

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

Brian Beamish
Information and Privacy Commissioner of Ontario

Emily Harris-McLeod
Senior Policy Advisor



Information and Privacy
Commissioner of Ontario

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

PART X
INFORMATION
SESSION
TORONTO

November 8, 2019

Background

- 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
- **Part X** of the *CYFSA* is new
- As of January 1, 2020, it will:
 - establish rights for individuals to access their information
 - set out privacy rules that service providers must follow

Strengths of Part X

- closes a legislative gap for access and privacy
- modeled on Ontario's health privacy law (*PHIPA*)
- facilitates transparency and consistency among service providers' information practices
- consent-based framework
- individuals' right of access to their information
- 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 privacy breaches
 - supporting implementation
 - publishing annual statistics about Part X
- The commissioner is appointed by and reports to the Legislative Assembly, and is independent of government

Part X of the *Child, Youth and Family Services Act*: A Guide to Access and Privacy for Service Providers





Who and What Does Part X Apply to?

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**
 - 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 Personal Information?

- **Personal information** means recorded information about an identifiable individual:
 - even without a name, it may be personal information if the individual can be identified
- **Record** means a record of information in any form:
 - includes electronic records, paper records, audio and video recordings, etc.



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

Fact Sheet

What is Personal Information?

October 2016

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* (the acts) protect the privacy of personal information while providing individuals with a right of access to their own information.

In this fact sheet, we provide guidance about how the Information and Privacy Commissioner (IPC) interprets the term "personal information."

HOW IS PERSONAL INFORMATION DEFINED IN THE ACTS?

The acts define personal information as "recorded information about an identifiable individual," and include a list of examples of personal information (see Appendix A for the full definition).

Recorded information

Information can be recorded in any format, such as paper records, electronic records, digital photographs, videos or maps.

About an identifiable individual

Information is about an identifiable individual if:

- it is about the individual in a personal capacity; that is, it reveals something of a personal nature about the individual, and
- it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information)

The listed examples include a person's name when combined with other information about them, such as their address, sex, age, education, or medical history. These examples are not exhaustive and many other kinds of information may still qualify as personal information.

What is a Service?

- Service means a program or service provided or funded **under the *CYFSA*** or a *CYFSA* licence
- It includes:
 - a service for a child who is or may be in need of protection or the child's family
 - counselling for a child or the child's family
 - a service related to residential care for a child

What is Custody or Control?

- If you possess a record, it's usually in your **custody**
 - you must have some right to deal with the record and some responsibility for its protection
- A record may be under your **control** even if you don't possess it (e.g., your consultant holds the record, but you have authority to manage it and you rely on it for business purposes)
- It is possible to have custody or control of:
 - records that were not created by your organization
 - records that are also in the custody or control of another organization



Privacy Rules

Collection, Use and Disclosure

- Consent is required for the collection, use and disclosure of personal information, subject to specific exceptions
- Even with consent, there are **limits**:
 - only as much as necessary for providing service
 - only where other (non-personal) information won't suffice
- When directly collecting someone's information, you must **inform** them about Part X

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
- ✓ Among children's aid societies 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're able to obtain it directly

Use of Information Without Consent: Examples

Permitted:

- ✓ Use for the purpose the information 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 for non work-related purpose)
- ✗ Using more information than necessary (e.g., reading whole file when you only need phone number)

IPC Decision: Snooping

- A hospital clerk viewed the health records of a famous patient and 443 others for no work related purpose
 - hospital detected the breach in a **proactive audit** and reported it to the IPC
 - clerk was fired and pled guilty to contravening *PHIPA*
- In *PHIPA* Decision 64, the IPC found:
 - unauthorized use of health information by clerk
 - hospital had sufficient safeguards

Information and Privacy Commissioner,
Ontario, Canada



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

PHIPA DECISION 64

HR15-115

A Public Hospital

December 18, 2017

Summary: A public hospital (the hospital) contacted the Office of the Information and Privacy Commissioner of Ontario (the IPC) to report a privacy breach under the *Personal Health Information Protection Act, 2004 (PHIPA)*. This breach involved a registration clerk (the employee) accessing records of personal health information relating to a media-attracting patient (the patient) as well as 443 other patients, without authorization. The IPC referred this matter to the Attorney General of Ontario to consider commencing a prosecution against the employee for offences under *PHIPA*. A prosecution was subsequently commenced and the employee pled guilty. As part of her plea, the employee agreed that she wilfully used personal health information in contravention of *PHIPA*. In light of the steps taken by the hospital to address this breach, including its acknowledgement of the benefits and importance of including enhanced auditing capabilities in any new system it implements, no review of this matter will be conducted under Part VI of *PHIPA*.

Statutes considered: *Personal Health Information Protection Act, 2004*, sections 2, 12(1), and 29.

Disclosure Without Consent: Examples

Permitted:

- ✓ Required/permitted by law
- ✓ Necessary to assess/reduce a risk of serious harm to any person
- ✓ Among children's aid societies to assess or reduce a risk of harm to a child
- ✓ To law enforcement to aid an investigation

Not permitted:

- ✗ To another service provider simply because you both serve the same client
- ✗ To friends or relatives of the client, if there's no reason for them to receive the information

Protection of Personal Information

- Service providers must take **reasonable steps** to ensure personal information is protected against theft, loss and unauthorized use or disclosure
- *PHIPA* Order 4: Theft of hospital laptop from doctor's car. It contained the unencrypted health information of 2,900 people.
 - IPC found the hospital had **not** taken reasonable steps to protect the information
 - IPC ordered the 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
- screening of visitors

- **Technical controls:**

- strong authentication and access controls
- encryption of mobile devices
- firewalls and anti-malware scanners
- detailed logging, auditing, monitoring

Mandatory Breach Notification

- You must **notify the individual** if their information is breached (stolen, lost, used or disclosed without authority)
- At the first reasonable opportunity, tell them:
 - what happened
 - steps taken to prevent and mitigate
 - how to contact an employee who can answer questions
 - their right to complain to the IPC

Breach Notification - IPC

- You must **notify the IPC** and ministry of significant privacy breaches, and those involving:
 - theft of personal information
 - a pattern of similar breaches
 - use/disclosure by someone who knew they lacked authority to do so
 - an employee being disciplined or resigning due to the breach
 - a breach that has or will lead to further breaches



Notice of Information Practices

- You must make **publicly available** an easy-to-understand description of:
 - your information practices (your policies for handling personal information and your privacy safeguards)
 - how to access records or request a correction
 - your complaints process
 - how to file a complaint with the IPC

Key Points for All Staff

- When directly collecting their information, you must inform people about Part X
 - know where to refer clients for more information (e.g., a notice of information practices on website/brochures)
- 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 personal information (subject to specific exceptions)
- 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
- An individual can be:
 - capable at one time, but not at another
 - capable of providing consent for some parts of their personal information, but not others

Capacity

- Service providers are responsible for determining capacity under Part X
- You may presume someone is capable — unless you have reason to believe otherwise
- People can challenge decisions of incapacity through the **Consent and Capacity Board**

Substitute Decision-Makers

- Substitute decision-makers 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 substitute decision-maker 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

- For a child under **age 16**, their custodial parent (or children's aid society or other person authorized to consent on the parent's behalf) can act as a substitute decision-maker
- Exception — does not apply to information 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 substitute decision-maker

Key Points for All 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 rules for substitute decision-makers, especially regarding children under 16



Access to Information

Individual's Right of Access

- Individuals have a right to access their personal information from a service provider within set timelines and at no charge
- The records of personal information 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** (and you think it's appropriate to keep their identify confidential)

IPC Decisions under Health Privacy Law

- *PHIPA* Decision 34: Individual 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 was **speculative or unlikely**
 - ordered the clinic to provide the individual with access to the record

Exceptions to Access Right

- Service providers may refuse access if the request is **frivolous or vexatious** or made in bad faith
- May include requests that are:
 - made for a purpose other than to obtain access – such as to purposefully burden the system
 - part of a pattern of conduct that amounts to an abuse of the right of access



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

Access Requests and Other People's Privacy

- There is no **overarching** access exception that requires you to redact other people's personal 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** (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
 - in either case, one or more access exceptions may apply

Access Requests and Other People's Privacy

- A client requests access to a record – is it **dedicated primarily** to providing services to him?
 - Would the record **exist** if it weren't for the provision of service to this client?
 - Is providing him a service **central** to the purpose for which the record exists?
 - Is the record several steps removed from the actual service experience?
 - Is it related to other matters, such as legal advice?
 - Does it contain information about many clients?
- Evaluate on a **record-by-record** basis. Cannot always be determined by whose name a record is filed under

Parents Seeking their Child's Information

- **Custodial** parents can make access requests on behalf of their child (under age 16). The capable child's wishes prevail.
- A **non-custodial** parent may seek information about their child
 - They do not have the same rights as custodial parents to make access requests
 - However, you may have discretion to disclose information in some cases
 - Regarding similar rules in *PHIPA*, the IPC found that organizations should consider whether:
 - disclosure is permitted or required by law (e.g., *Children's Law Reform Act*)
 - there is consent
 - there is a court order

Access Requests

- Must be made **in writing**
- Must contain **sufficient detail** to enable you to identify and locate the record
 - If not, you must offer to assist the requester in reformulating the request
 - 30 day timeline doesn't start until sufficient detail is received
- **No fees** can be charged

IT'S ABOUT YOU

Your File and Your Rights Under Ontario's Child and Family Services Law

You have the right to:

- ask to see and get a copy of your personal information in your file
- request a correction if your information isn't correct or complete
- know if your personal information is lost, shared, stolen or viewed when it shouldn't be

You have the right to file a complaint with the Information and Privacy Commissioner of Ontario.

1-800-387-0073

info@ipc.on.ca

www.ipc.on.ca

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

Who to talk to here if you would like to:

- ask about your privacy rights
- make an access or correction request
- make a complaint

Responding to an Access Request

- Must respond in writing within **30** calendar days to:
 - grant access (make record available or provide copy on request)
 - refuse access (with reasons), and/or
 - extend the deadline for a full response
- You may extend the deadline by up to **90** more days, 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

Complaints to IPC

- Individuals can complain to the IPC within **six months** if their access request is partially or fully refused
- Can also complain if they receive no response (“deemed refusal”):
 - One third of access-related complaints to the IPC under *PHIPA* were about deemed refusals in 2018 (58 complaints)
 - 97% 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 provide the correct information
- Two exceptions — you are **not** required to correct the record if:
 - it consists of a professional opinion or observation made in good faith
 - it was not originally created by your organization, and you lack sufficient knowledge, expertise or authority to correct it

Correction of Records

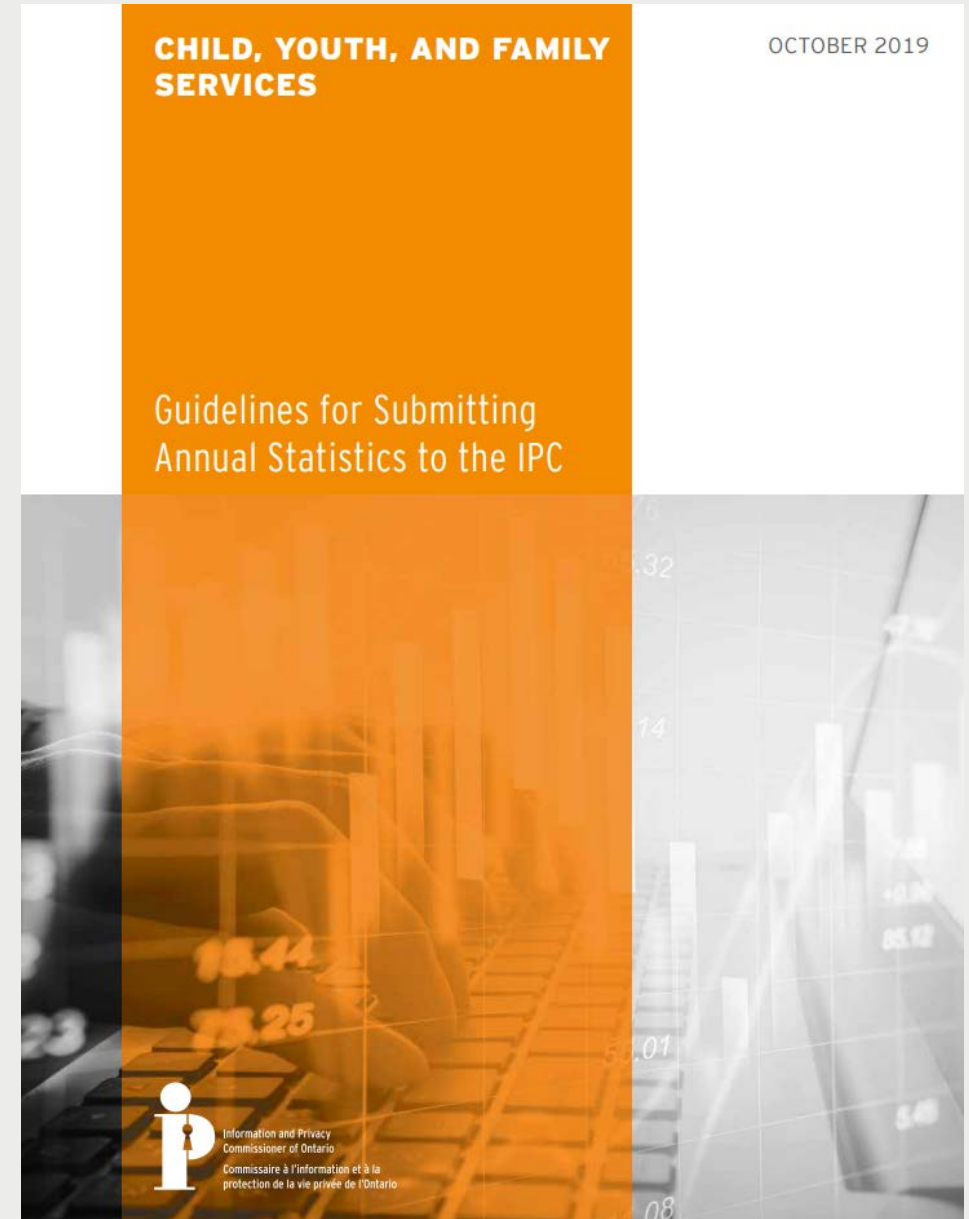
- Process and timeline rules are similar to access requests
- If you refuse the correction, the individual can require you to attach a **statement of disagreement** to the record
- Individuals can complain to the IPC if their correction request is refused (or if there's no response)

Key Points for All Staff

- Individuals have a **right** to access records of their 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

Annual statistics to IPC

- The IPC collects annual statistics from all service providers
- First report due March **2021**, including:
 - the number of access/correction requests received in 2020
 - response times
 - how often you refused access/correction, and on what grounds
 - number and types of privacy breaches (e.g., loss, theft, etc.)



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 you have appropriate privacy **safeguards** (including staff training)
- Draft a public notice of your information practices
- Plan how you will collect statistics
- Know where to go for support (associations, IPC)

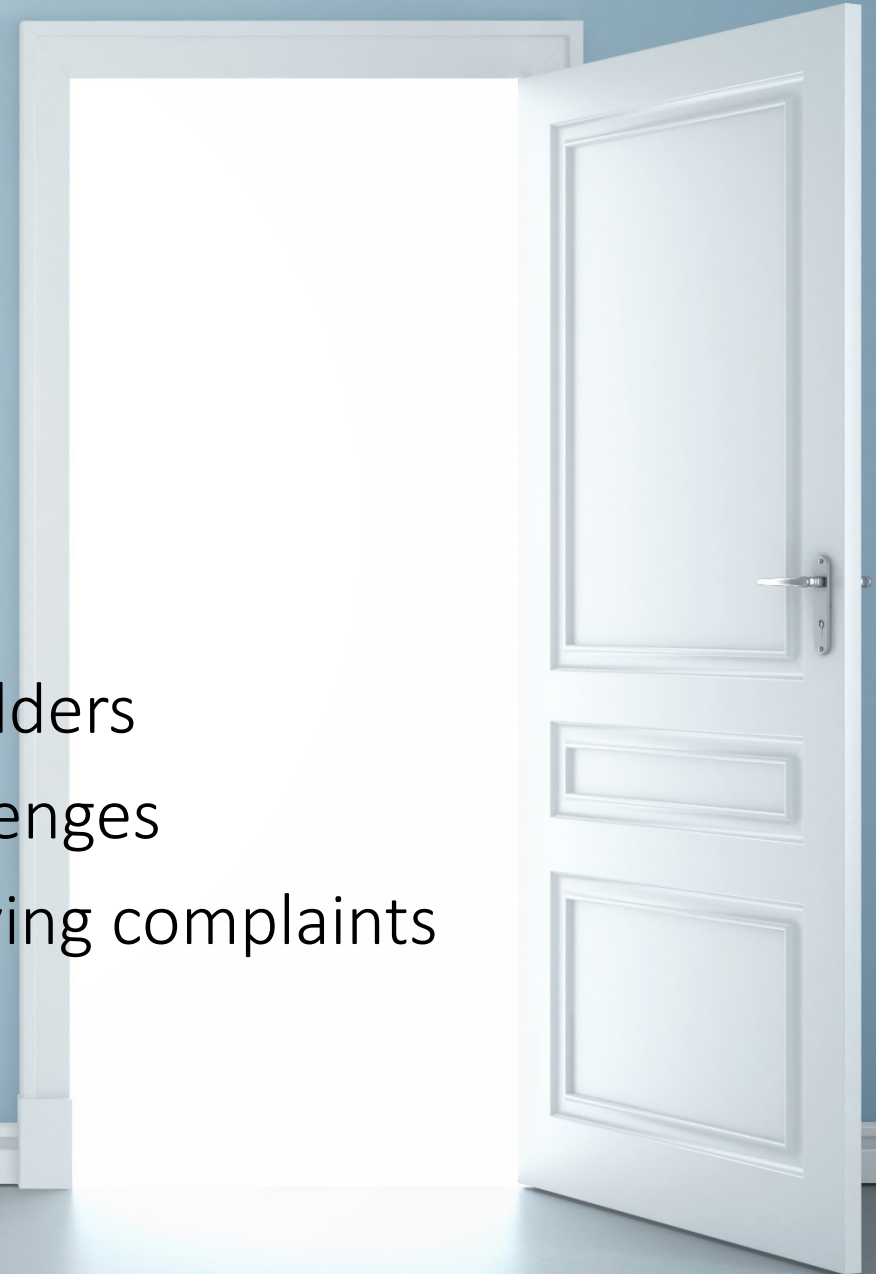
Our Open Door Policy

Service providers 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