New Updates and Guidance from the Ontario IPC

David Goodis

Assistant Commissioner
Information and Privacy Commissioner of Ontario

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

Canadian Institute Privacy and Data Security Compliance Forum

January 30, 2018

Who is the Information and Privacy Commissioner?

- Brian Beamish appointed by Ontario Legislature (March 2015)
- 5 year term
- reports to Legislature, not government or minister
- ensures independence as government “watchdog”

Ontario's Legislative Framework

Public Sector	Health Sector	Private Sector
Government e.g. ministries, agencies, hospitals, universities, cities, police, schools, hydro	Individuals, organizations delivering health care e.g. hospitals, pharmacies, labs, doctors, dentists, nurses	Private sector businesses engaged in commercial activities
Freedom of Information and Protection of Privacy Act (*FIPPA*) *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)	*Personal Health Information Protection Act* (*PHIPA*)	*Personal Information Protection and Electronic Documents Act* (*PIPEDA*)
IPC/O oversight	IPC/O oversight	Privacy Commissioner of Canada oversight

Our Mandate

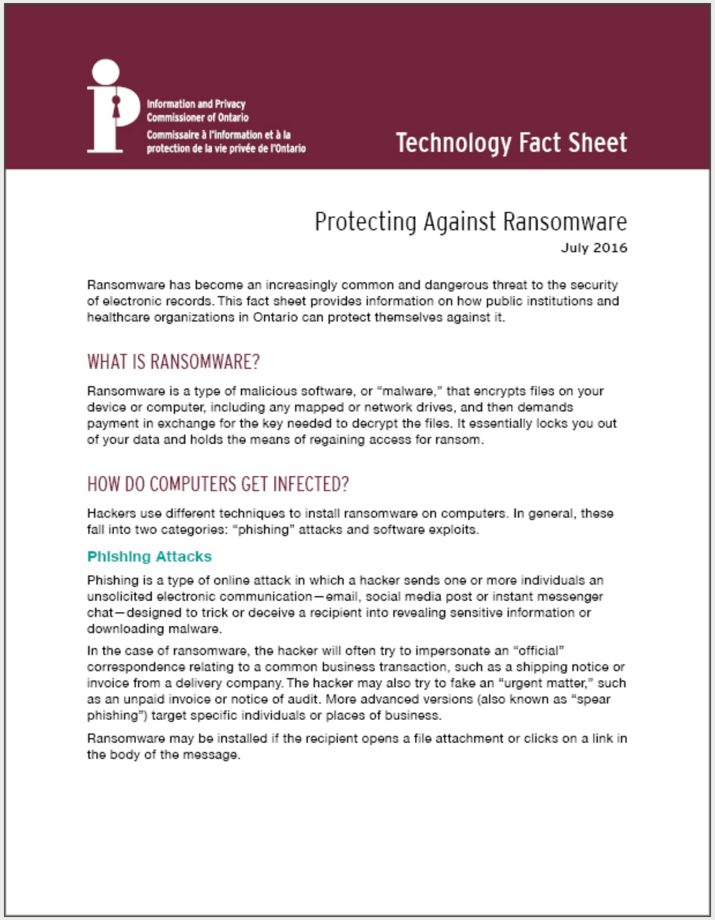
- *resolve* access to information appeals
- *investigate* privacy complaints (public sector, health)
- *research* access and privacy issues
- *comment* on proposed legislation, programs
- *educate* the public on access and privacy

Privacy Threats

Common Privacy Breaches

1. Insecure disposal of records
   - records in paper format intended for shredding are recycled
   - insecure disposal of hard drives
2. Mobile and portable devices
   - lost or stolen, unencrypted devices such as laptops, USB keys
3. Unauthorized access
   - snooping by otherwise authorized staff, malware (e.g. ransomware)

Ransomware



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

Technology Fact Sheet

Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: "phishing" attacks and software exploits.

Phishing Attacks

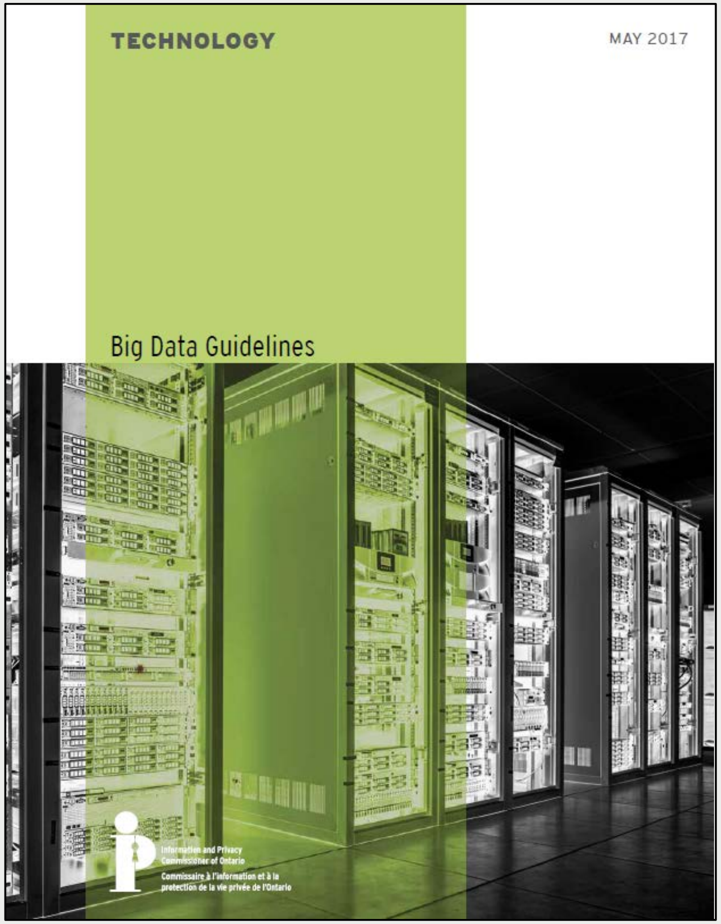
Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

In the case of ransomware, the hacker will often try to impersonate an "official" correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an "urgent matter," such as an unpaid invoice or notice of audit. More advanced versions (also known as "spear phishing") target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

- what is ransomware?
- how computers get infected
  - ▪ phishing attacks
  - ▪ software exploits
- how to protect your organization
  - administrative, technological measures e.g. employee training, limiting user privileges, software protections
- how to respond to incidents

Big Data



TECHNOLOGY

MAY 2017

Big Data Guidelines

Information and Privacy Commissioner of Ontario

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

- key issues, best practices when conducting big data initiatives involving personal information
- considerations at each stage of big data project, including
  - collection
  - integration
  - analysis
  - profiling

Big Data in the Government Context

- governments want to **share, link, analyze data** across agencies to obtain new insights, to support
  - policy development
  - system planning
  - resource allocation
  - performance monitoring
- sometimes called data integration
- benefits may be compelling, but we worry about uses of PI that are
  - unexpected
  - invasive
  - inaccurate
  - discriminatory

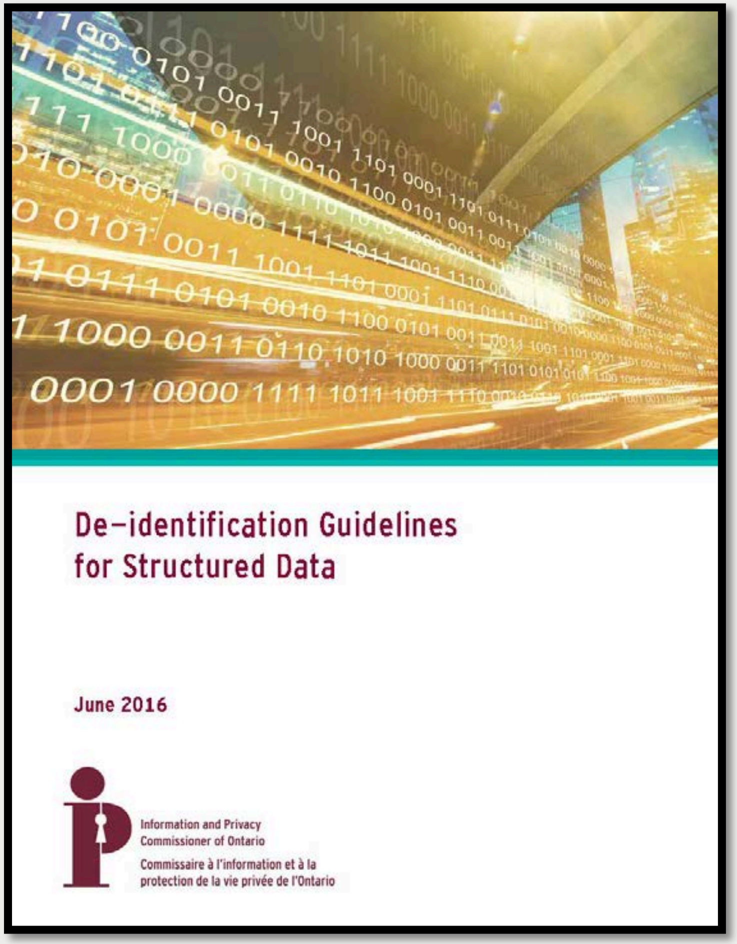
We Need Legislative Reform!

- current law treats government institutions as silos; sharing/linking across government not envisioned
- need **single dedicated unit** in government to
  - collect PI across government
  - link records securely
  - de-identify
  - make de-identified data available to public bodies
- this is *PHIPA* approach [s. 55.9]
- avoids **replicating databases** of sensitive PI across government
- ethical review, strong IPC oversight

Reducing Risk of Privacy Breaches

De-identification

- risk-based, step-by-step process to assist organizations to de-identify
- key issues when publishing
  - release models
  - types of identifiers
  - re-identification attacks
- IPC wins global privacy award for excellence in research [International Conference of Data Protection and Privacy Commissioners, Hong Kong 2017]



De-identification Guidelines for Structured Data

June 2016

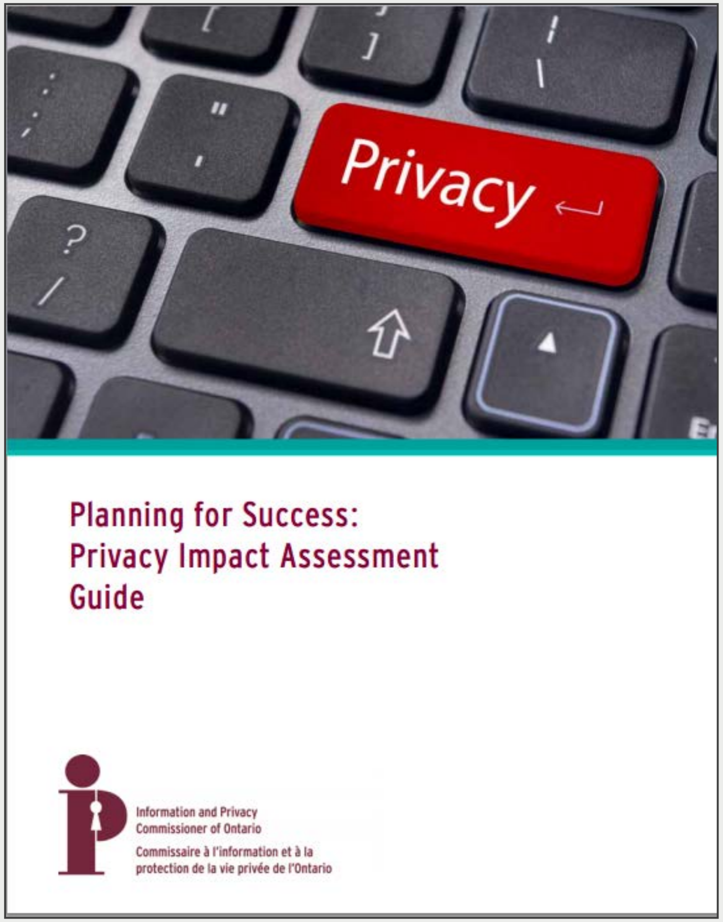
Information and Privacy Commissioner of Ontario

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

Reducing Risk of Privacy Breaches Best Practices

Administrative	Technical	Physical
• privacy and security policies • auditing compliance with rules • privacy and security training • data minimization • confidentiality agreements • Privacy Impact Assessments	• strong authentication and access controls • detailed logging, auditing, monitoring • strong passwords, encryption • patch and change management • firewalls, anti-virus, anti-spam, anti-spyware • protection against malicious code • Threat Risk Assessments, ethical hacks	• controlled access to premises • controlled access to locations within premises where PI is stored • access cards and keys • ID, screening, supervision of visitors NOTE – when determining appropriate safeguards consider • sensitivity and amount of information • number and nature of people with access to the information • threats and risks associated with the information

Planning for Success: Privacy Impact Assessment Guide



Planning for Success:
Privacy Impact Assessment
Guide

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

- tools to identify privacy impacts and risk mitigation strategies
- step-by-step advice on how to conduct a PIA
- not required by legislation, but considered privacy best practice

How to Respond to Privacy Breach

Responding to a Privacy Breach

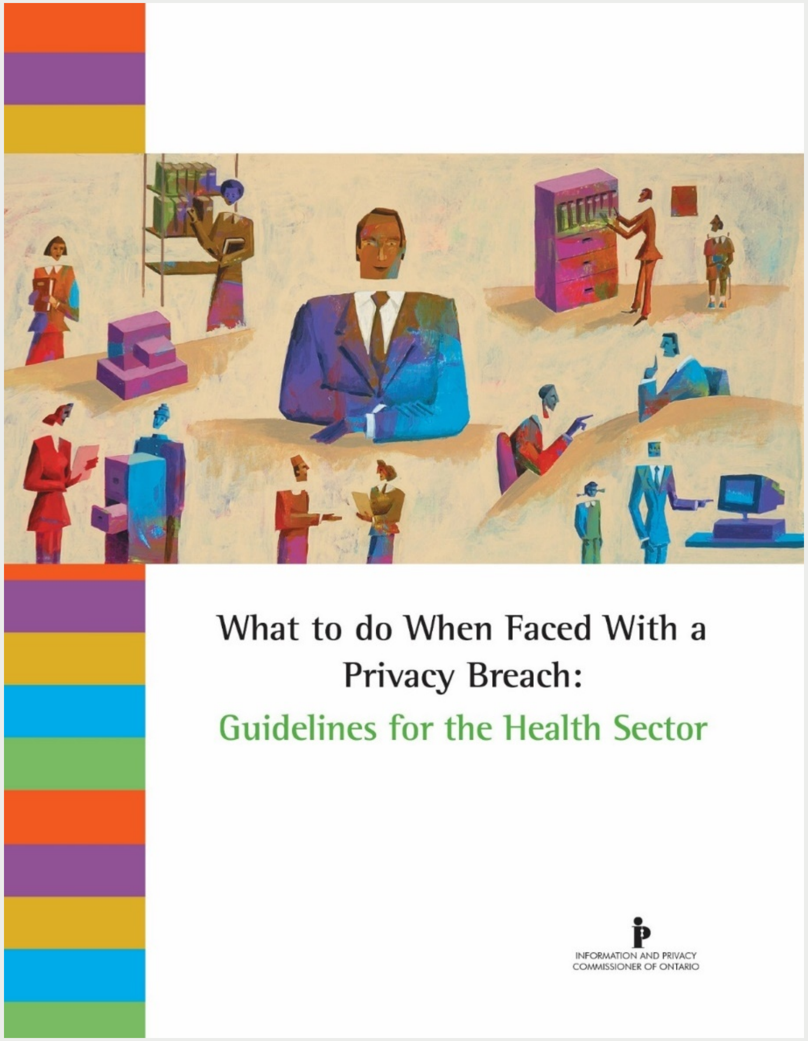
1. Contain Breach
   - initial investigation
   - notify police if theft or other criminal activity
2. Evaluate Risks
   - personal information involved?
   - cause and extent of breach
   - individuals affected
   - possible harm?
3. Notify
   - affected individuals
   - Privacy Commissioner
4. Prevent Future Breaches
   - security audit
   - review of policies and practices, staff training, 3P service contracts

OPC Resource: **Key Steps for Organizations in Responding to Privacy Breaches**

- https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gl_070801_02/

What to do When Faced with a Privacy Breach

- *PHIPA* sets out the rules that health information custodians must follow when collecting, using, disclosing, retaining and disposing of personal health information
- guidance to health information custodians when faced with a privacy breach



What to do When Faced With a Privacy Breach:

Guidelines for the Health Sector

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

Commissioner’s Response to Privacy Breach

Mandatory *PHIPA* Breach Reporting

- as of October 2017, health information custodians **must notify IPC** of certain privacy breaches
  - use or disclosure without authorization
  - stolen information
  - further use/disclosure following breach
  - breaches as part of pattern
  - breaches related to disciplinary action
  - significant breaches

SEPTEMBER 2017

GUIDELINES FOR THE
HEALTH SECTOR

Reporting a Privacy Breach to the Commissioner

To strengthen the privacy protection of personal health information, the Ontario government has amended the *Personal Health Information Protection Act* (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect **October 1, 2017**.

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

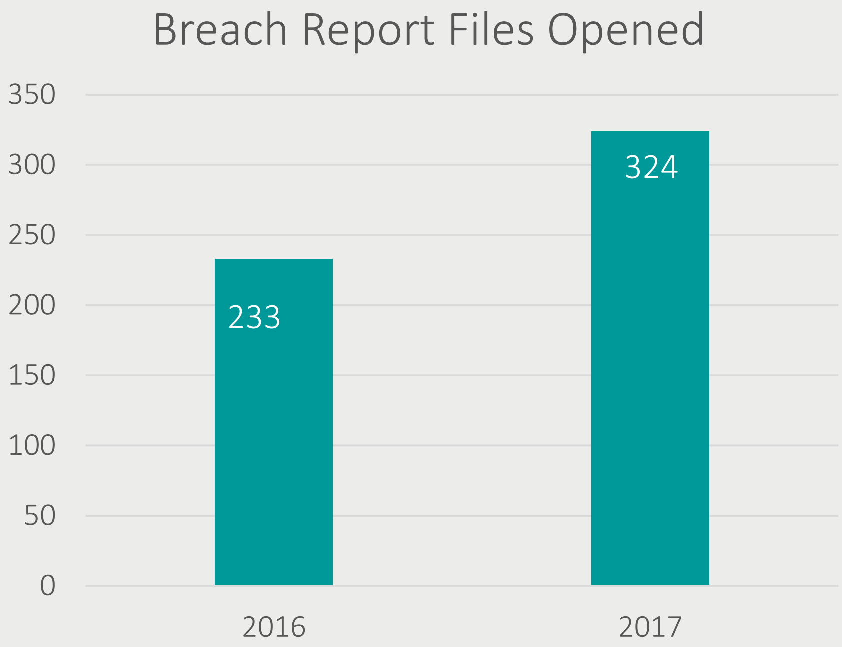
1. Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

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

Health Privacy Breach Statistics

- of 324 reported breaches in 2017:
  - 60 snooping
  - 8 ransomware/cyberattack
- remaining 256:
  - lost or stolen PHI
  - misdirected information
  - records not properly secured
  - general collection, use and disclosure



What Happens when the IPC Reviews a Breach

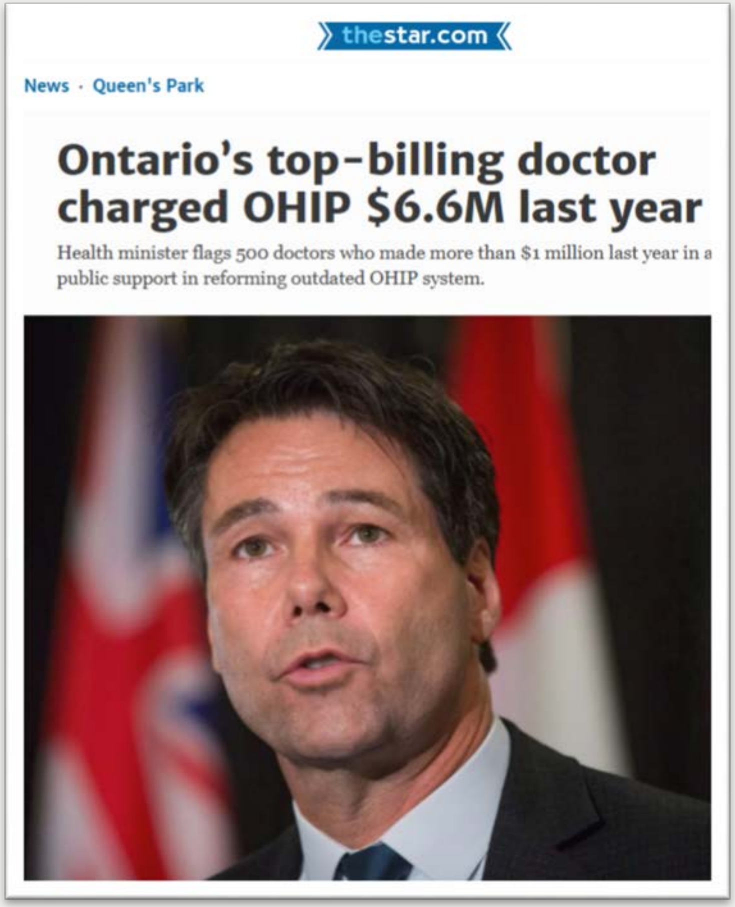
- IPC may:
  - ensure adequate containment, notification
  - interview appropriate individuals
  - review organization’s position on the breach
  - ask for status report of organization’s actions
  - review, give advice on current policies
  - report with recommendations (rarely order)

Privacy and Transparency – Public Interest

Jurisdictional Attitudes Towards Public’s Right to Know

American vs. Canadian expectations about public disclosure of politicians’ health status

Doctor’s billings - Public Interest Override



thestar.com

News · Queen's Park

Ontario’s top-billing doctor charged OHIP $6.6M last year

Health minister flags 500 doctors who made more than $1 million last year in a public support in reforming outdated OHIP system.

Significant public attention to doctors’ OHIP billings

Order **PO-3617**, requires disclosure – personal privacy exemption does not apply

Even if exempt, compelling public interest in disclosure given importance of transparency in spending substantial public money

Divisional Court upholds IPC order (June 2017); ONCA grants doctors leave to appeal

Yes, you can share information with a Children’s Aid Society to protect a child.

Find out more at www.ipc.on.ca

YES,

YOU

CAN.

DISPELLING THE MYTHS ABOUT SHARING INFORMATION WITH CHILDREN’S AID SOCIETIES.

Information and Privacy
Commissioner of Ontario

Provincial Advocate
for Children & You

Philadelphia Model

- annual meeting of advocates, representatives from Women's Law Project, search police sexual assault files (alongside senior police) looking for deficiencies and biases
- since began 17 years ago, "unfounded rape" rate dropped to 4%, national average is 7%

UNFOUNDED

WHY POLICE DISMISS 1 IN 5 SEXUAL ASSAULT CLAIMS AS BASELESS

Globe and Mail series "Unfounded"

Working with Police on an Ontario-based Philadelphia Model

- identify external partners with experience to assist with the review of sexual assault files, appoint them police agents
- reviewers subject to background check, sign oath of confidentiality, receive privacy training
- reviewers see names of principals so can recuse if needed
- reviewers study complete closed files, subject only to redactions or restrictions required by law
- reviews at police facilities, no identifying information copied, retained, removed

Looking Ahead

Child, Youth and Family Services Act

- child and youth protection sector will be subject to privacy rules
- service providers like children's aid societies will need to:
  - get consent for PI collection, use, disclosure
  - report serious privacy breaches to the IPC
- individuals will have right to access PI held by service providers, may request correction
- "PHIPA"-like rules

Anti-Racism Act

- requires Ontario government to develop, maintain anti-racism strategy including:
  - initiatives to eliminate systemic racism
  - measures to advance racial equity
  - targets and indicators to measure effectiveness
- includes privacy protective provisions
- IPC has oversight role

Questions?

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