REACHING OUT TO ONTARIO

PART X of the *CHILD, YOUTH AND FAMILY SERVICES ACT*

Brian Beamish, Commissioner

Emily Harris-McLeod, Senior Policy Advisor

Sudbury

October 11, 2019

Agenda

- Part X of the *Child, Youth and Family Services Act, 2017 (CYFSA)*:
  - Background
  - Application of Part X (who and what is covered?)
  - Privacy rules
  - Consent and capacity
  - Access and correction rules
  - Role of the IPC

Background

Brian Beamish, Commissioner

Background

- The *CYFSA* replaced the *Child and Family Services Act* in 2018
  - governs many of Ontario's programs and services for children and youth, including child protection and residential services
- The paramount purpose of the *CYFSA* is to promote the best interests, protection and well-being of children
  - one additional purpose is to recognize that appropriate sharing of information to plan and provide services is essential for creating successful outcomes for children and families

Background

- Part X of the *CYFSA* is new. As of January 1, 2020, it will:
  - establish rights for individuals to access and request correction of their information
  - set out privacy rules that service providers must follow
- Part X is modeled on Ontario's health privacy law (*PHIPA*)

Strengths of Part X

- Part X represents a big step forward for Ontario's child and youth sectors:
  - closes a legislative gap for access and privacy
  - facilitates transparency and consistency among service providers' information practices
  - consent-based framework
  - presumption of capacity
  - individuals' right of access to their PI
  - mandatory privacy breach reporting
  - oversight powers for IPC to ensure that complaints are properly reviewed

Role of the IPC

- The IPC is the oversight body for Part X. Our role includes:
  - resolving complaints
  - receiving notification of significant privacy breaches
  - publishing annual statistics about Part X
  - supporting implementation (public education, guidance materials)
- The commissioner is appointed by and reports to the Legislative Assembly, and is independent of government

Application of Part X

Who is Covered by Part X?

- Part X contains requirements for service providers, which includes:
  - any person or entity that provides a service funded under the *CYFSA*
  - all children's aid societies
  - all *CYFSA* licensees (e.g., group and foster care licensees. However, foster **parents** are not service providers)

Who is Covered by Part X?

- Service providers are **exempt** from the core rules of Part X if they are already covered by other privacy legislation:
  - institutions under *FIPPA* or *MFIPPA*
  - health information custodians under *PHIPA* - when handling personal health information

What 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
- Some exceptions:
  - Part X does not apply to records related to finalized adoptions
  - The *Youth Criminal Justice Act* prevails over Part X. An individual cannot access information under Part X if restricted under the *YCJA*

What is Covered by Part X?

- **Personal information** (PI) is recorded information about an identifiable individual:
  - even without a name, may be PI if the individual can be identified
  - does not include information associated with an individual in a professional capacity, or a person deceased for over 30 years
- **Record** means a record of information in any form:
  - includes electronic records, audio recordings, paper records, etc.
  - when *collecting* information, the definition of PI also includes information that is not recorded (e.g., intake interview)

Part X Privacy Rules

Collection, Use and Disclosure

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

Direct Collection

- PI is often collected directly from the individual, with consent
  - you must notify people that their PI may be used or disclosed in accordance with Part X
- Direct collection **without** consent is permitted in limited circumstances
  - Example: CAS collecting PI where necessary to assess/reduce risk of harm to a child

Indirect Collection Without Consent: Examples

Permitted:

- ✓ Required or permitted by law (e.g., duty to report)
- ✓ To assess/reduce risk of serious harm or provide service, **and** you can't get accurate or timely information directly
- ✓ Between CASs, to assess or reduce risk of harm to a child

Not permitted:

- ✗ Information not necessary to provide a service or assess/reduce harm
- ✗ Information **is** necessary to provide a service/reduce harm, but you are able to obtain it directly

Use of Information Without Consent: Examples

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)

IPC Decision Under Health Privacy Law

- ***PHIPA* Decision 64** - A hospital clerk 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 contravening *PHIPA*
- The IPC concluded:
  - the employee had used PI in contravention of *PHIPA*
  - the hospital had sufficient safeguards in place

Disclosure Without Consent: Examples

Permitted:

- ✓ Required/permitted by law (e.g., disclosure to First Nation, Métis, Inuit communities where required by the *CYFSA*, s. 73)
- ✓ Necessary 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

Protection of PI

- Service providers must take reasonable steps to ensure PI 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:
  - Theft of hospital laptop from doctor's car. Contained unencrypted health information of 2900 people. Hospital alerted IPC.
  - 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: Examples

- Administrative controls:
  - privacy and security policies
  - staff training
- Physical controls:
  - controlled access to premises
  - identification, screening, supervision of visitors
- Technical controls:
  - strong authentication and access controls
  - firewalls and anti-malware scanners
  - detailed logging, auditing, monitoring

Mandatory Breach Notification

- If PI is stolen or lost, or if it is used or disclosed without authority, you must notify the individual right away, including:
  - description of what happened
  - steps taken to prevent and mitigate
  - contact information for employee who can answer questions
  - Information about their right to complain to the IPC
- You must also notify the IPC and minister of significant privacy breaches and of breaches that meet certain categories (e.g., theft, pattern of similar breaches)

Notice of Information Practices

- You must make **publicly available** – through your website or other means – an easy-to-understand description of:
  - your policies for handling personal information (e.g., collection, use, disclosure, retention, privacy safeguards)
  - how to access records or request a correction
  - how to contact you
  - your complaints process, and how to file a complaint with the IPC

Key Points for General Staff

- Collect PI directly where possible, and inform people about Part X
  - Notice of information practices – know where to find this
- Understand snooping and how it must be avoided
- Explicit consent is needed for most disclosures
  - However - Part X is **not** a barrier to sharing information where necessary to prevent serious harm, duty to report, etc.
- Privacy breaches: how to avoid them, and who to notify

Consent and Capacity

Consent

- You must get consent before collecting, using or disclosing PI (except in certain cases permitted by the act)
- Consent may be:
  - implied in some cases (e.g., direct collection)
  - written or oral (if you make a written record of it)
- Consent must be given freely and voluntarily by the individual (if capable) — or their substitute decision-maker

Consent

- Consent must be **knowledgeable**, which means it is reasonable to believe the individual knows:
  - the purpose of the collection, use or disclosure, and
  - that they may give, withhold, or withdraw consent
- The individual may put a condition on, or **withdraw** their consent:
  - withdrawal of the consent cannot have a retroactive effect
  - doesn't apply where consent is not required

Capacity

- A capable individual of any age may give, withhold or withdraw consent.
- Capable means being able to understand:
  - the information that is relevant to deciding whether to consent *and*
  - the consequences of giving or withholding the consent
- Presumption of capacity: You can assume someone is capable - unless you have reason to believe otherwise

Capacity

- An individual can be:
  - capable at one time, but not at another
  - capable of providing consent for some parts of their PI, but not others
- Service providers are responsible for determining capacity under Part X
- People can challenge decisions of incapacity through the Consent and Capacity Board

Substitute Decision Makers

- SDMs can, on behalf of an individual:
  - consent to a collection, use or disclosure
  - give instructions and make requests, including access requests
- Part X explains who can be a SDM for:
  - incapable individuals of any age
  - capable individuals over 16 (with their written authorization)
  - a child under age 16, whether capable or not

Substitute Decision Makers

- A custodial parent, CAS or other person authorized to consent on the parent's behalf can act as SDM for a child under age 16
  - Exception - does not apply to PI related to:
    - counselling which the child consented to on their own under the *CYFSA* or
    - treatment about which the child made a decision under the *Health Care Consent Act*
- A decision to give or withhold consent by a capable child prevails over a conflicting decision by the SDM

Key Points for General Staff

- A capable person of any age can give consent
- Capable means being able to understand:
  - the information relevant to deciding whether to consent *and*
  - the consequences of giving/not giving the consent
- Presume someone is capable unless you have reason to think otherwise
- Understand the basic SDM rules, especially regarding children under 16

Access to Information and Correction of Records

Individual's Right of Access

- Individuals have a right to access their PI from a service provider within set timelines and at no charge.
- The records of PI must:
  - be in a service provider's custody or control
  - relate to the provision of a *CYFSA* service to the individual
- There are some exceptions to the right of access
  - if an exception applies to part of a record, they may still have a right to access the remaining part

Exceptions to Access Right

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 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 identify someone who was required by law to give the information
6. Granting access could identify a confidential source
7. The access request is frivolous or vexatious, or made in bad faith

IPC Decisions Under Health Privacy Law

- *PHIPA* 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

- *PHIPA* Decision 87: Private clinic denied access — access would result in serious harm to the individual requester. The IPC:
  - found that the risk of harm described by the clinic was speculative or unlikely
  - ordered the clinic to provide the individual 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 PI before granting access
- It 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** (even if it incidentally contains information about other individuals and other matters)
  - if **no**, they have a right to access only **their own PI** from the record
    - in both cases, one or more access exceptions may apply

Making an Access Request

- Access requests must be made in writing
- Access requests must contain sufficient detail to enable you to identify and locate the record:
  - if not, you must offer assistance in reformulating the request
  - 30 day timeline doesn't start until request contains sufficient detail
- No fees can be charged for access

Responding to an Access Request

- Within 30 calendar days, you must respond in writing in order to:
  - grant access (make record available or provide copy on request)
  - refuse access, and/or
  - extend the deadline for a full response
- You may extend the deadline by up to 90 additional days, but only if responding within 30 days would:
  - unreasonably interfere with operations, because of numerous pieces of information or the need for lengthy search, or
  - not be practical given the time required to assess the individual's right to access

Refusal of 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"):
  - 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

Correction of Records

- Individuals have the right to request correction of their PI
- You **must** correct the record if they demonstrate to your satisfaction it is inaccurate/incomplete, and give you the correct information
- Exceptions: 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; or
  - consists of a professional opinion or observation made in good faith

IPC Decision Under Health Privacy Law

- **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 CCAC - agreed that these were professional opinions or observations (derived from the exercise of special knowledge, skills, qualifications, judgment or experience relevant to the profession)
  - IPC found insufficient evidence to rebut the presumption of good faith: no evidence of malice, intent to harm, serious carelessness or recklessness

Correction of Records

- If you refuse to make a correction, you must advise the requester of their rights to:
  - make a complaint to the IPC
  - draft a statement of disagreement
- If they submit a statement of disagreement, you must attach it to the record and disclose it whenever you disclose the record

Correction Procedures

- Timelines and procedures are similar to access requests:
  - correction requests must be in writing
  - your written response is required within 30 days
  - you may extend the deadline for a full response by up to 90 days, if certain criteria are met
  - no fees may be charged
- Individuals may complain to the IPC if a service provider refuses or doesn't respond to a correction request

Key Points for General Staff

- Individuals have a right to access records of personal information relating to providing them services
- Know where to direct access requests (e.g., certain department)
  - Service provider must respond within 30 days, no fees
- Right to request correction
  - Does not apply to good faith professional opinions
  - If correction is refused, the individual may submit a statement of disagreement

Organizational Readiness

- Assign staff roles (e.g., access department, privacy lead)
- Do inventory of the types of records you hold
- Ensure relevant policies are in place (collection, disclosure, retention, etc.)
- Ensure appropriate privacy safeguards are in place (including staff training)
- Draft a public notice of information practices (website, brochures)
- Know where to go for support (associations, IPC)

REACHING OUT TO ONTARIO

Oversight and Enforcement of Part X

Brian Beamish, Commissioner

Role of the IPC

- As of January 1, 2020, the IPC will be the oversight body for Part X of the *CYFSA*
- 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, and may also self-initiate a review

Role of the IPC

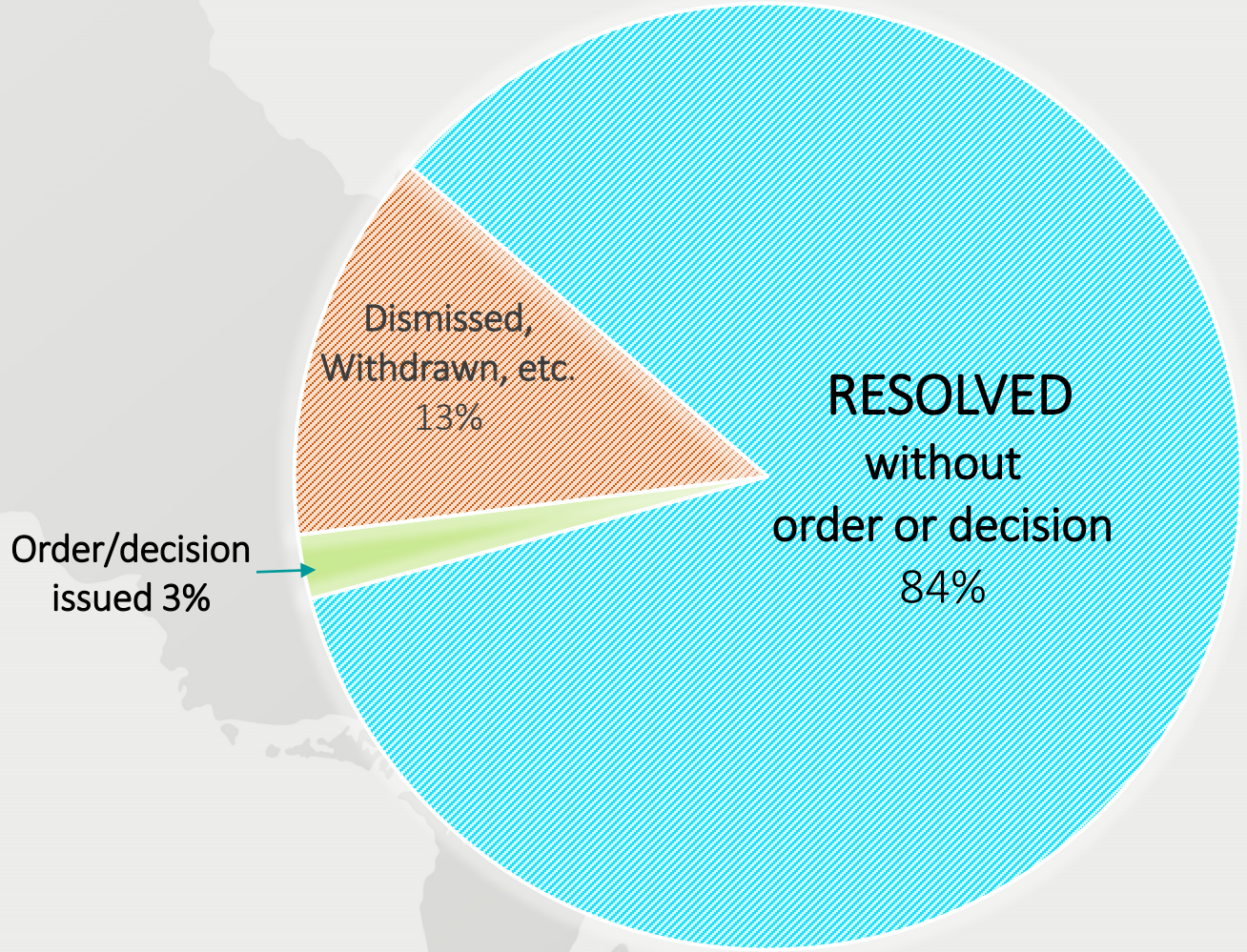
- Service providers must report **significant privacy breaches** to the IPC
  - IPC will look into the circumstances of the breach and **may** decide to investigate
- The IPC collects **annual statistics** from all service providers. The first report is due in March 2021, including:
  - the number of Part X access and correction requests you received in 2020
  - how often you responded within 30 days, or within 90 additional days
  - how often you refused access or correction, and why
  - number and types of privacy breaches

IPC Complaints Process

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

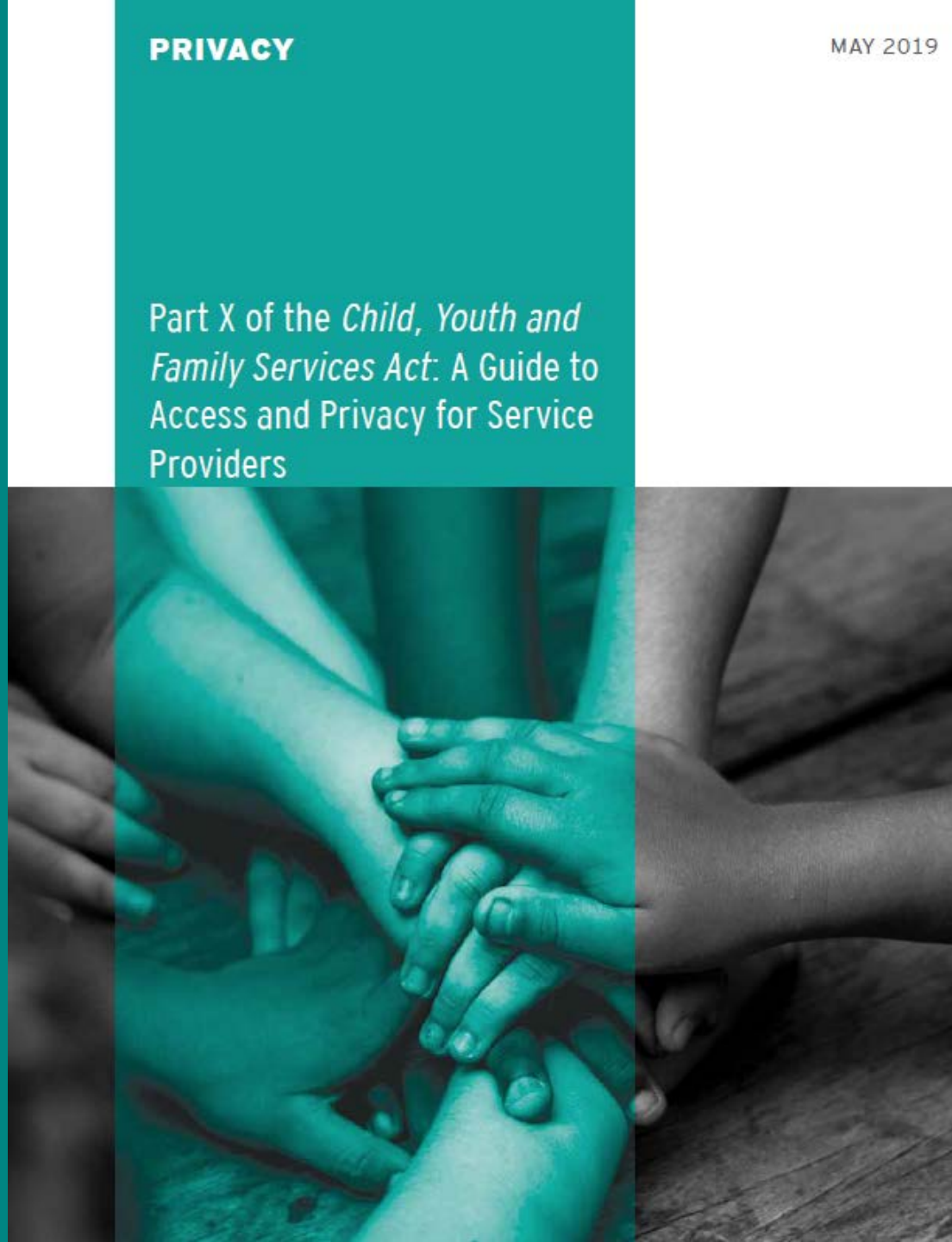
Importance of Early Resolution - PHIPA

- **97%** of *PHIPA* complaints and breach reports in 2018 (727) were resolved without an order or decision



IPC guidance materials

- Guide to Part X for service providers
- Searchable web-based FAQs
- Responding to access requests: Guide for service providers (coming soon)
- Preventing, responding to, and reporting privacy breaches
- How to collect and report annual statistics
- Youth-focused materials
- Orders and decisions on our website



Supporting Implementation

- The IPC wants to work with service providers to build understanding of the new Part X requirements:
  - Consultation: opening lines of communication with stakeholders
  - Collaboration: working together to support implementation and find solutions
  - Co-operation: rather than confrontation in resolving complaints

CONTACT US

Office of the 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