension, costs

Examples from Other Jurisdictions—Saskatchewan

Investigation Report H-2010-001

- Pharmacist used the Pharmaceutical Information Program, a domain repository in Saskatchewan's electronic health record, to view drug profiles of three individuals on nine occasions after a business arrangement with the individuals dissolved

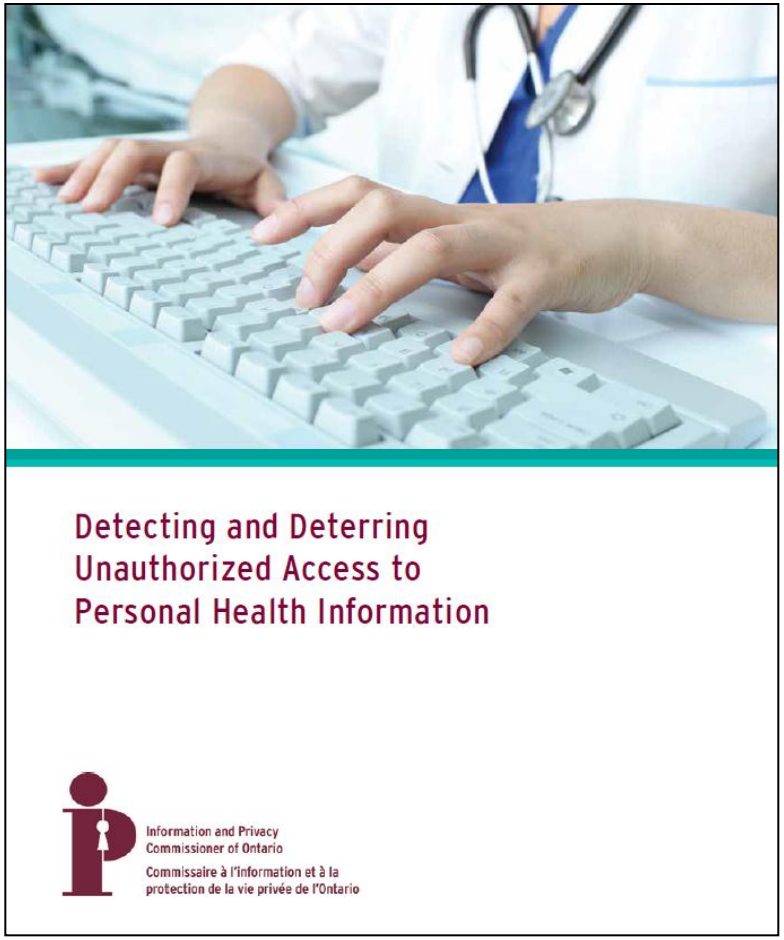
Investigation Report H-2013-001

- Employees of Regina Qu'Appelle Regional Health Authority viewed their own health information, viewed and modified the health information of other employees and viewed the health information of other individuals

Detecting and Reducing the Risk of Snooping

- Clearly articulate the purposes for which employees, staff and other agents may access PHI
- 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 PHI
- Impose appropriate discipline for unauthorized access

New Guidance Document: Detecting and Deterring 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

thestar.com
CRIME

Hospital staff, financial reps charged in patient RESP scheme

Charges have been laid against two hospital staff members who stole hospital patient records and the three financial executives who bought them.

By: Marco Chown Oved Staff Reporter, Published on Tue Jun 02 2015

One year after the Star revealed that staff at Rouge Valley hospital had sold the confidential patient informationof thousands of new mothers to financial corporations, Ontario's securities regulator has finally named the companies and sales representatives involved and laid 12 charges against them.

The criminal and securities charges are the most serious consequences any health professional has faced for a privacy breach, and come days after the provincial privacy watchdog called for a criminal crackdown.

Prosecution

Offence Provisions

- *PHIPA* creates offences for contravention, including an offence for wilfully collecting, using or disclosing PHI in contravention of *PHIPA*
- Limitation period for commencing a prosecution is six months ***from the date of the offence***
- The Attorney General **not** the IPC is responsible for commencing prosecutions
- On conviction, an individual may be liable for a fine of up to $50,000 and a corporation of up to $250,000

Three Referrals for Prosecution

- **2011** – Nurse at North Bay Health Centre. Case was dismissed due to an unreasonable delay in getting to trial

- **2015** – Two healthcare professionals at the University Health Network snooping Rob Ford's medical records

- **2015** – Breaches involving a family health team.

Examples from Other Jurisdictions - Alberta

Prosecution in 2007

- A medical office clerk plead guilty and was fined $10,000 under the *Health Information Act*
- She accessed, on six different occasions, the information of the wife of a man with whom she was having an affair

Prosecution in 2011

- A pharmacist plead guilty and was fined $15,000 under the *Health Information Act*
- She used Alberta Netcare to access the records of a number of women who attended her church and posted the prescription information of some of the women on Facebook

Examples from Other Jurisdictions - Alberta

Prosecution in 2014

- A medical laboratory assistant received a four month conditional sentence, eight months probation and a $500 fine
- Accessed the PHI of 34 individuals in contravention of the *Health Information Act* and uttered forged documents in contravention of the *Criminal Code*

Referrals for Prosecution in 2015

- On April 16, 2015, fourteen charges were laid against an individual and on April 23, 2015 eight charges were laid against another individual for gaining access to health information in contravention of the *Health Information Act*

Examples from Other Jurisdictions - Newfoundland and Labrador

Prosecution in September 2014

- An employee of Western Health pleaded guilty and was fined $5000 under the *Personal Health Information Act*
- Accessed PHI for unauthorized purposes on 75 occasions within a span of less than one month

Prosecution in October 2014

- A nurse employed by Eastern Health was found guilty and fined $1000 under the *Personal Health Information Act*
- Accessed PHI for unauthorized purposes on 18 occasions over a one year period

Expected PHIPA Amendments

- Mandatory reporting of breaches to the IPC and relevant regulatory colleges
- Facilitating prosecutions by removing the six month limitation period
- Doubling fines for offences to $100,000 for individuals and $500,000 for organizations

Actions

Statutory Actions

- A person affected by a **final order** issued by my office may commence a proceeding for damages for actual harm suffered as a result of the contravention of *PHIPA*
- A person affected by conduct that gave rise to a **conviction for an offence** under *PHIPA* that is final may commence a proceeding for damages for actual harm suffered
- Where the harm was caused wilfully or recklessly, an amount not exceeding $10,000 for mental anguish may be awarded

Common Law Actions – Tort of "Intrusion Upon Seclusion"

- In *Jones* v. *Tsige*, the Court of Appeal recognized a new common law cause of action for the **tort of intrusion upon seclusion**
- There are three required elements of the cause of action:
  - Intentional or reckless conduct
  - Unjustified invasion into the plaintiff's private affairs or concerns
  - Highly offensive conduct causing distress, humiliation or anguish
- Proof of actual loss is not one of the required elements
- Damages will "ordinarily be measured by a modest conventional sum," generally to a maximum of $20,000

Common Law Actions – Health Context

- *Hopkins v. Kay* is the first court decision in Ontario to apply the tort of intrusion upon seclusion to the health sector
- The hospital argued that *PHIPA* was an "an exhaustive code that ousts the jurisdiction of the Superior Court to entertain any common law claim for invasion of privacy."
- The Ontario Court of Appeal rejected this argument
- Leave to appeal to the Supreme Court has been sought

Common Law Actions – Health Context

- *Hopkins v. Kay* has been relied upon by courts outside Ontario to find that actions for privacy breaches should not be dismissed at the pleadings stage:
  - *Condon v. Canada,* 2014 FC 250 cites the trial decision in *Hopkins* to support certification of a class action relating to a lost hard drive containing personal information of student loan recipients
  - *Grant v. Winnipeg Regional Health Authority et al.,* 2015 MBCA 4: cites the Court of Appeal decision in *Hopkins* in support of a claim by the sister of the deceased alleging disclosure of the deceased's confidential patient information

PHIPA Process Review

- 10+ years of experience handling PHIPA complaints
- Volume of complaints will continue to increase with no expectation of increased resources
- Are changes to our processes required for efficiency, fairness, consistency?
- Are IPC processes transparent enough to the public/custodians?
- Can we do a better job of providing precedents and guidance through our tribunal function (e.g. are 13 orders in 10 years enough?)

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