Access and Privacy Under Part X of the *Child, Youth and Family Services Act*

Brian Beamish

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

OARTY ANNUAL CONFERENCE

June 13, 2019

Our Office

- Provides independent review of government decisions and practices on access and privacy
- Commissioner is appointed by, and reports to, the Legislative Assembly to ensure impartiality
- Oversees Ontario's access and privacy laws
- These laws establish the public's right to access government-held information and protect their personal privacy rights

IPC's Mandate

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - Covers 300 provincial institutions
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - Covers 1,200 municipal organizations
- *Personal Health Information Protection Act* (*PHIPA*)
  - Covers individuals and organizations involved in the delivery of health care services
- Expanded Mandate: *Child, Youth and Family Services Act*

Child, Youth and Family Services Act

- Based on PHIPA, Part X represents a big step forward for Ontario's child and youth sectors:
  - closes a legislative gap for access and privacy
  - promotes transparency and accountability
  - uses consent-based framework; presumption of capacity
  - rights of individuals to access/correct their personal information
  - requires mandatory privacy breach reporting

Part X and Personal Information

Who is Covered by Part X?

- Any person or entity providing a service funded under the *CYFSA*
- A *CYFSA* licensee (e.g., group and foster care licensees – foster parents are **not** service providers under Part X)
- All children's aid societies, including Indigenous societies

- Service providers are **exempt** from the core rules of Part X if they are already covered by Ontario's other access and privacy laws:
  - institutions under *FIPPA* or *MFIPPA*
  - health information custodians under *PHIPA*

What Information is Covered by Part X?

- Part X contains requirements for records of personal information which are:
  - collected for or relating to the provision of a service (under the *CYFSA)*
  - in the custody or control of a service provider
  - recorded before or after Part X comes into force
- Exceptions:
  - Part X does not apply to records related to finalized adoptions
  - An individual cannot access information under Part X if access is restricted under the *Youth Criminal Justice Act*

Collection, Use and Disclosure

Consent

- Consent is required for the collection, use and disclosure of personal information, with some exceptions
- Even with consent, there are limits:
  - only as much personal information as necessary for providing service
  - only where other (non-personal) information won't suffice

Indirect Collection Without Consent

Permitted:

- ✓ Required or permitted by law
- ✓ To assess/reduce risk of serious harm or provide service, **and** you can't get accurate or timely information directly
- ✓ Between children's aid societies, to assess/reduce risk of harm to a child

Not permitted:

- ✗ Information not necessary to provide a service or assess/reduce harm
- ✗ Collecting excessive information (e.g., political affiliation)

Use of Information Without Consent

Permitted:

- ✓ Use for the purpose the info was collected, including providing to your employees/agents
- ✓ To assess/reduce risk of serious harm to any person
- ✓ Planning, managing services
- ✓ Quality assurance

Not permitted:

- ✗ Snooping (e.g., reading neighbour's record out of curiosity or genuine concern)
- ✗ Using more information than necessary (e.g., reading whole file when you only need phone number)
- ✗ Using information for personal financial gain

IPC Decision: Snooping

- *PHIPA* Decision 64 - A hospital reported a breach involving a registration clerk who viewed the health records of a media-attracting patient and 443 other patients without authorization
  - the breach was discovered by the hospital during a proactive audit and reported to the IPC
  - the clerk was fired from the hospital and pled guilty to breaking Ontario's health privacy law
- The IPC concluded:
  - employee used personal information in contravention of *PHIPA*
  - hospital had sufficient safeguards in place

Disclosure Without Consent

Permitted:

- ✓ Required or permitted by law
- ✓ To assess/reduce a risk of serious harm to any person
- ✓ To law enforcement to aid an investigation

Not permitted:

- ✗ To friends or relatives of the client, if there's no reason for them to receive the information
- ✗ To former service providers wondering how the client is doing

Protecting Personal Information

- Service providers must take reasonable steps to ensure personal information is:
  - protected against theft, loss and unauthorized use or disclosure
  - protected against unauthorized copying, modification or disposal
  - retained, transferred and disposed of in a secure manner

- *PHIPA* Order 4
  - Unencrypted hospital laptop with health information of 2,900 people stolen from a car
  - IPC found the hospital had not taken reasonable steps to protect the information
  - IPC ordered hospital to put in place or revise certain policies, procedures and staff training

Privacy Controls

Administrative:

- privacy and security policies
- privacy and security training

Physical:

- controlled access to premises
- identification, screening, supervision of visitors

Technical:

- strong authentication and access controls
- firewalls and anti-malware scanners
- detailed logging, auditing, monitoring

Mandatory Breach Notification

- If personal information is stolen or lost, or if it is used or disclosed without authority, you must notify the individual right away
- You must also notify the IPC and minister of significant privacy breaches involving:
  - a part of a pattern of similar breaches
  - theft of personal information
  - personal information being used or disclosed by someone who knew they were doing so without authority
  - personal information being further breached
  - an employee being terminated or disciplined, or resigning

Consent and Capacity

Obtaining Consent

- In most cases, you must get consent before collecting, using or disclosing personal information
- Consent can be:
  - implied in some cases (e.g., direct collection)
  - written or oral (if you make a written record of it)
- Consent must be:
  - given by the individual (if capable) — or their substitute decision-maker
  - given freely and voluntarily
  - related to the information that you are collecting, using or disclosing
  - knowledgeable

Capacity

- A capable individual of any age may give, withhold or withdraw consent.
- To be capable means being able to understand:
  - the information that is relevant to deciding whether to consent
  - the consequences of giving or withholding the consent
- You can assume someone is capable — unless you have reason to believe otherwise
- Service providers are responsible for determining capacity under Part X
  - people can challenge decisions of incapacity through Ontario's Consent and Capacity Board

Substitute Decision-Makers

- Can, on behalf of an individual:
  - consent to the collection, use or disclosure of information
  - give instructions and make requests, including access requests
- Part X explains who can be a substitute decision-maker for:
  - incapable individuals of any age
  - capable individuals over the age of 16 (with their written authorization)
  - children under the age of 16, whether capable or not
- A custodial parent or children's aid society can be substitute decision-maker for a child under the age of 16 (subject to exceptions):
  - if there's a conflict, the capable child's decision prevails

Access and Corrections

Access Rights

- Individuals have the right to access records of their personal information in a service provider's custody or control that relate to the provision of a service to them
- There are some exceptions to the right of access
- If an exception applies to part of a record, you must sever or redact the record and provide access to the remaining part

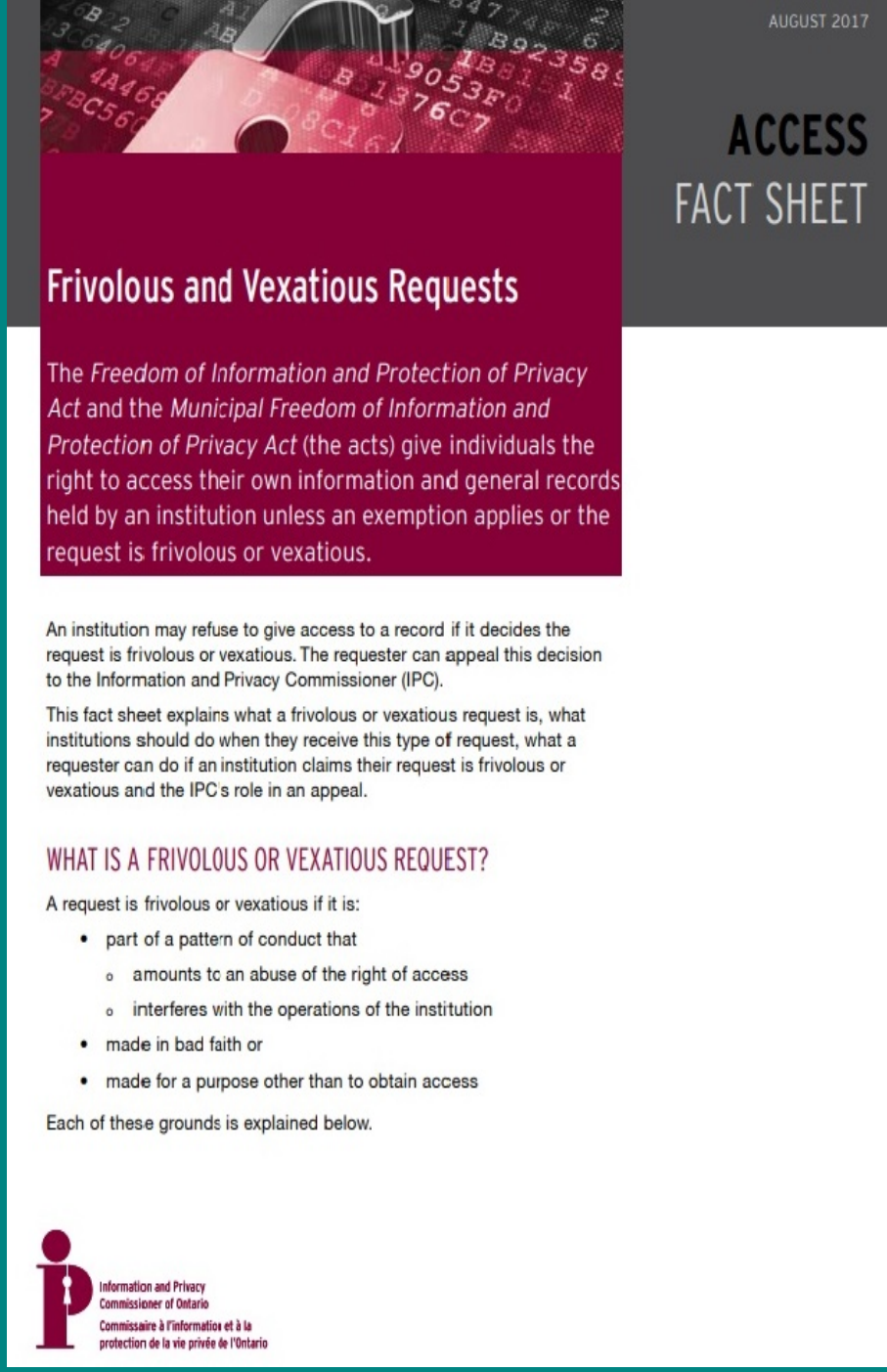
Access Exceptions

An individual does not have a right of access if:

1. A legal privilege restricting disclosure applies
2. Another act or court order prohibits disclosure
3. The information in the record was collected for a proceeding that has not concluded
4. Granting access could result in a risk of serious harm to any individual
5. Granting access could lead to identification of someone who was required by law to give the information
6. Granting access could identify a confidential source (discretionary)

Access Exceptions

- Service providers may refuse access requests that are **frivolous or vexatious** or made in bad faith
- **Example:** request made for the purpose of harassing the provider
- High threshold for deciding that a request is frivolous or vexatious



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

IPC Decisions: Risk of Harm

- **Decision 34**: Individual was denied access to his information from a mental health facility — risk of harm to the nurses who drafted the records.
  The IPC:
  - reviewed evidence provided by the facility, including psychiatrist notes
  - upheld the decision to deny access based on risk of harm

- **Decision 87**: Private clinic denied access – request made in bad faith, and access would result in harm.
  The IPC:
  - found that the client's alleged failure to pay for the clinic's services was not grounds for finding that his request for access was made in bad faith
  - found that the risk of harm was speculative or unlikely
  - ordered the clinic to provide the client with access to the record

Access Requests and Other People's Privacy

- There is no overarching access exception that requires you to redact other people's information before granting access
- Depends on if the record is dedicated primarily to the provision of a service to the individual requesting access:
  - if yes, they have a right to access the entire record (subject to the six exceptions) even if it incidentally contains information about other individuals and other matters
  - if no, they have a right to access only their own personal information from the record

Responding to an Access Request

You must respond in writing **within 30 calendar** days:

- grant access (make record available or provide a copy)
- refuse access
- extend the deadline for a full response (up to 90 days)

Refusing Access

- When refusing access in whole or in part, you must provide a written explanation (e.g., because a legal privilege applies)
- Individuals can complain to the IPC if their access request is refused or if there's no response ("deemed refusal")
- IPC has an accelerated process for resolving deemed refusal complaints:
  - in 2018, the IPC closed 58 deemed refusal complaints under *PHIPA* (36% of total *PHIPA* access/correction complaints)
  - 56 of these were resolved without an order

Correcting Records

- Individuals have the right to request correction of their information
- You must correct the record if they demonstrate to your satisfaction that it is inaccurate/incomplete, and they give you the correct information
- You are not required to correct the record if:
  - it was not originally created by your organization, and you lack sufficient knowledge, expertise or authority to correct it
  - it consists of a professional opinion or observation made in good faith
- Individual requesting the correction can require that you attach a statement of disagreement to the record

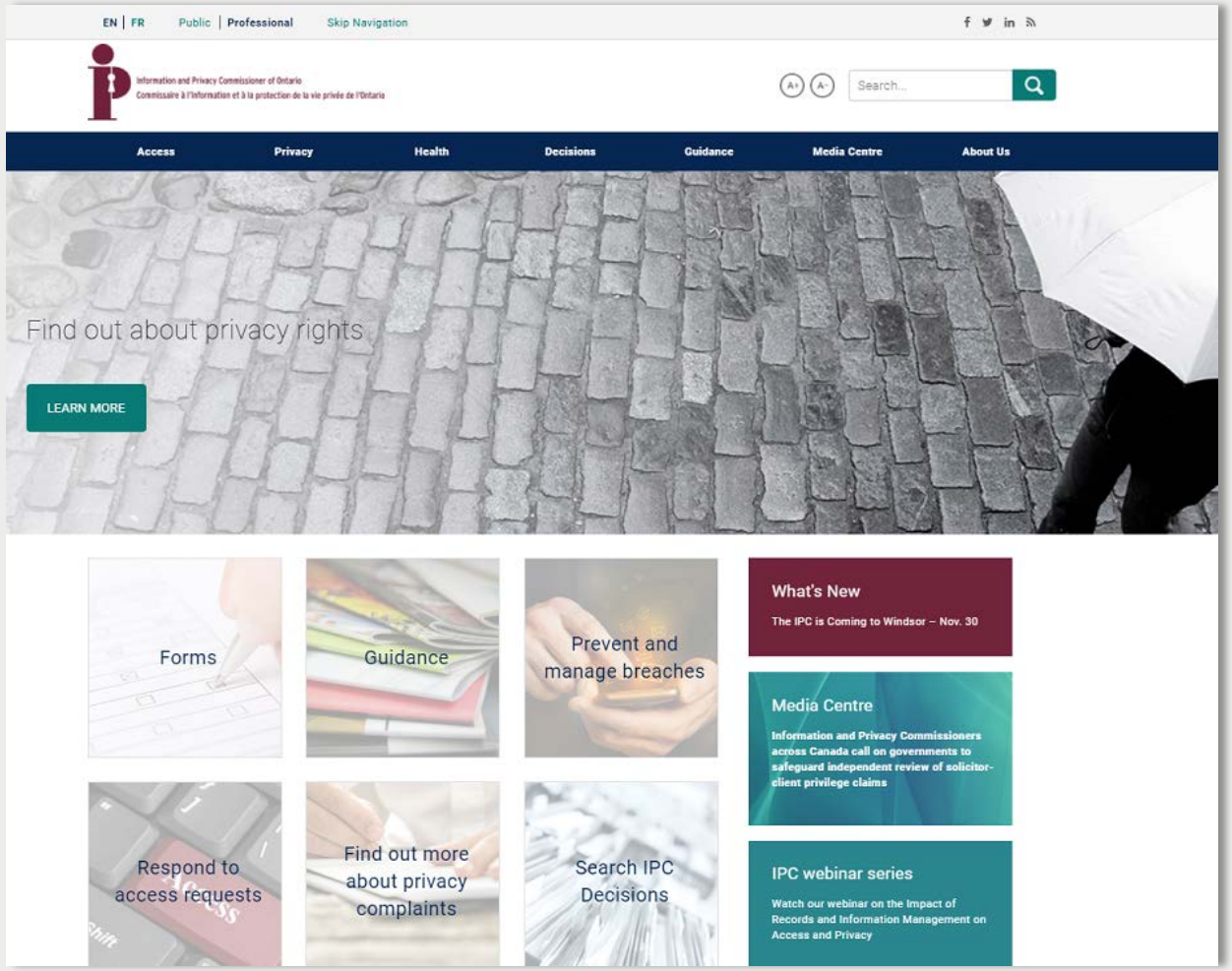
IPC Decision: Professional Opinion

- **Decision 67**: Community Care Access Centre received a 62-part request for correction of a social worker's assessment report
  - two corrections made and refused the rest — on the grounds these were the social worker's professional opinions and observations made in good faith
  - IPC upheld the decision of the care centre — agreed these were professional opinions or observations gained from the exercise of special knowledge, skills, qualifications, judgment or experience relevant to the profession
  - IPC found insufficient evidence to disprove the presumption of good faith — no evidence of malice, intent to harm, serious carelessness or recklessness

Role of the IPC

Role of the IPC

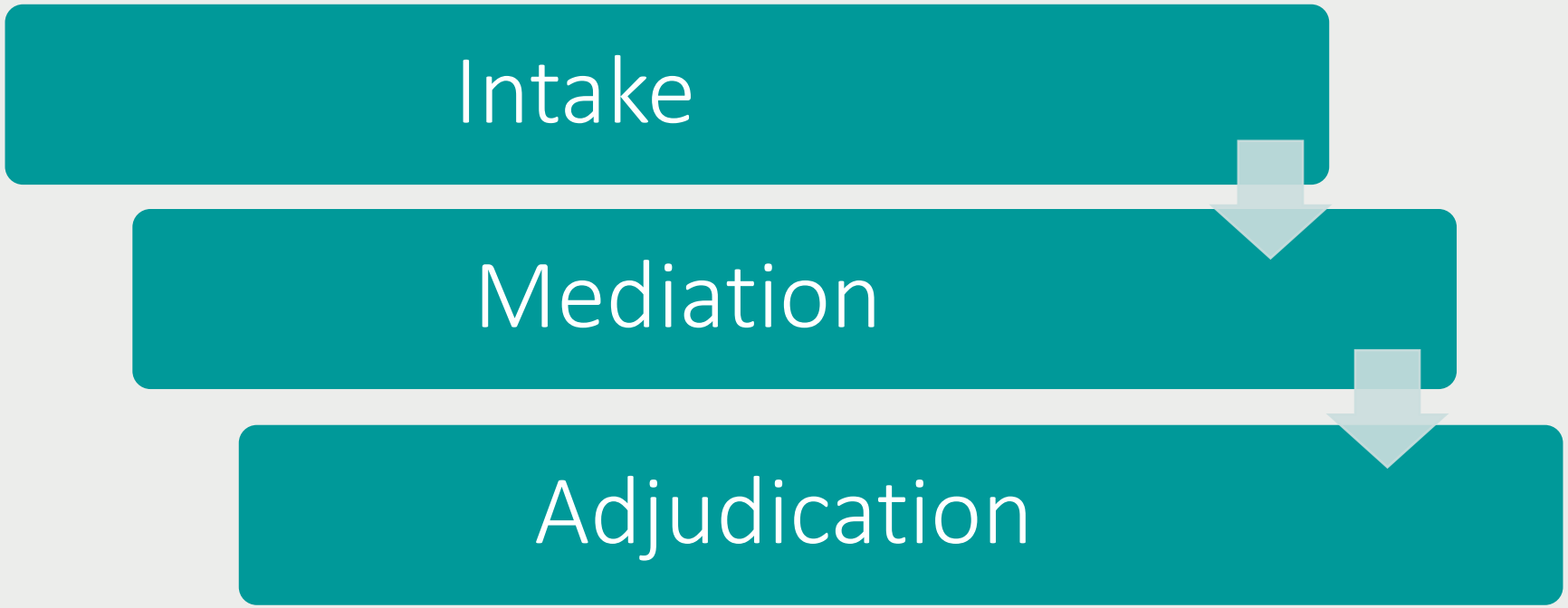
- As the oversight body for Part X, the IPC's role includes:
  - resolving complaints
  - receiving notification of significant privacy breaches
  - publishing annual statistics about Part X
  - supporting application of Part X (public education, guidance materials)



Complaints

- Anyone can complain to the IPC if they believe that someone has broken any Part X rule (or is about to)
- Complaints must be filed in writing within:
  - six months for access and correction refusals (including deemed refusals)
  - one year for all other types of complaints
- The IPC may conduct a review in response to a complaint or self-initiate a review

IPC Complaints Process



- Most complaints are **resolved** before reaching the adjudication stage

Intake Stage

- All complaints are received by the IPC registrar
- The registrar or intake analyst may attempt to resolve the complaint informally
- Complaint can be dismissed at an early stage if:
  - it is clearly outside the IPC's jurisdiction
  - the IPC is satisfied with your response to the complaint

Mediation

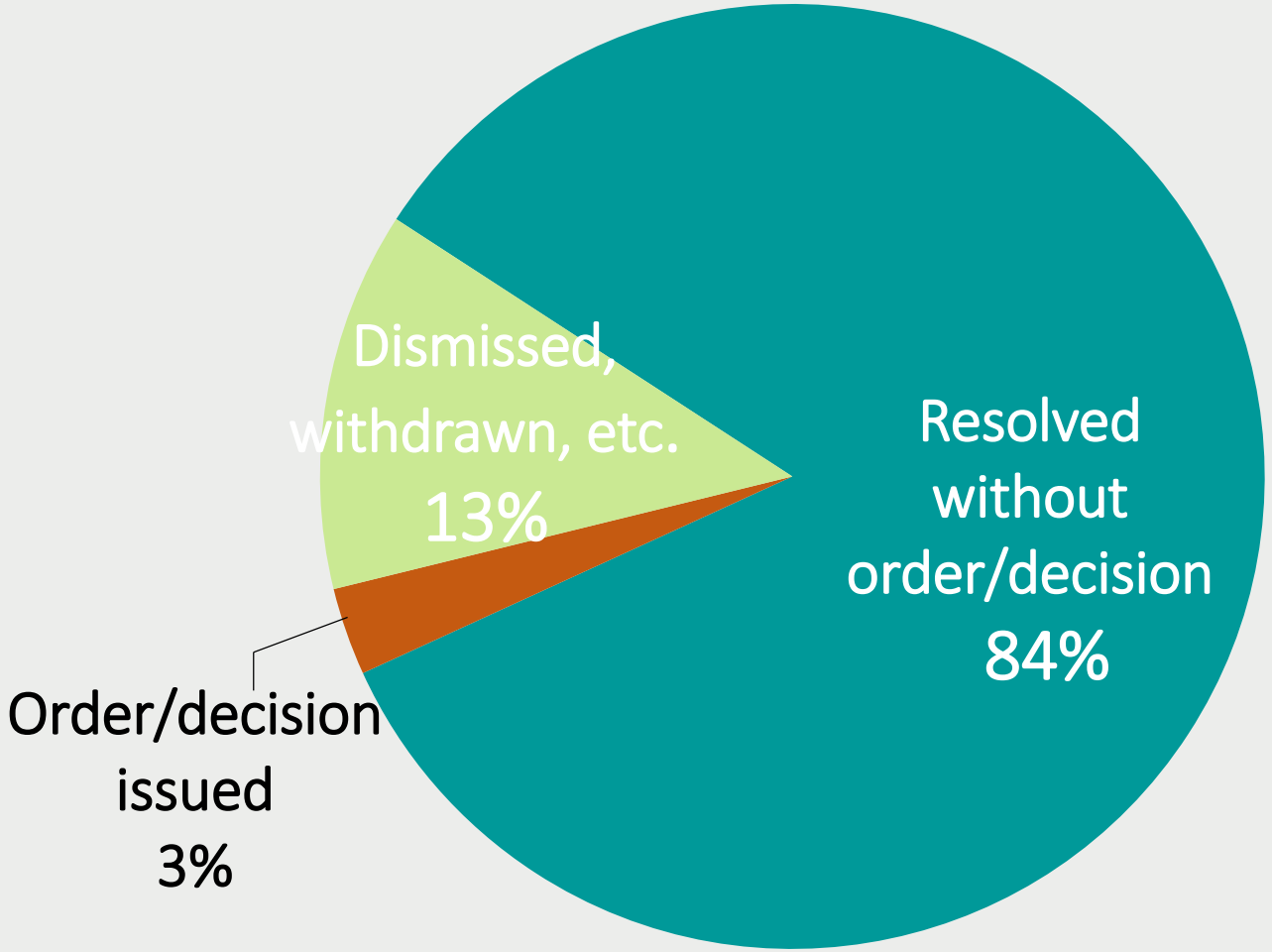
- Complaints not resolved at intake may be sent to mediation
- Mediation is usually conducted by telephone, with the IPC mediator speaking separately with each party
- IPC mediator acts as a neutral third party
  - goal is to find a resolution which satisfies the needs of all involved
  - saves significant time and resources for all parties

Adjudication

- If a complaint can't be resolved informally, the IPC may decide to conduct a formal review:
  - reviews typically conducted in writing
  - IPC has broad powers during a review – for example, to require access to a record
- After review, the IPC may make orders and recommendations:
  - may order a record be provided to an individual
  - recommend that a privacy practice be put in place
- IPC orders can be appealed to Ontario's Divisional Court

Early Complaint Resolution

- Most complaints are resolved before reaching the adjudication stage
- 97% of *PHIPA* complaints and breach reports in 2018 (727) were resolved without an order or decision



Privacy Breach and Statistics Reporting

- Service providers must report significant privacy breaches to the IPC
  - IPC will look into the circumstances of the breach and may decide to investigate
- The IPC collects annual statistics from all service providers
- The first report due in March 2021 to include:
  - the number of Part X access and correction requests received in 2020
  - how often you responded within 30 days, or within up to 90 additional days
  - how often you refused to provide access or correction, and on what grounds
  - number and types of privacy breaches (e.g., loss, theft, etc.)

Mandatory *PHIPA* Breach Reporting

- As of October 1, 2017, health information custodians are required to notify IPC of certain privacy breaches
  - use or disclosure without authorization
  - stolen information
  - further use or disclosure
  - breaches occurring as part of a pattern
  - breaches related to a disciplinary action against a college or non-college member
  - significant breaches
- Custodians began collecting breach statistics in January 2018 for reporting in March 2019

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.

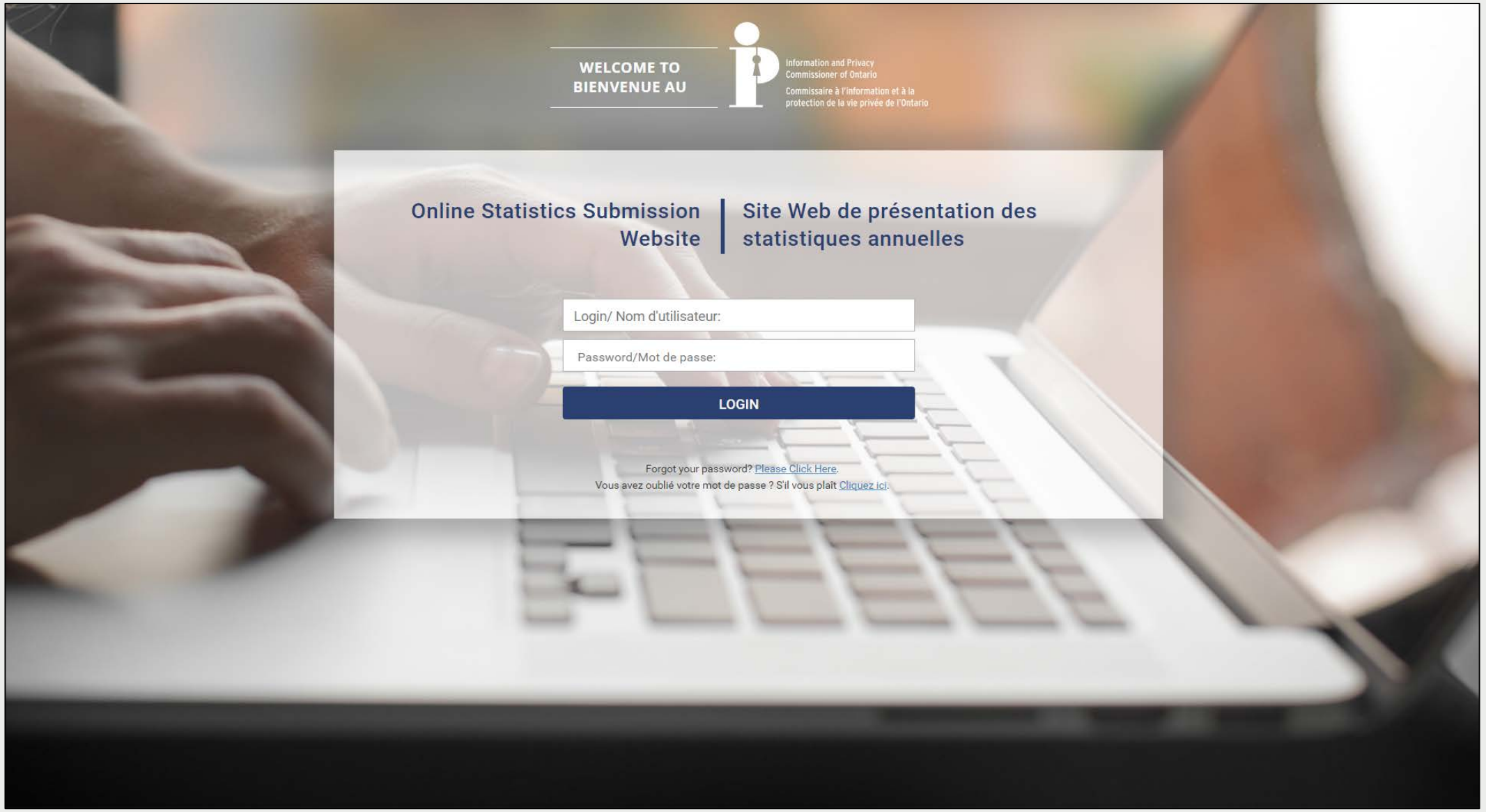
It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

1. Use or disclosure without authority

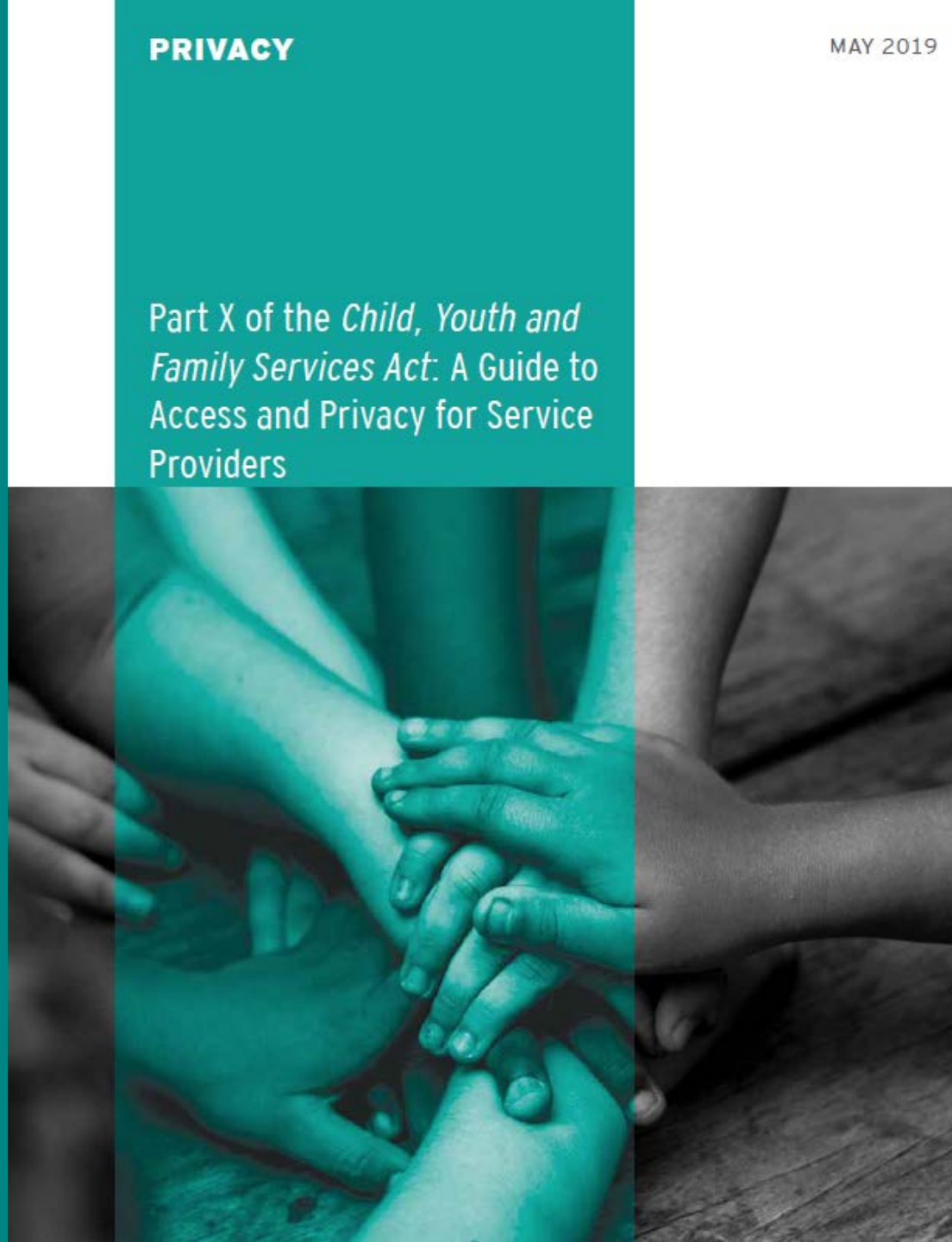
This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

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


WELCOME TO
BIENVENUE AU
Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario
Online Statistics Submission Website
Site Web de présentation des statistiques annuelles
Login/ Nom d'utilisateur:
Password/Mot de passe:
LOGIN
Forgot your password? Please Click Here.
Vous avez oublié votre mot de passe ? S'il vous plaît Cliquez ici.

IPC Guidance Materials

- Guide to Part X for service providers
- Searchable web-based FAQs
- Detailed fact sheets about processing access requests
- Information about preventing, responding to, and reporting privacy breaches
- Youth-focused materials
- Orders and decisions



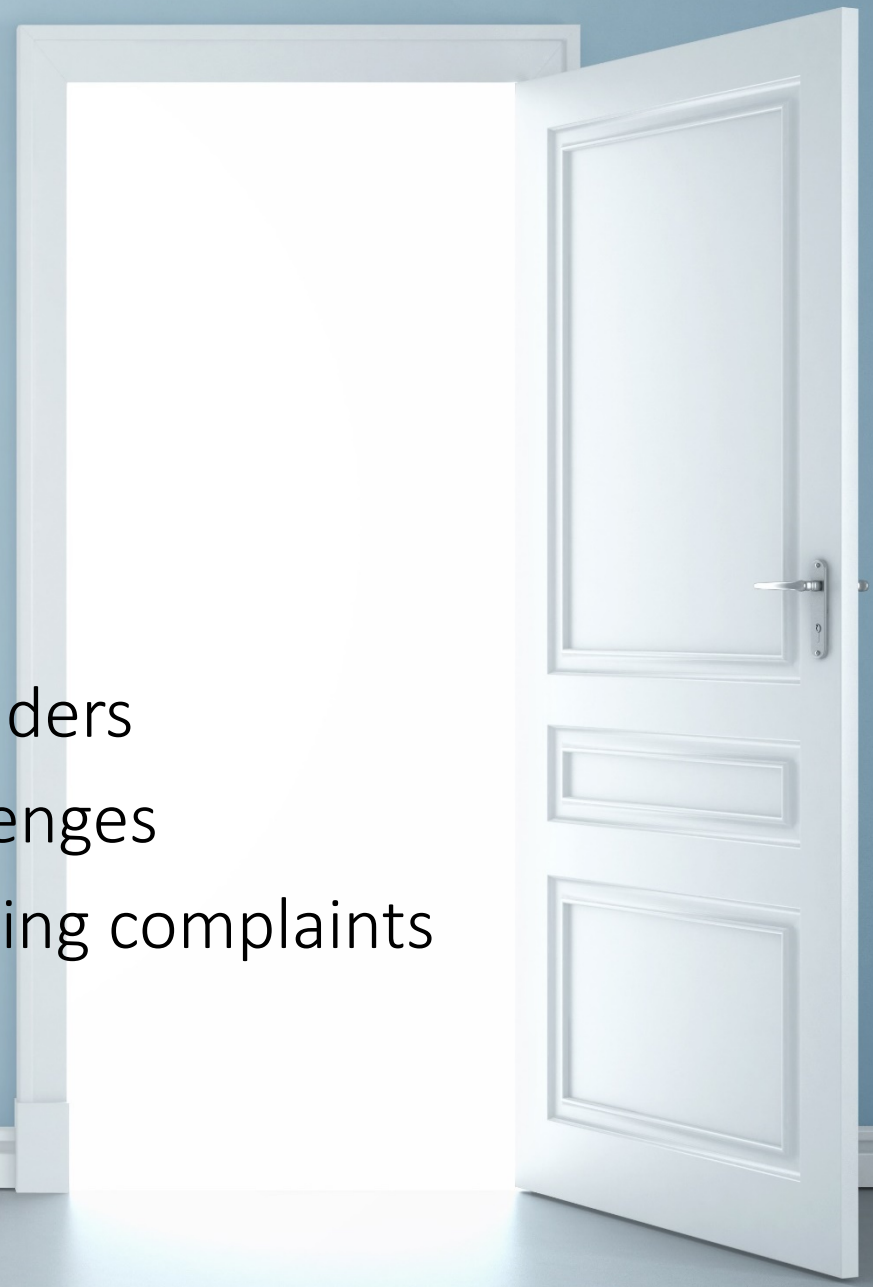
Our Open Door Policy

Any public institution or agency considering programs with privacy impacts can approach the IPC for advice

Consultation: open communication with stakeholders

Collaboration: working together to address challenges

Co-operation: rather than confrontation in resolving complaints



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