Privacy and the *Child, Youth and Family Services Act*

Debra Grant, Director of Health Policy
Renee Barrette, Director of Policy

Information and Privacy Commissioner of Ontario

Organization of Counsel for Children's Aid Societies
Fall Conference
October 19, 2017

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

Agenda

- **IPC's mandate**
- ***CYFSA***
  - Background
  - Service providers – new rules and responsibilities
  - Access and Correction
  - Oversight and enforcement
- **Privacy Breaches**
  - Common causes of privacy breaches
  - Reducing the risk of privacy breaches
  - Responding to a privacy breach
- **IPC Guidance Documents**
- **Next steps**

Our Office

- The Information and Privacy Commissioner (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; and remains independent of the government of the day to ensure **impartiality**

The Three Acts

The IPC currently oversees compliance with:

- *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**)*

The Three Acts

The IPC ensures compliance with:

FIPPA and ***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

PHIPA

- Provides comprehensive privacy protections for personal health information and right to complain about a breach
- Primarily a privacy statute – also provides patients with a right of access to their health information, and a right to appeal access decisions to the IPC

New Mandates

- *Child, Youth and Family Services Act, 2017*
- *Anti-racism Act, 2017*

The *Child, Youth and Family Services Act, 2017*

Background

- The *Child, Youth and Family Services Act, 2017* (*CYFSA*) was introduced as Schedule 1 of Bill 89, the *Supporting Children, Youth and Families Act, 2017*, which received Royal Assent on June 1
- The **paramount purpose** of the *CYFSA* is to promote the best interests, protection and well-being of children
  - One additional purpose of the act is to recognize that appropriate sharing of information in order to plan for and provide services is essential for creating successful outcomes for children and families
- The *CYFSA* is expected to come into force in Spring 2018

Part X of the *CYFSA*

s. 281 - 332

- Sets out rules for the **collection, use and disclosure of personal information** (PI) by child, youth and family service providers, including:
  - Children's Aid Societies (CASs)
  - Minister of Children and Youth Services (the Minister)
- Gives individuals the rights of access, correction, and complaint, with oversight by the IPC
- Modeled after *PHIPA* – **Fair Information Practices**

Fair Information Practices

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

What is personal information?

s. 2(1)

- Recorded information about an **identifiable individual**, including:
  - race, colour, religion, age, sex, sexual orientation or marital or family status of the individual
  - any identifying number or symbol assigned to the individual
  - address, telephone number, fingerprints or blood type of the individual
  - individual's name where it appears with other personal information relating to the individual

What is <u>not</u> personal information?

- PI **does not** include:
  - information associated with an individual in a professional, official or business capacity, for example:
    - names of individuals who provided services to a government institution on a fee-for-service basis
    - information relating to business costs incurred by named employees during the course of their employment as public employees

Who is covered by Part X?

s. 2(1) and 281

- "**Service provider**" means:
  - the Minister of Children and Youth Services
  - a licensee (e.g., children's residences)
  - a person or entity that provides a service funded under the *CYFSA* (e.g., CASs)
  - a prescribed person or entity
- It does not include a foster parent
- For the purposes of Part X, includes a "lead agency" designated under s. 30

Exceptions

s. 285

- Service providers that are also institutions under *FIPPA* or *MFIPPA*, or health information custodians under *PHIPA* are **exempt from many of the privacy and access provisions of Part X**

- Many of these provisions also **do not apply** to adoption matters, the child abuse register, certain production orders, and assessment reports

Service Providers:
New Rules and Responsibilities

Consent under Part X

s. 286 and 295

- Consent is required for the collection, use, disclosure of PI, subject to specific exceptions
- Consent must:
  - be a consent of the individual;
  - be knowledgeable;
  - relate to the information; and
  - not be obtained through deception or coercion
- Consent to the collection and use of PI can be implied in certain circumstances

Consent (continued)

s. 295-296

- Consent is **knowledgeable** if it is reasonable in the circumstances to believe that the individual knows:
  - the purpose and
  - that the individual may give, withhold, or withdraw consent
- Individual is deemed to know the purposes if the service provider posts a notice or gives it to the individual
- Individual may **withdraw consent** by providing notice to the service provider, but the withdrawal of the consent cannot have retroactive effect

Capacity

s. 281, 299 and 301

- **There is a presumption of capacity**. Capable individual may give, withhold or withdraw consent
- **Part X defines "capable"** as being able to understand the information that is relevant to deciding whether to consent to the collection, use or disclosure of personal information and able to appreciate the reasonable foreseeable consequences of giving, withholding or withdrawing the consent
- **16 or older**: may authorize another individual who is 16 or older and capable to be the individual's substitute decision-maker under Part X
- **Under 16**: the parent, CAS, or other authorized person may be the child's substitute decision-maker (subject to exceptions)
  - A **capable child's decision prevails** over a conflicting decision of the substitute decision-maker
- For an incapable individual, a person authorized under *PHIPA* may be the individual's substitute decision-maker

Collection, Use and Disclosure

s. 286 and 287

- Service providers may **only** collect, use or disclose personal information if:
  - the individual **consents and** the collection, use or disclosure is **necessary for a lawful purpose** or
  - the ***CYFSA* permits or requires** the collection, use or disclosure without consent

- **Data minimization requirements** limit a service provider's authority to collect, use or disclose personal information

Permitted Indirect Collections

s. 288

- The individual **consents** to indirect collection
- Indirect collection is **reasonably necessary** to either:
  - provide service
  - assess, reduce or eliminate risk of serious harm to a person or group

  and it is **not possible to collect the PI directly** that will be accurate or timely
- Authorized by IPC
- Authorized by law (e.g., "Duty to Report", *CYFSA* s. 125-126)

Permitted Indirect Collection

s. 288

- In addition, **CASs** may indirectly collect PI without consent:
  - from another CAS (or child welfare authority outside of Ontario) if necessary to assess, reduce or eliminate a risk of harm to a child
  - if necessary for a prescribed purpose

Permitted Direct Collection (without consent) s. 289

- Necessary to provide a service and not possible to obtain consent in a timely manner
- Necessary to assess, reduce or eliminate a risk of serious harm to a person or group
- In addition, **CASs** may directly collect PI without consent if the information is necessary to assess, reduce or eliminate a risk of harm to a child

Notice re: Direct Collection

s. 290

- Service providers **must notify** individuals from whom they directly collect PI that the information may be used or disclosed in accordance with Part X

Permitted Uses (without consent)

s. 291

- For purpose for which it was collected (subject to exceptions)
- If reasonably necessary to assess, reduce or eliminate a risk of serious harm to a person or group
- For the purpose for which a law required the disclosure to the service provider
- For planning, managing or delivering services
- For risk management and error management activities
- For activities to improve/maintain quality of service
- For disposing of or de-identifying information

Permitted Uses (without consent)

- To seek consent (name and contact info)
- For a proceeding
- For research purposes (subject to requirements)
- If permitted or required by law

Exceptions – Overriding Consent

s. 291 (2)

- CASs may override an individual's consent to use PI:
  - if it is necessary to assess, reduce, or eliminate a **risk of harm to a child**
  - for a prescribed purpose

- Service providers may override an individual's consent to use PI:
  - If it is necessary to assess, reduce or eliminate a **risk of serious harm** to a person or group

Permitted Disclosures (without consent) s. 292

- To a Canadian law enforcement agency to aid an investigation
- To appoint a litigation guardian or legal representative
- To a litigation guardian or legal representative
- To contact a relative, friend etc if individual is injured, incapacitated or not capable
- To contact a relative, friend etc if individual is deceased
- To comply with an order in a proceeding
- If necessary to assess, reduce or eliminate a risk of serious harm to a person or group
- If permitted or required by law
- To a successor (subject to other requirements)

Permitted Disclosures (without consent)

- In addition, CASs may disclose PI without consent:
  - to another CAS (or child welfare authority outside of Ontario) if necessary to assess, reduce or eliminate a risk of harm to a child
  - if the information is necessary for a prescribed purpose

Disclosures for Planning and Managing Services s. 293

- Service providers may disclose PI for purposes that include planning, managing and evaluating services to:
  - a **prescribed entity** if it meets certain requirements
  - a **person or entity that is not prescribed**, if it complies with any prescribed requirements and restrictions

- Minister may require a service provider to disclose PI to a prescribed entity or person or entity that is not prescribed for planning, managing and evaluating services

Integrity and Protection of PI

s. 306 - 309

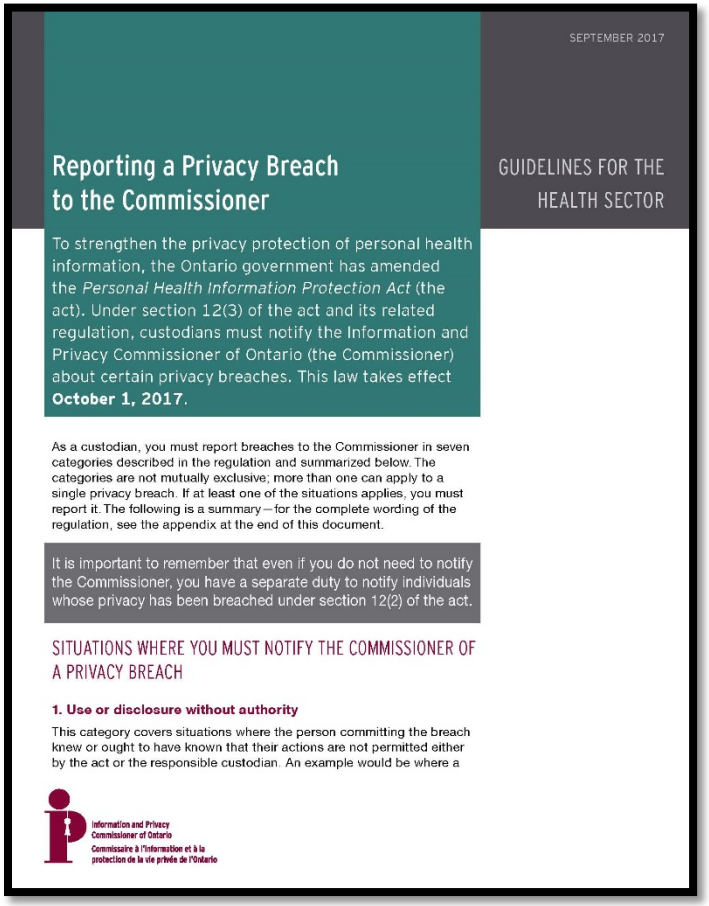
- Service providers **must** take reasonable steps to ensure PI is:
  - accurate, complete and up to date as necessary for the purpose for which it uses and discloses the information
  - not collected without proper authority
  - protected against theft, loss and unauthorized use or disclosure and protected against unauthorized copying, modification or disposal
  - retained, transferred and disposed of in a secure manner

Breach Notification

s. 308 (2-3)

- If PI is **stolen or lost or if it is used or disclosed without authority**:
  - Service providers **must notify the individual of a breach** of their personal information
  - If the breach meets **prescribed requirements**, the service provider must also notify the **IPC** and **Minister**

Health Sector
Privacy Breach Reporting



SEPTEMBER 2017

Reporting a Privacy Breach to the Commissioner

GUIDELINES FOR THE HEALTH SECTOR

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

- as of **October 1, 2017**, health information custodians are required to report privacy breaches to the IPC in seven categories
- the categories are described in the regulations and summarized in the guidelines
- more than one category can apply to a single privacy breach

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

Information Practices

s. 311 (1)

- Service providers **must** make the following publicly available:
  - A general description of their information practices
  - Contact information
  - How to obtain access to or request correction of a record of PI about the individual
  - How to make a complaint to the service provider and to the IPC under Part X

Information Practices

s. 311 (2)

- If service provider uses or discloses PI without consent outside the scope of their description of information practices, the service provider must:
  - notify the individual (unless the individual does not have access to the record)
  - make note of the uses and disclosures
  - keep the note as part of the record of PI or linked to the record

Access and Correction

Right of Access and Correction

s. 312 and 315

- Part X gives individuals the right to:
  - **access** records of PI about the individual in the custody or control of a service provider (some exceptions)
  - **correct** their records of PI (some exceptions)

Individual's Right of Access
s. 312

- Individuals have the right to access:
  - records of their PI
  - in a service provider's custody or control
  - that relate to the provision of a service to the individual

Exceptions to Access

s. 312

- An individual **does not** have a right of access if
  - the record is subject to a legal privilege restricting disclosure
  - another act or order prohibits disclosure to the individual
  - the information in the record was collected for a proceeding, and the proceeding and any appeals have not concluded

Exceptions to Access (continued)

s. 312

- Granting access could reasonably be expected to:
  - result in a risk of serious harm to the individual or another individual,
  - lead to the identification of an individual who was required by law to provide information in the record to the service provider, or
  - lead to the identification of an individual who provided information in the record to the service provider explicitly or implicitly in confidence if the service provider considers it appropriate

Exceptions to Access (continued)

s. 314(6)

AUGUST 2017

ACCESS
FACT SHEET

Frivolous and Vexatious Requests

The *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the acts) give individuals the right to access their own information and general records held by an institution unless an exemption applies or the request is frivolous or vexatious.

An institution may refuse to give access to a record if it decides the request is frivolous or vexatious. The requester can appeal this decision to the Information and Privacy Commissioner (IPC).

This fact sheet explains what a frivolous or vexatious request is, what institutions should do when they receive this type of request, what a requester can do if an institution claims their request is frivolous or vexatious and the IPC's role in an appeal.

WHAT IS A FRIVOLOUS OR VEXATIOUS REQUEST?

A request is frivolous or vexatious if it is:

- part of a pattern of conduct that
  - amounts to an abuse of the right of access
  - interferes with the operations of the institution
- made in bad faith or
- made for a purpose other than to obtain access

Each of these grounds is explained below.

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

- Service providers may refuse to grant access if they believe the request is **frivolous or vexatious** or is made in bad faith

- IPC Fact Sheet on Frivolous and Vexatious Requests:
  - www.ipc.on.ca/resource/frivolous-and-vexatious-requests/

Access

s. 312

- If the right of access is to part of a record only, then the right applies to that part that can reasonably be severed from the part of the record to which the individual does not have a right of access

- If a record is not a record **dedicated primarily to the provision of a service to the individual** requesting access, the individual has a right of access only to the PI about the individual in the record that can reasonably be severed from the record

Responding to Access Requests

s. 313-314

- In responding to a request, service provider must:
  - make the record available or provide a copy, if requested
  - respond to request within 30 days, with a possible 90 day extension
  - take reasonable steps to be satisfied of the individual's identity
  - offer assistance in reformulating a request that lacks sufficient detail

Expedited Access

s. 314 (5)

- Service provider must provide expedited access if:
  - the individual requests expedited access
  - the individual provides evidence that the information is needed within a specified time period, and
  - the service provider is **reasonably** able to respond within the requested time period

Time Extension for Access

s. 314 (3-4)

- Service providers may extend deadline by up to 90 days, if responding within 30 days would:
  - unreasonably interfere with operations, because of numerous pieces of information or the need for lengthy search, or
  - be not reasonably practical given the time required to assess the individual's right to access (under s. 312 (1))

- The service provider must give the individual written notice of the reason for the extension and its length, within 30 days

Correction of Records

s. 315

- Individuals have the **right to correct** records of their PI
- Individuals may request in writing that a service provider correct a record of PI if:
  - the service provider has granted the individual access to the record and
  - the individual believes that the record is **inaccurate** or **incomplete**

Corrections and Exceptions

s. 315 (9-10)

- The service provider **must correct the record** if the individual:
  - demonstrates to the service provider's satisfaction that the record is inaccurate or incomplete, and
  - gives the service provider the correct information

Exceptions:

- The service provider is **not required to correct the record** if:
  - it was not originally created by the service provider, and the provider lacks sufficient knowledge, expertise or authority to correct it; or
  - it consists of a professional opinion or observation made in good faith

How to Correct Records

s. 315 (11)

- by **striking out** the incorrect information in a manner that does not obliterate it or
- by **labeling** the information as incorrect and severing it from the record, while maintaining a link to the record or
- if the correction cannot be recorded in the record, the custodian must ensure there is a practical system to **inform persons** accessing the record that the information is incorrect and where to obtain correct information

Notice of Correction

s. 315 (11)(c)

- **At the request of the individual**, the service provider must give written notice of the requested correction, **to the extent reasonably possible**, to persons to who the service provider has disclosed the information

- **Exception –** if the correction cannot reasonably be expected to have an effect on the ongoing provision of services

Statement of Disagreement

s. 315 (12) and (14)

- If the service provider refuses a correction request, the individual is entitled to require the service provider to attach to the record a **statement of disagreement** prepared by the individual

- Service provider must make reasonable efforts to **notify** anyone who would have been notified if there was a correction

Oversight and Enforcement

Role of the IPC under *CYFSA*

s. 316 - 329

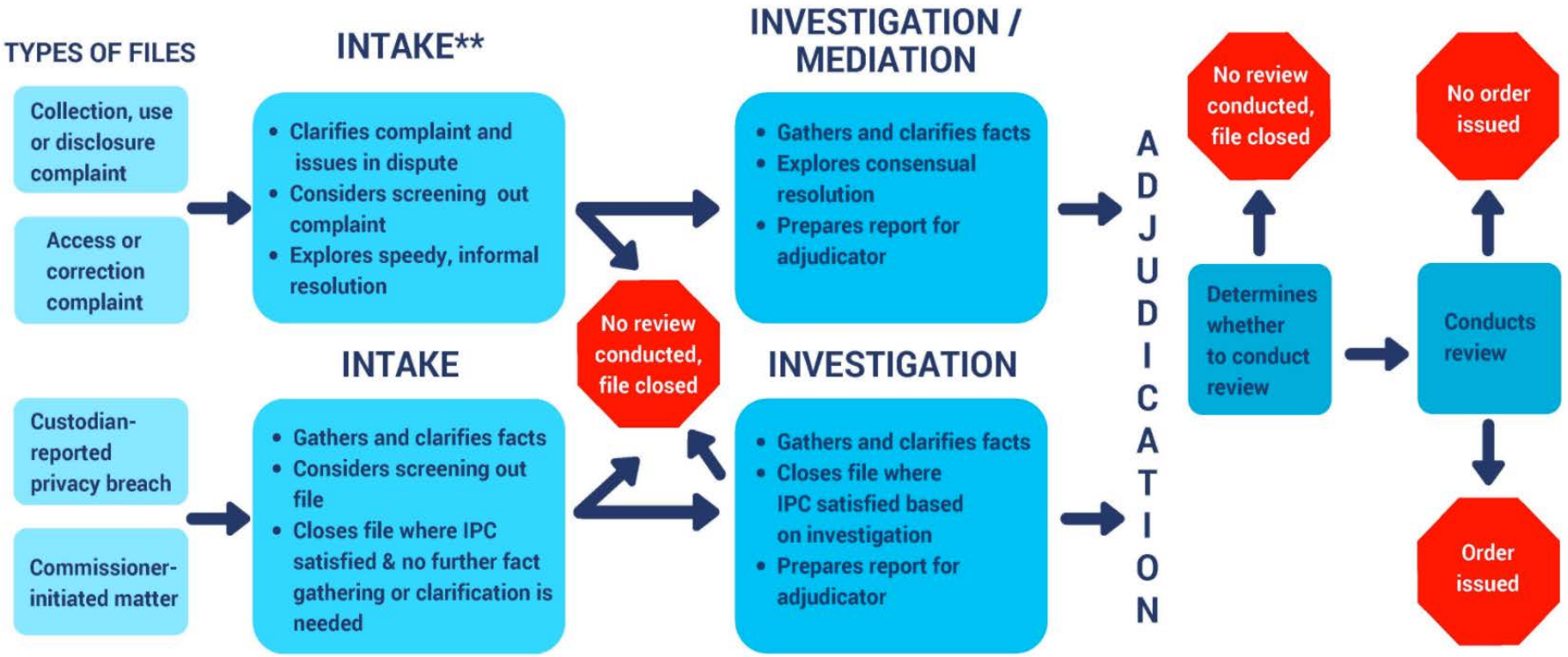
- IPC is the oversight body for Part X
- Individuals **may make a complaint to the IPC** about any person who has or is about to contravene Part X, for example:
  - complaints about access or correction decisions
  - complaints about the improper collection, use or disclosure of PI

Complaints to the IPC

s. 317 - 318, 320 - 322, 325

- IPC may **conduct a review** in response to a complaint or conduct a **self-initiated review** about a contravention
- During a review, IPC has power to enter and inspect premises, require access to PI, and compel testimony
- After review, IPC has power to make **orders** and recommendations regarding access and correction and collection, use and disclosure in regard to service providers, their agents or employees
  - The IPC may decide not to issue an order
- IPC orders can be **appealed** to the Divisional Court, and individuals may seek **damages** for harm and/or mental anguish

PHIPA Processes Flowchart



* The above process may be varied at the discretion of the IPC to achieve the fair, just and timely resolution of proceedings before the Commissioner or his delegates. Note specifically that urgent matters may be expedited to the adjudication stage.
** In addition to the general procedures outlined in the above flowchart, Intake also adjudicates time-sensitive complaints related to deemed refusals, failures to provide access and expedited access requests.

IPC's General Powers
s. 326

- **IPC's general powers include:**
  - engaging in research about carrying out Part X
  - conducting public education programs and providing information about Part X and the IPC's role
  - receiving representations from the public about the operation of Part X
  - offering comments on a service provider's information practices (when requested)
  - assisting investigations of other Commissioners across Canada
  - authorizing the indirect collection of PI

Offences and Immunity

s. 331 and 332

- Offences under Part X include
  - wilfully collecting, using or disclosing PI in contravention of Part X or its regulations
  - disposing records of PI to evade an access request
  - wilfully disposing a record in contravention of the record handling provisions
  - wilfully failing to notify an individual of a breach of their PI
  - wilfully obstructing the Commissioner
- The max fine for conviction is $5,000
- Service providers are protected against actions or other proceedings for damages where they have **acted in good faith** and reasonably in the circumstances

Supporting Implementation

- The IPC wants to work with the child welfare sector, along with other sectors and the Ministry of Children and Youth Services, to support implementation
  - Consultation, Co-operation, Collaboration
- Providing information and education is part of the IPC's role. For the *CYFSA*, this will include:
  - Tools, training and guidance documents for service providers and for the public
  - Dedicated phone-line for *CYFSA* queries
- Your feedback and questions will guide the development of new tools and trainings

Privacy Breaches:
Best Practices for Prevention

Common Causes of Privacy Breaches

Common Causes of Privacy Breaches

1. Insecure disposal of records
2. Lost/stolen portable devices
3. Unauthorized access (snooping)

Common Causes of Privacy Breaches

1. Insecure disposal

- records intended for shredding are **recycled**
  - film shoot case (IPC order HO-001)
- improper **destruction** of electronic records
  - hard drives not wiped/destroyed
- records **abandoned** when business transfer or termination
  - common in health sector (doctors, dentists)
  - *PHIPA* Decision 23 (2016)

Common Causes of Privacy Breaches

2. Lost/stolen portable devices

- IPC order HO-008 (2010)
  - hospital laptop stolen from employee's car
  - device not encrypted
- IPC Elections Ontario Investigation (2012)
  - unencrypted USB key lost with voting PI of up to 2.4 million people

Common Causes of Privacy Breaches

3. Unauthorized access

- malware
  - e.g. ransomware that locks organization out of its data
- stolen credentials to access system
- snooping
  - IPC order HO-013 (Rouge Valley Hospital, 2014)
    - staff selling new baby info RESP companies
  - interpersonal conflicts, personal gain, curiosity

Reducing Risk of Privacy Breaches

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

1. Administrative
2. Technical
3. Physical

Reducing Risk of Privacy Breaches

1. Administrative

- privacy and security policies and procedures
- **auditing** compliance with rules
- privacy and security **training**
- data minimization ("need to know" limit)
- confidentiality agreements (alone or part of broader contracts)
- other means of communicating privacy messages (privacy notices, warning flags)
- privacy impact assessments

Reducing Risk of Privacy Breaches

2. Technical

- strong authentication and access controls
- detailed logging, auditing, monitoring
- strong passwords, encryption
- patch and change management
- firewalls, hardened servers, intrusion detection and prevention, anti-virus, anti-spam, anti-spyware
- protection against malicious and mobile code
- threat risk assessments, ethical hacks

Reducing Risk of Privacy Breaches

3. Physical

- controlled access to premises
- controlled access to locations within premises where identifying information is stored
- access cards and keys
- identification, screening, supervision of visitors

Reducing Risk of Privacy Breaches

- In determining what safeguards are applicable, consider:
  - **sensitivity** and **amount** of information
  - number and nature of **people with access** to the information
  - **threats** and **risks** associated with the information

Responding to a Privacy Breach

Information and Privacy Commissioner of Ontario

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

Responding to a Privacy Breach

1. Implement, Identify, Contain

- implement privacy breach management policy
- determine if actual breach
- identify PI breached
- notify senior management
- **containment measures** to prevent further harm:
  - prevent further copies of records
  - ensure records retrieved/disposed of

Responding to a Privacy Breach

2. Notify

- notice to individuals (*CYFSA* requires, s. 308(2))
- form, timing of notice (direct or indirect?)
- notice should contain:
  - nature and extent of breach
  - nature and extent of PI
  - containment steps taken
  - any further actions the organization will take
  - be **transparent!**

Responding to a Privacy Breach

2. Notify

- Service providers will be **required to notify the IPC and Minister** under *CYFSA* (s. 308(3)) about certain privacy breaches
- These requirements will be prescribed by regulation

Responding to a Privacy Breach

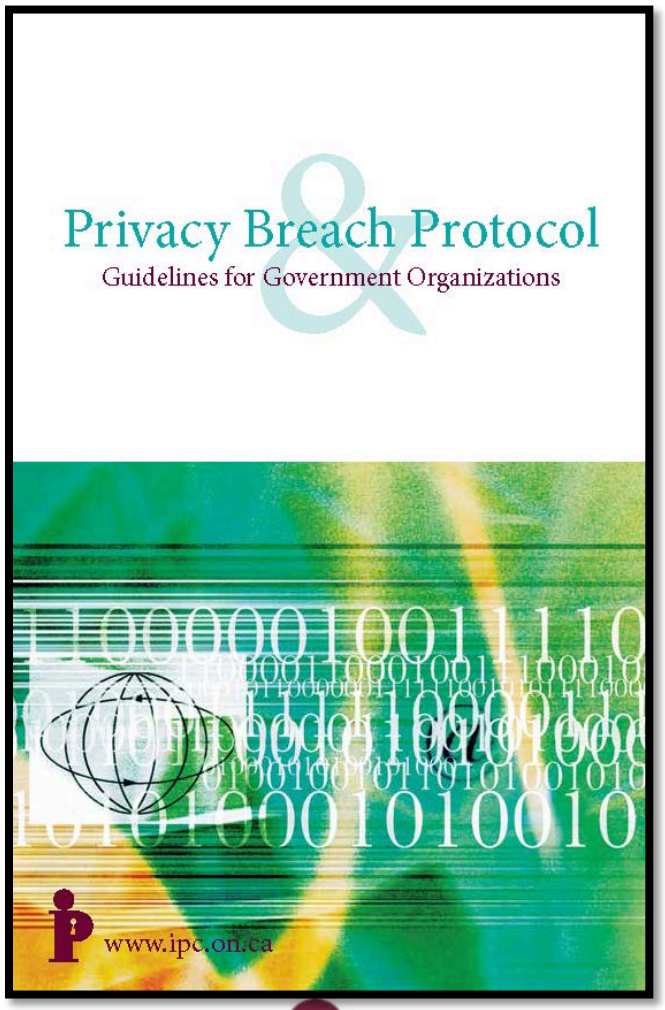
3. Investigate and remediate

- conduct internal investigation to:
  - review containment measures taken
  - determine if breach effectively contained
  - ensure individuals notified
  - review circumstances of breach
  - review adequacy of policies and procedures
  - recommendations to prevent future breaches
- document investigation, recommendations
- implement recommendations

IPC Guidance

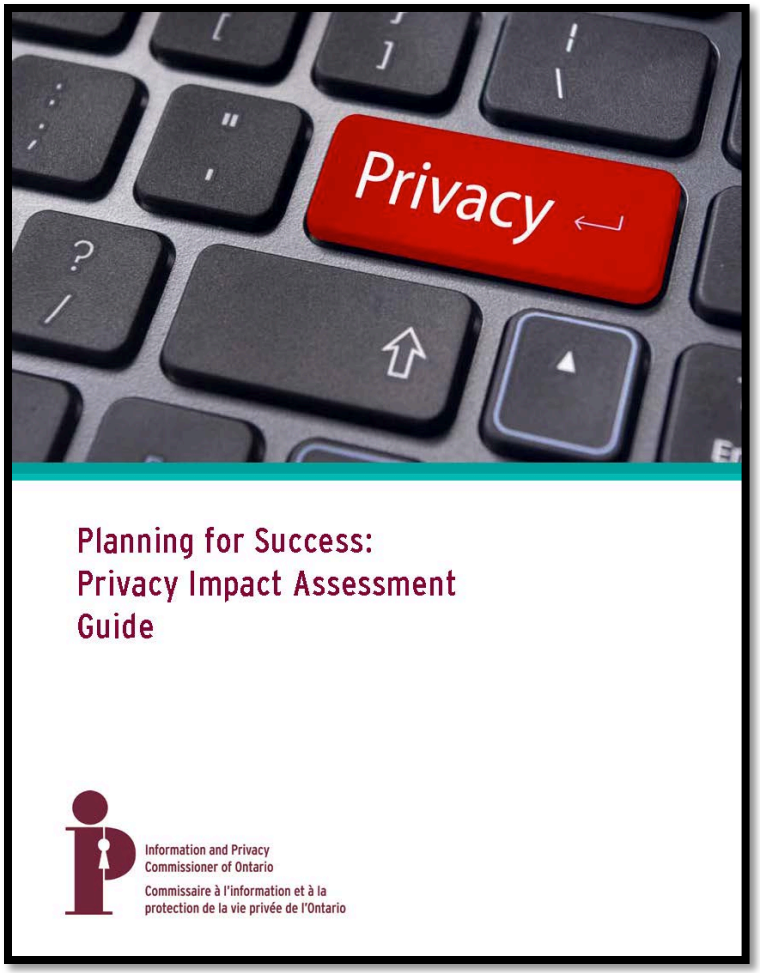
Privacy Breach Protocol Guide

- privacy breach protocol helps identify privacy risks, potential and actual breaches
- ensure training on protocol
- ensure staff know their responsibilities when a breach occurs

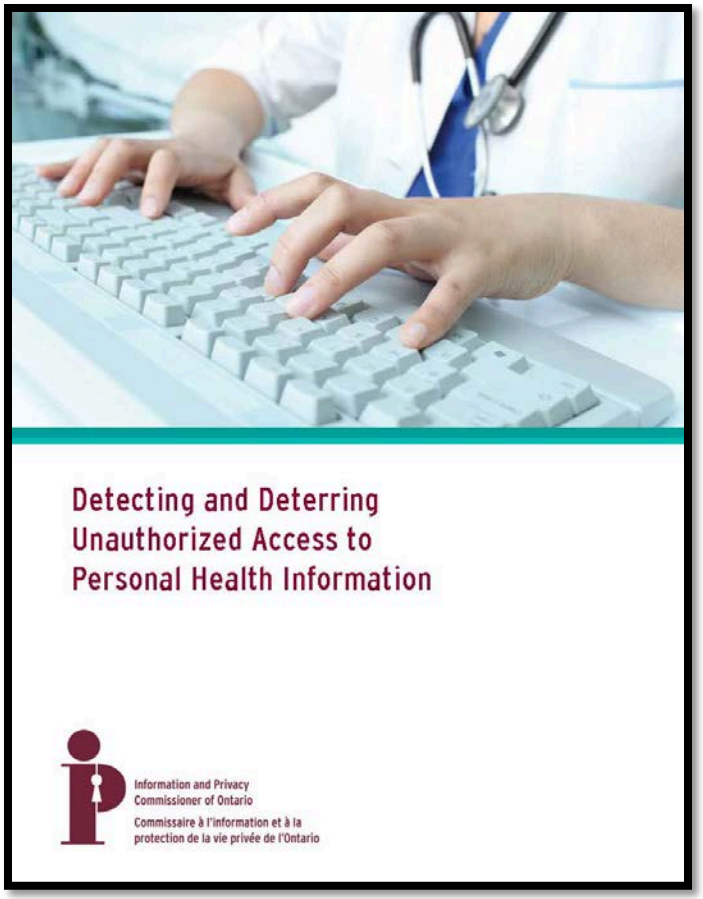


Privacy Impact Assessment Guide

- PIAs are tools to identify privacy impacts and risk mitigation strategies
- PIAs are widely recognized as a **best practice**
- step-by-step advice on how to conduct a PIA from beginning to end



Guidance on Snooping



- benefits and risks of electronic records
- impact of unauthorized access
- **reducing the risk** of unauthorized access
- recent ON convictions added deterrence

Contact Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

(416) 326-3333 / 1-800-387-0073
TDD/TTY: 416-325-7539
www.ipc.on.ca
info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965