REACHING OUT TO ONTARIO

PART X OF THE *CHILD, YOUTH AND FAMILY SERVICES ACT*

Brian Beamish, Commissioner

Emily Harris-McLeod, Senior Policy Advisor

Waterloo

May 31, 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
  - Oversight (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 rules that service providers must follow to protect privacy
- 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*
  - a *CYFSA* licensee (e.g., group and foster care licensees)
  - all children's aid societies, including Indigenous societies
- Foster parents are not service providers under Part X

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
  - recorded before or after Part X comes into force
- 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 the access is 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, video footage, 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

Indirect Collection Without Consent: Examples

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 CASs, to assess/reduce risk of harm to a child

Not permitted:

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

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)
- ✗ Using information for personal financial gain

IPC Decision Under Health Privacy Law

- *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 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 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

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 - Unencrypted hospital laptop with health information of 2900 people stolen from a car
  - IPC found the hospital had not taken reasonable steps to protect the information
  - IPC ordered hospital to implement or revise certain policies, procedures and staff training

Privacy Controls: Examples

- Administrative controls:
  - privacy and security policies
  - privacy and security 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
- You must also notify the IPC and minister of significant breaches:
  - part of a pattern of similar breaches
  - involves theft of PI
  - involves PI being used or disclosed by someone who knew they were doing so without authority
  - will likely result in PI being further breached
  - results in an employee being terminated or disciplined, or resigning

Notice of Information Practices

- You must make publicly available an easy-to-understand description of:
  - your policies for collection, use, modification, disclosure, retention and disposal of PI, as well as the safeguards you have in place
  - how to access or request a correction of PI
  - how to contact your organization
  - your complaint processes, and how to file a complaint with the IPC
- When you collect information directly, you must notify people that their information may be used or disclosed in accordance with Part X

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 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 and
  - knowledgeable

Consent

- Consent is **knowledgeable** if 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
- 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 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)
  - children under 16, whether capable or not
- A custodial parent or children's aid society can be SDM for a child under 16 (subject to exceptions):
  - if there's a conflict, the capable child's decision prevails

Access to Information and Correction of Records

Individual's Right of Access

- Part X gives individuals 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 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

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 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)

Exceptions to Access Right

- 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 Under Health Privacy Law

- **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
- 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 (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 PI from the record

Making an Access Request

- Access requests must be made **in writing**:
  - no specific form is required
  - no requirement to specify the request is under Part X of the *CYFSA*
- 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
- **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)
  - refuse access, and/or
  - extend the deadline for a full response
- You may extend the deadline by up to 90 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")
- IPC has an expedited 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

Correction of 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
- Two 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
  - it consists of a professional opinion or observation made in good faith
- Individual can require you to attach a statement of disagreement to the record

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 Procedures

- Correction 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 is 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

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 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.)

Role of the IPC

- The IPC also has a broader mandate to:
  - offer comments on a service provider's information practices, at their request
  - provide information and public education about Part X and the IPC's role
  - receive representations from the public about the operation of Part X
  - engage in research about Part X

IPC Complaints Process

- Most complaints are resolved before reaching the adjudication stage

IPC Complaints Process - Intake

- All complaints are received by the IPC registrar
- The registrar or intake analyst may attempt to resolve the complaint informally
- They may **dismiss** the complaint, for example if:
  - it is clearly outside the IPC's jurisdiction
  - they are satisfied with your response to the complaint

IPC Complaints Process - Mediation

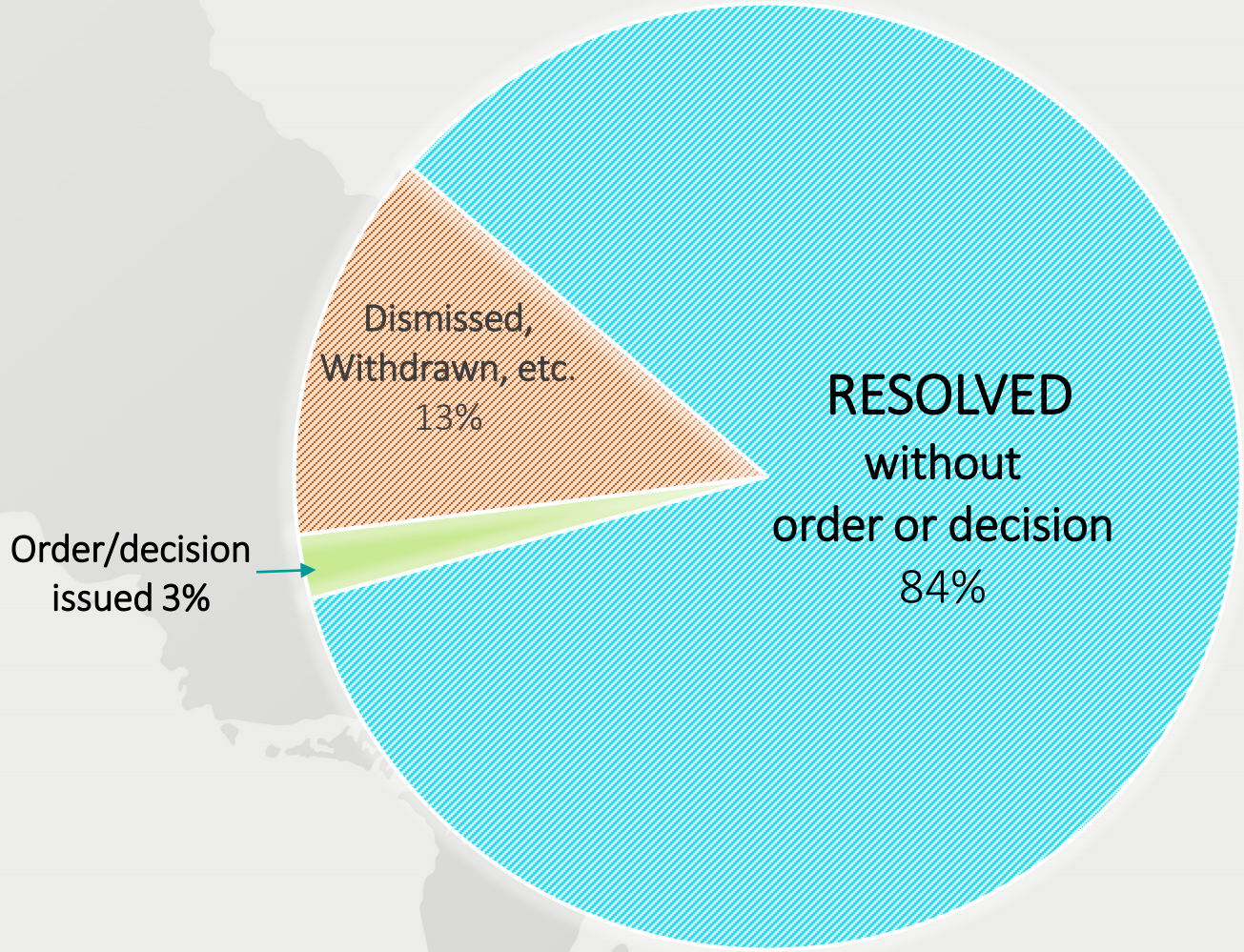
- Complaints that are not resolved at intake may be sent to mediation
- Mediation is usually conducted by telephone, with the IPC mediator speaking separately with each party
- IPC mediator acts as a neutral third party
  - goal is to find a resolution which satisfies the needs of all involved
  - saves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

IPC Complaints Process - 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:
  - for example, may order that a record of PI be provided to the individual, or that a privacy practice be implemented
  - IPC may decide not to issue an order
  - IPC orders can be appealed to the Divisional Court

Importance of Early Resolution - PHIPA

- 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

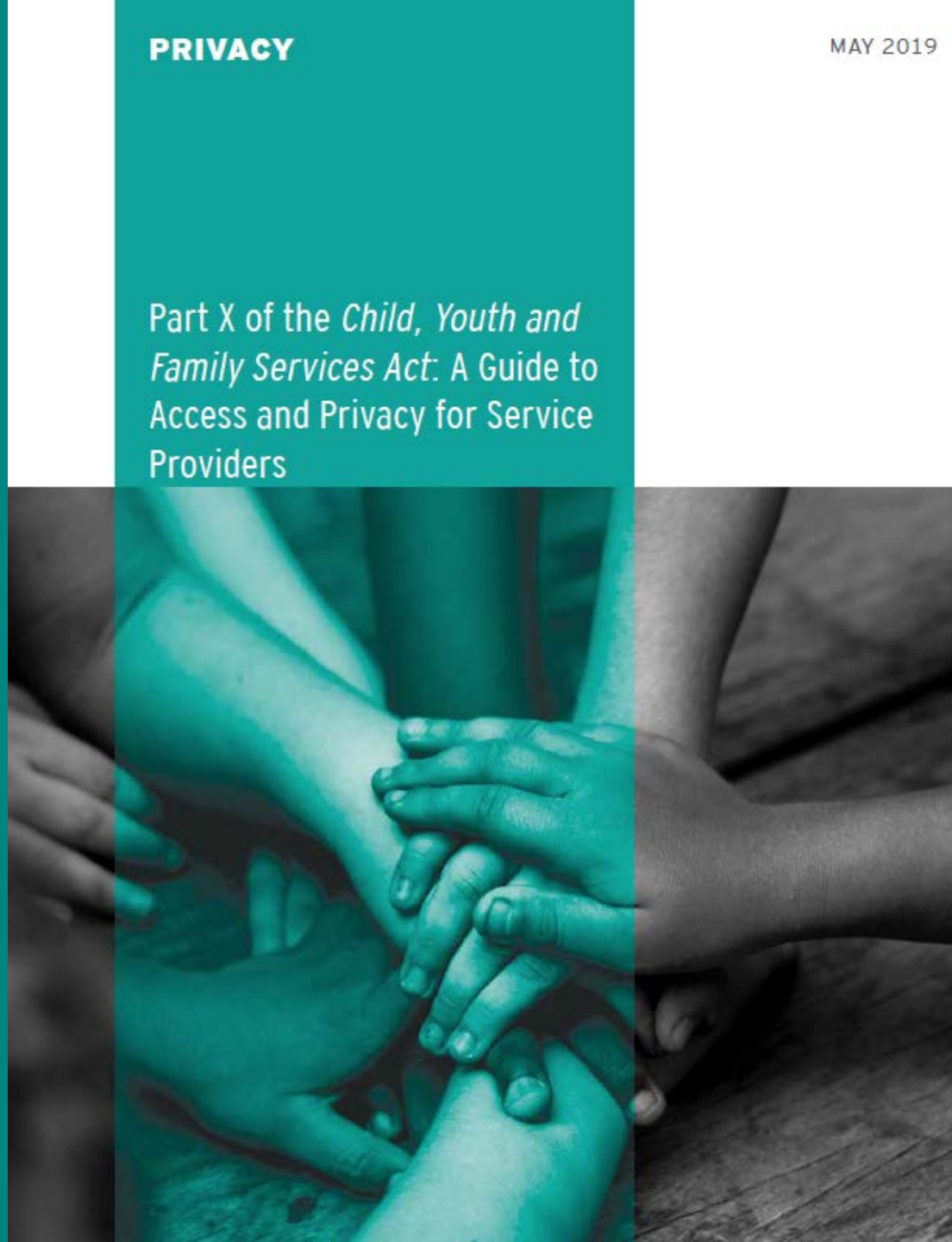


Supporting Implementation

- 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

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 on our website



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