Preventing Privacy Breaches and Building Confidence in Electronic Health Records

Brian Beamish

Commissioner (Acting)

Ontario Information and Privacy Commission

Cyber Risk National Conference

February 9, 2015

Information and Privacy Commissioner of Ontario

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

Mandate and Role

- The Office of the Information and Privacy Commissioner of Ontario (IPC) provides an independent review of government decisions and practices concerning access and privacy.
- The Commissioner is appointed by and reports to the Legislative Assembly while remaining independent of the government of the day to ensure impartiality.

Oversees Three Acts

- ***Freedom of Information and Protection of Privacy Act (FIPPA)***; and the ***Municipal Freedom of Information and Protection of Privacy Act (MFIPPA):***
  - Provides right of access to information and appeals to the IPC.
  - Privacy complaints may be filed with IPC – investigations may result in recommendations or orders.
- ***Personal Health Information Protection Act (PHIPA)***:
  - Provides comprehensive privacy protections for personal health information; right of access to personal health information, and a right to complain to the IPC.

Importance of Protecting Personal Health Information

Unique Characteristics of Personal Health Information

- Highly sensitive and personal in nature.
- Must be shared immediately and accurately among a range of health care providers.
- Widely used and disclosed for secondary purposes seen to be in the public interest (e.g., research, operational planning).
- Dual nature is reflected in *PHIPA*.

Consequences of Inadequate Attention to Privacy

Consequences for Individuals

- Discrimination, stigmatization, psychological harm.
- Deterred from seeking testing or treatment.
- Withhold or falsify information.
- Loss of trust or confidence in the health care provider.
- Loss of confidence in electronic health records

Consequences for Health Information Custodians and their Agents

- Suspension or termination.
- Disciplinary action.
- Damage to reputation.
- Lost time and expenditure of resources.
- Legal liabilities and ensuing proceedings.

Common Causes of Breaches Related to Electronic Records

Health Orders concerning 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 memory stick 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 Prevent This Type of Breach

- **STOP** and ask, *Do I really need to store personal health information on this device?*
- **THINK** about alternatives:
  - De-identify or code information.
  - Use remote access through a secure connection.
- **PROTECT** the information on mobile devices:
  - Encrypt and protect with strong passwords.
  - Carry the least amount of identifying information.
  - Have policies and procedures, training and audits.

Unauthorized Access to Electronic Records

The Meaning of "Unauthorized Access"

- There have consistently been cases of "unauthorized access" in Ontario where health records have been accessed without consent and for purposes not permitted by *PHIPA*.
- Unauthorized access includes viewing PHI.
- This problem becomes more acute with the growth of electronic health records.

Order HO-002
The Story

- A patient told a hospital that her estranged husband and his girlfriend were employees and she did not want them to know she was a patient.
- The girlfriend, a nurse who was not involved in the health care of the patient, viewed the patient's record on numerous occasions.

Order HO-002
The Outcome

The hospital was ordered to:

- Review and revise its practices and procedures relating to personal health information and privacy.
- Implement a protocol to cease unauthorized access upon notification of a breach.
- Ensure that staff and agents are informed of their duties under *PHIPA*, and any revised information practices.
- Issue an apology to the patient.

Order HO-010
The Story

- A patient complained to a hospital that an employee inappropriately accessed their records.
- The employee was the former spouse of the patient's current spouse.
- An audit revealed that the records of the patient were accessed by the employee on six separate occasions.

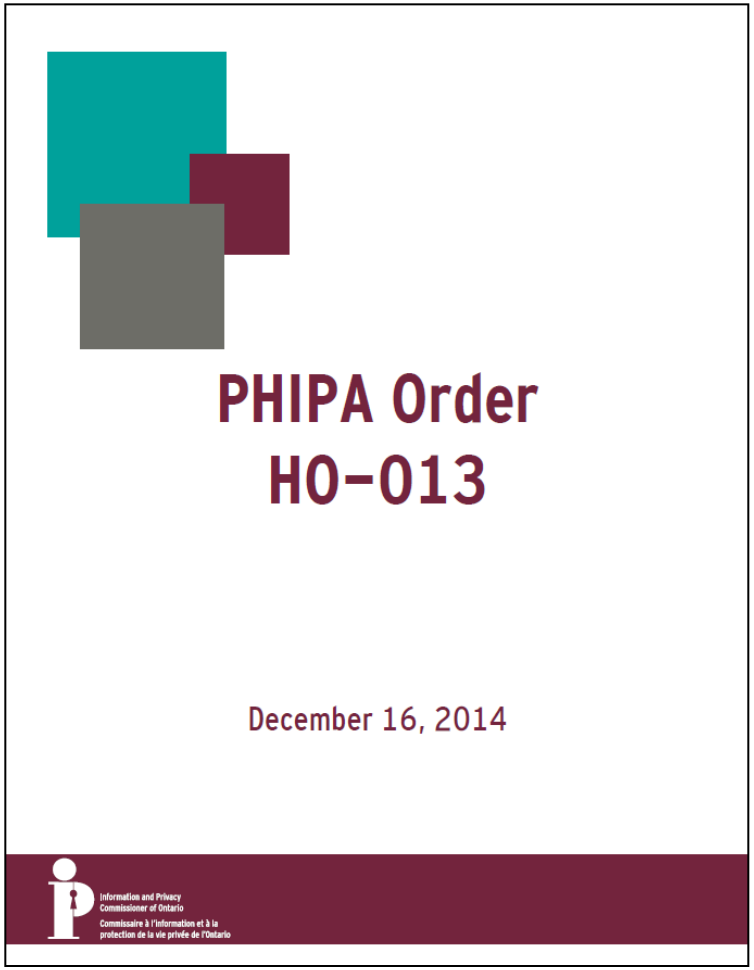
Order HO-010
The Outcome

The hospital was ordered to:

- Review the audit functionality on all systems and ensure that audit capability is “turned on.”
- Require agents who have contravened *PHIPA* to sign a confidentiality undertaking and non-disclosure agreement.
- Conduct privacy retraining programs.
- Review its policies, procedures and information practices.
- Implement a system that can display notice/warning when an agent accesses personal health information.

Order HO-013
The Story

- HO-013 was issued after two hospital employees used and disclosed information for the purpose of marketing RESPs.
- Hospital did not limit the search functionality of its electronic record system.

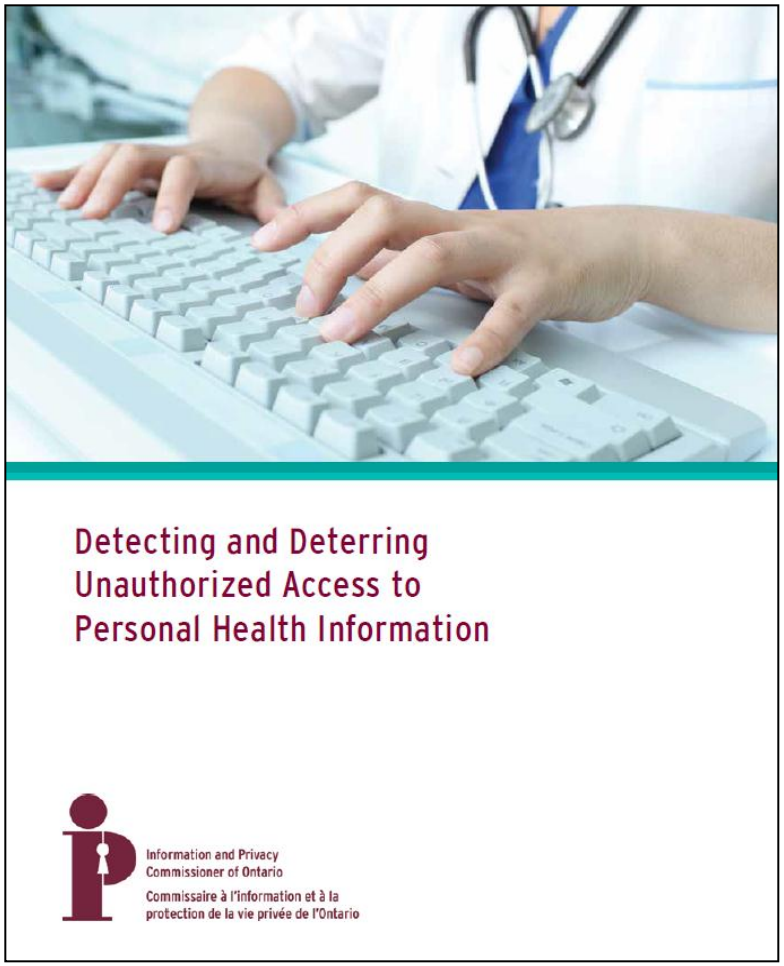


Order HO-013
The Outcome

The hospital was ordered to:

- Implement measures to audit all instances when agents access personal health information.
- Develop a solution that will limit search capabilities so that agents are unable to perform open-ended searches.
- Review the Privacy Audits policy, the Pledge of Confidentiality policy and the Pledge of Confidentiality, and the Privacy Advisory.
- Develop a Privacy Training Program policy, a Privacy Awareness Program policy, and a Privacy Breach Management policy, as well as review privacy training tools and materials.
- Immediately conduct privacy training for all applicable staff and agents.

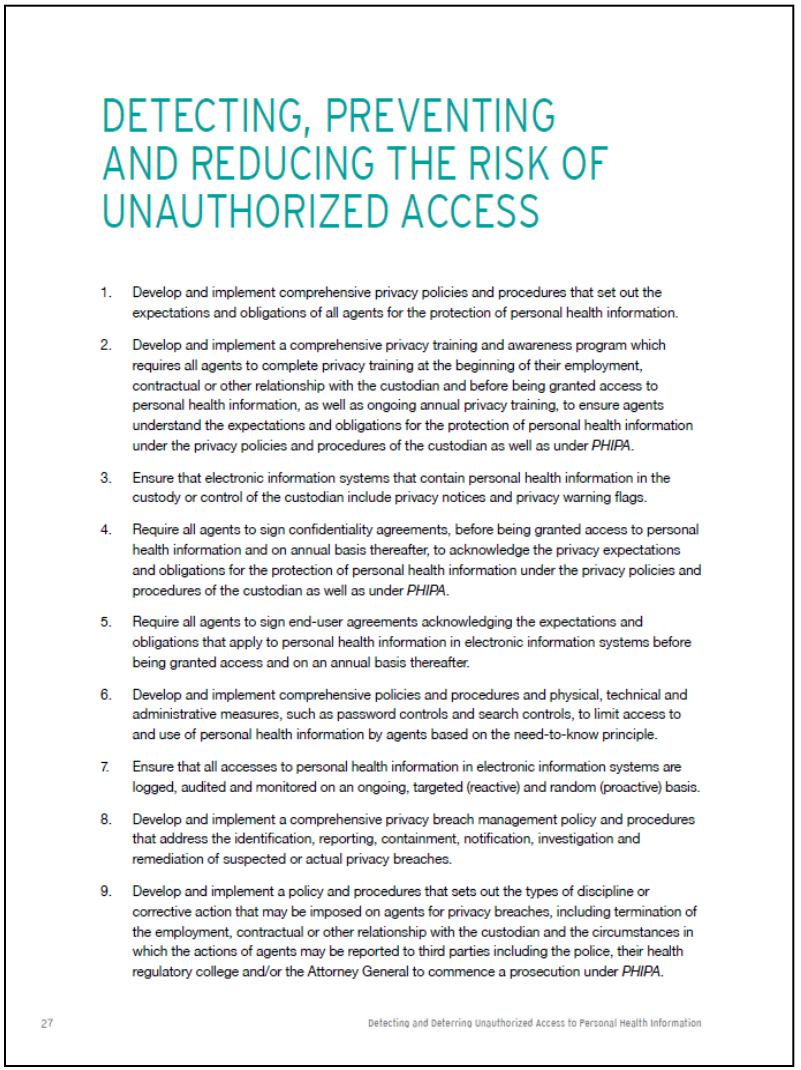
Educational Outreach: New Guidance Document



- Benefits and Risks of Electronic Records
- Impact of Unauthorized Access
- Preventing or Reducing the Risk of Unauthorized Access

Detect, Prevent and Reduce

- Comprehensive policies and procedures.
- Comprehensive training programs.
- Privacy notices and warning flags.
- Confidentiality agreements.
- End-user agreements regarding expectations and obligations.
- Physical, technical and administrative measures to limit access.
- All access is logged, audited and monitored.
- Comprehensive privacy breach management.
- Policies and procedures that set out the types of discipline and/or corrective action that may be imposed when unauthorized access occurs.



DETECTING, PREVENTING AND REDUCING THE RISK OF UNAUTHORIZED ACCESS

1. Develop and implement comprehensive privacy policies and procedures that set out the expectations and obligations of all agents for the protection of personal health information.
2. Develop and implement a comprehensive privacy training and awareness program which requires all agents to complete privacy training at the beginning of their employment, contractual or other relationship with the custodian and before being granted access to personal health information, as well as ongoing annual privacy training, to ensure agents understand the expectations and obligations for the protection of personal health information under the privacy policies and procedures of the custodian as well as under *PHIPA*.
3. Ensure that electronic information systems that contain personal health information in the custody or control of the custodian include privacy notices and privacy warning flags.
4. Require all agents to sign confidentiality agreements, before being granted access to personal health information and on annual basis thereafter, to acknowledge the privacy expectations and obligations for the protection of personal health information under the privacy policies and procedures of the custodian as well as under *PHIPA*.
5. Require all agents to sign end-user agreements acknowledging the expectations and obligations that apply to personal health information in electronic information systems before being granted access and on an annual basis thereafter.
6. Develop and implement comprehensive policies and procedures and physical, technical and administrative measures, such as password controls and search controls, to limit access to and use of personal health information by agents based on the need-to-know principle.
7. Ensure that all accesses to personal health information in electronic information systems are logged, audited and monitored on an ongoing, targeted (reactive) and random (proactive) basis.
8. Develop and implement a comprehensive privacy breach management policy and procedures that address the identification, reporting, containment, notification, investigation and remediation of suspected or actual privacy breaches.
9. Develop and implement a policy and procedures that sets out the types of discipline or corrective action that may be imposed on agents for privacy breaches, including termination of the employment, contractual or other relationship with the custodian and the circumstances in which the actions of agents may be reported to third parties including the police, their health regulatory college and/or the Attorney General to commence a prosecution under *PHIPA*.

“Is It Worth It?” Campaign

https://www.youtube.com/watch?v=tgB7yu7zXAo

Prosecution for Offences

- *PHIPA* creates offences for contraventions.
- It is an offence to willfully collect, use or disclose PHI in contravention of *PHIPA*.
- The Attorney General is responsible for commencing prosecutions under *PHIPA*.
- On conviction, an individual may be liable for a fine of up to $50,000 and an organization up to $250,000.

Detecting, Deterring and Reducing the Risk of Unauthorized Access

Everyone has a role to play:

- Health Information Custodians
- IPC
- Employees/Agents
- Regulatory Colleges
- MOHLTC/Attorney General

Lack of Clarity About Roles in Shared Electronic Systems

Need for A Governance Framework

- The custody and control of personal health information is not left to just one health information custodian.
- This can lead to a lack of clarity as to who is responsible for the various duties and obligations in *PHIPA.*
- Imperative that harmonized privacy policies and procedures be developed.

Harmonized Policies and Procedures: Why are They Essential?

Harmonized privacy policies and procedures are essential to:

- Clarify roles and responsibilities of custodians.
- Ensure consistency of experience across the sector.
- Minimize burden on individuals wishing to exercise their rights.
- Foster trust with patients and among custodians.

Long-Term Legislative Framework

- We need a long-term legislative framework for the provincial electronic health record.
- While *PHIPA* has served as a model health privacy statute, it does not adequately address the rights of individuals and the duties of custodians in a shared provincial system.

Bill 78, *Electronic Personal Health Information Protection Act*

The Bill would have required prescribed organizations to:

- Have in place and comply with privacy and security practices and procedures that are approved by the IPC every three years.
- Audit and monitor the EHR.
- Manage consent directives in the EHR.
- Respond or facilitate a response to access and correction requests.
- Maintain records of all accesses to the EHR.
- Maintain records of all instances where a consent directive is made, withdrawn, modified or overridden in the EHR.

Build A Culture of Privacy

- Start from the top down.
- Ensure your staff know how to apply privacy policies and procedures.
- Provide on-going privacy training.
- Use multiple means to communicate.
- Regularly assess the effectiveness of your privacy program.

How to Contact Us

Brian Beamish

Acting Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca