Protecting Patient Privacy
Preventing Patient Harm

Brian Beamish

Information and Privacy Commissioner of Ontario

Ottawa Hospital
June 5, 2015

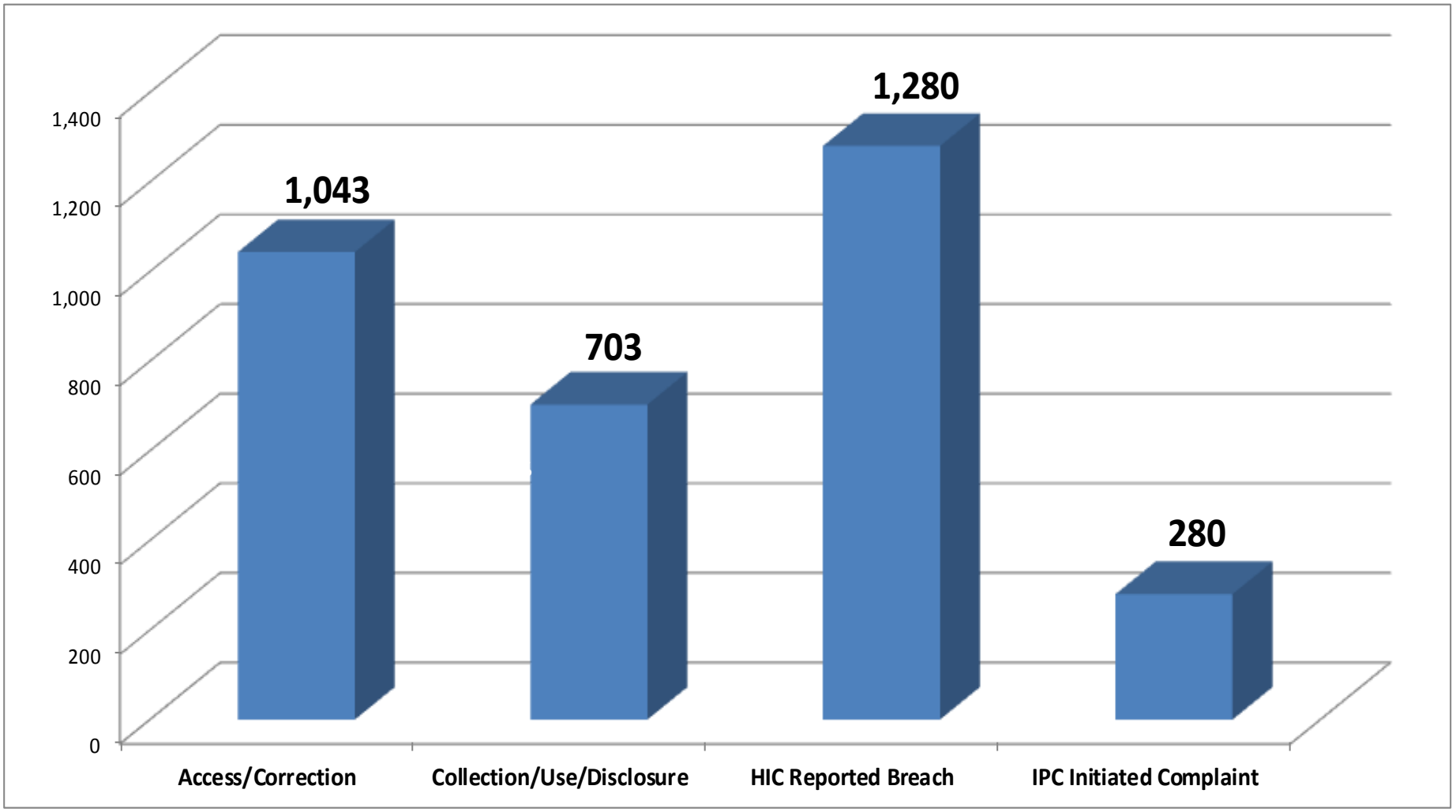
The Road to *PHIPA*

- 1980 Krever Commission – 170 recommendations.
- Served as the impetus for *PHIPA*.
- *PHIPA* is now recognized across Canada as a benchmark for health privacy legislation.

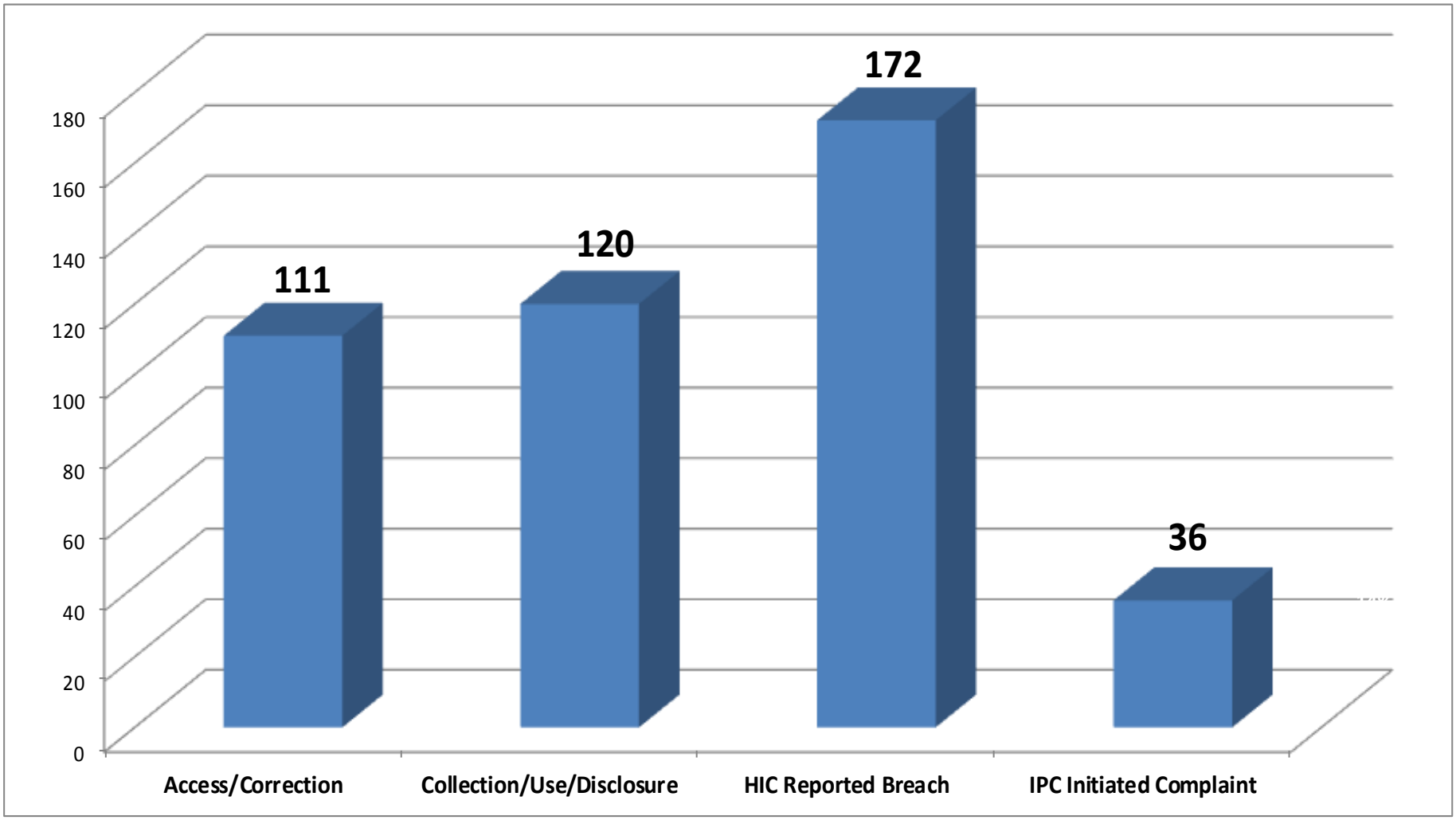
Unique Characteristics of Personal Health Information

- Highly sensitive and personal in nature.
- Must be shared seamlessly among a range of health care providers to deliver timely, efficient and effective health care to the individual.
- Dual nature of personal health information (PHI) is recognized in *PHIPA*.

PHIPA Complaints 2004-2014



PHIPA Complaints 2014



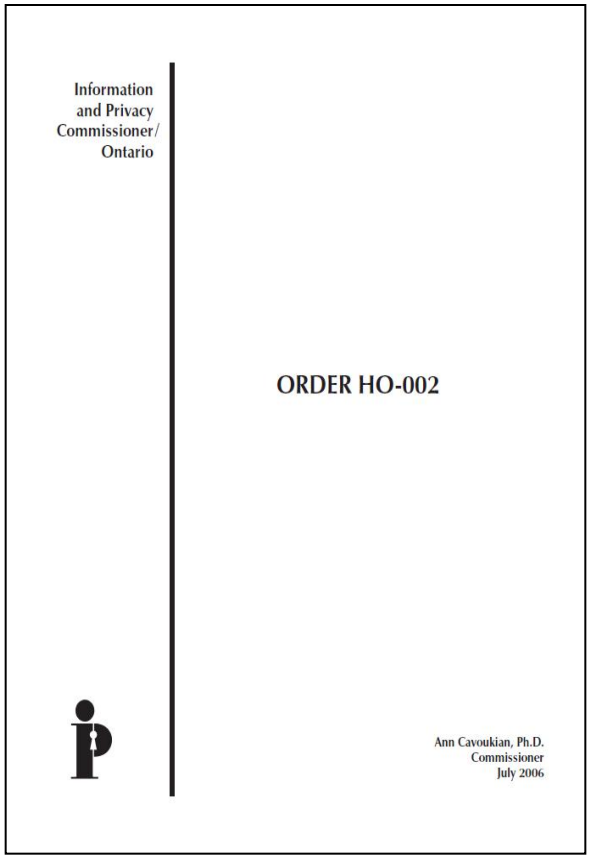
The Meaning of "Unauthorized Access"

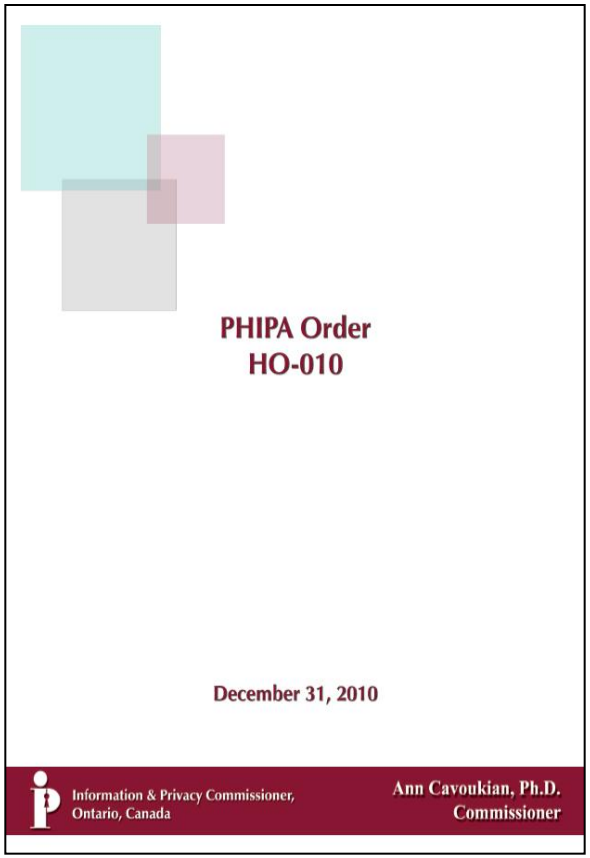
- There have consistently been cases of unauthorized access or "snooping" in Ontario where health records have been accessed in contravention of *PHIPA*.
- Snooping includes "only" viewing PHI.
- More serious with the growth of electronic health records.

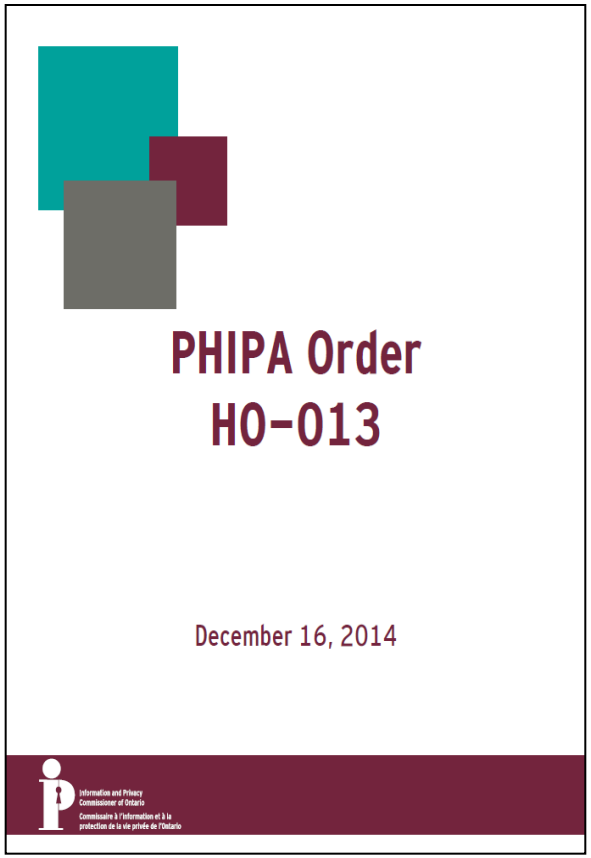
Consequences of Unauthorized Access

- Unauthorized access can have significant consequences for all involved.
  - Individuals
  - Health Information Custodians
  - Employees/Agents

Health Orders Issued in Response to "Snooping"







Prosecution for Offences

- 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*.
- An individual may be liable for a fine of up to $50,000 and an organization 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.

thestar.com
CRIME

News / 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.

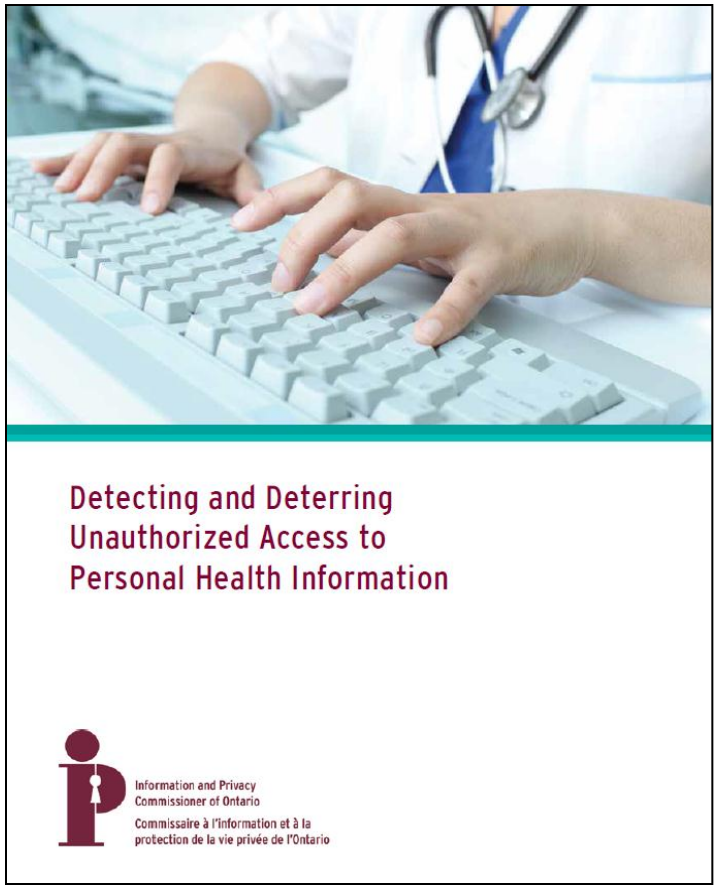
The criminal and securities charges are the most serious consequences any health professional has faced for a privacy breach, and come days after the provincial privacy watchdog called for a criminal crackdown.

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

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

Challenges Posed by Shared EHRs

- 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.
- These pose unique privacy risks and challenges for compliance with *PHIPA.*

The Need for *ePHIPA*

- A governance framework and harmonized privacy policies and procedures are needed to:
  - Set out the roles and responsibilities of each participating 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.

Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies and procedures should address:

- Governance
- Consent Management
- Logging, auditing and monitoring
- Privacy training
- 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.

Build A Culture of Privacy

- Build a culture of privacy from the top down.
- Ensure staff know how to apply privacy policies and procedures in their day-to-day work.
- Provide on-going privacy training.
- Use multiple means to communicate privacy messages.
- Regularly assess the effectiveness of your privacy program.

How to Contact Us

Brian Beamish

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