Privacy standards and best practices for situation tables

Stephen McCammon
Legal Counsel

Office of the 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

Community Mobilization and Acutely Elevated Risk

Peterborough, Ontario

September 26, 2022

The Information and Privacy Commissioner (IPC):

- *is appointed by and reports to the Legislative Assembly*
- *provides independent review of access and privacy decisions and practices*
- *has quasi-judicial duties and powers*

The IPC's functions include:

- *resolving* access to information appeals
- *investigating* privacy complaints – public sector and health
- *conducting reviews of information handling practices of prescribed entities*
- *researching* access and privacy issues
- *commenting* on proposed government legislation and programs
- *informing* the public and government about access and privacy issues

Disclaimer

- This presentation should not be relied on as a substitute for the applicable legislation itself, or legal advice. It is not an official legal interpretation of the relevant law and does not bind the office of the Information and Privacy Commissioner of Ontario.

Situation table related legislation overseen by the IPC

- *Personal Health Information Protection Act* (*PHIPA*)
  - covers *individuals* and organizations involved in the delivery of health care services (health information custodians or HICs)
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - covers over 1,200 municipal organizations
- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - covers 300 provincial institutions

- Part X of the *Child, Youth and Family Services Act* (*CYFSA*)
  - modeled on PHIPA
  - comprehensive privacy protections that apply to child, youth and family service providers
  - Individuals' right to access, correct, and complain
  - promotes transparency and accountability

Additional provincial legislation of interest ...

- The IPC also oversees privacy rules under:
  - *the Anti-Racism Act, 2017, and*
  - *the Coroners Act*

- The *Police Services Act, 2018:*
  - *mandates community safety and well being planning*
  - *municipalities must monitor, evaluate and publicly report on their plan's effectiveness*

- And see the *Community Safety and Policing Act, 2019* provisions that, *once in force, will* facilitate the establishment of First Nations police service boards with the consequent application of MFIPPA

A word about federal privacy legislation

- *The Privacy Act applies to personal information handled by some First Nations run institutions such as Land and Water Boards*
- *The Personal Information Protection and Electronic Documents Act or PIPEDA applies to*
  - *A Band Council's collection, use or disclosure of the personal information of its employees and job applicants, and*
  - *the collection, use or disclosure of personal information by an organization in the course of commercial activities*
- *For more information about the Privacy Act and PIPEDA, see the Privacy Commissioner of Canada*

A word about the OCAP principles

- *OCAP: the standard for how to conduct research with First Nations*
- *OCAP stands for ownership, control, access and possession*
- *Under OCAP®, First Nations have control over data collection processes in their communities, and that they own and control how this information can be used:*
  - *"OCAP® is a way for First Nations to express principles of information governance and community privacy in an aggregate sense."*
  - *"Personal privacy, on the other hand, is a universal value that is reflected in western society, through laws, policies and ethics. … Canadian laws protect personal privacy."*
  - *"Respecting OCAP® principles and concepts of community privacy add an additional layer of privacy protection for individuals; not only is an individual's personal identity protected from disclosure and any resulting harm, but their group identity and status as a member of a community is also protected."*

    OCAP: The Path to First nations Information Governance; May 2014, First Nations Information Governance Centre
- *For more information about the OCAP® principles, see the FNIGC*

A word about the *Youth Criminal Justice Act* …

- Information sharing at situation tables must comply with Ontario's public sector privacy laws and other laws regulating privacy, including those affecting youth, such as the *Youth Criminal Justice Act* (YCJA).
- The IPC is not aware of any provision of the YCJA that would permit the disclosure of information identifying a person dealt with under the YCJA by an entity, police force, department, agency, person, or organization referred to in sections 114 to 116 of that Act to the range of parties typically participating in a situation table.
- In addition, the YCJA generally prohibits the publication of any information that would identify a young person as having been dealt with under that Act.

Back to Ontario: privacy legislation – the broad strokes

- Institutions, service providers and HICs must :
  - follow rules governing how they collect, use, retain, disclose and dispose of personal information (PI) and personal health information (PHI)
  - collect, use or disclose PI and PHI only for legitimate, limited and specific purposes
  - inform individuals how they intend to use their information and how they can learn more
- Individuals have the right to:
  - request access to their own PI or PHI
  - file privacy complaints
  - request access to any information held by institutions
  - appeal access requests and privacy complaint decisions to the IPC

The IPC's situation table work:

- **Participated** in the Ontario Law Reform Commission community safety workshop (2013), Waterloo Region Crime Prevention Council dialogue (2014) and *Economics of Policing Workshop* (Ottawa, 2015)
- **Visited and provided comments** to the Cambridge, North Bay and Rexdale FOCUS situation tables (2015)
- **Reviewed and commented** on the OPP's *Situation Table Guidance Manual* and the Ministry of the Solicitor General's (Ministry) *Guidance on Information Sharing in Multi-Sectoral Risk Intervention* ***Model*** (2015-2016)
- **Hosted** a webinar on situation tables (2016)
- **Met with and provided comments** to the SPIDER table (Toronto, 2017)
- **Participated** in the Durham Connect Summit (2018)
- **Met with and provided guidance** to the Ministry re: the Risk Tracking Database (2019)
- **Continue to engage** with communities around the province regarding situation table-related privacy issues and solutions

Looking at situation tables through the required privacy lens

Facing the privacy concerns

- **Situation tables rely** on information-sharing to enable local agencies to develop intervention strategies in individual cases involving "acutely elevated risks of harm"
- **Wide range of agencies involved** (e.g. police, health, schools, etc.)
- **Agencies face** different privacy requirements in Ontario

- **Success requires** understanding of and respect for privacy rights of clients and privacy requirements of all participating partners
- Key privacy issues under *FIPPA*, *MFIPPA, CYFSA* and ***PHIPA*** include:
  - Agency by agency compliance with rules re: authority to collect, retain, use and disclose PI/PHI
  - Not sharing PI/PHI **pre-maturely** (i.e. when a de-identified discussion will serve the purpose)
  - Ensuring sufficient governance, training and oversight

Sustainable situation table success is built on:

- **Strong governance** to ensure all participants understand and are in a position to fulfill their privacy-related responsibilities
- **Information sharing agreements or MOUs** to confirm privacy requirements, especially for participants not covered by privacy legislation
- **Training, policies, procedures and practices** in place to help ensure continued adherence to privacy requirements and best practices
- **Data-minimization:** a “need-to-know” approach is essential
- **Transparency:** Participating agencies should be open with the public about their involvement in a situation tablec

A roadmap for success

The IPC's supports the Ministry's *Guidance on Information Sharing in Multi-Sectoral Risk Intervention Model*:

- It provides a **roadmap** for compliance with privacy requirements
  - Designed to allow multi sector agencies to collaborate to reduce significant risks of serious harm
  - Built on a need-to-know approach to information sharing

- The IPC recommends the use of the roadmap: if another route is chosen, participating agencies must still ensure information sharing practices comply with privacy requirements

- **Taking another route**: proceed with caution, consider a **PIA** or privacy impact assessment
- Caution flag: disclosure of name, address, DOB to the entire table – e.g. at Filter 3 – links an individual to the de-identified information discussed earlier = privacy breach risk

The relationship between acutely elevated risk of harm and privacy legislation

- The phrase “acutely elevated risk of harm” is not found in provincial privacy legislation

- Privacy legislation does contain provisions that permit the disclosure of personal information for the purpose of eliminating or reducing serious harm

Key risk reduction related provisions under privacy legislation in force today

- Disclosure provisions:
  - *PHIPA – ss. 30, 40(1)*
  - *MFIPPA* and *FIPPA* – ss. 32(h) and 42(1)(h) respectively
  - Part X of the *CYFSA* – ss. 286, 287 and 292(1)(g)

- Collection provisions:
  - *PHIPA – ss. 30, 36*
  - *MFIPPA and FIPPA – ss. 28(2), 29(1); and 38(2), 39(1) respectively*
  - Part X of the *CYFSA* – ss. 286-290

Working from the *same page*

- To help ensure effective and consistent collaboration, **consider** employing a single set of situation table privacy practices drawing on the highest relevant privacy standards
- In terms of disclosures, the key risk reduction related standard would be grounded in sections 30 and 40(1) of *PHIPA*:

30(1) and (2): A HIC shall not collect, use or disclose:

- PHI if other information will serve the purpose of the collection, use or disclosure
- More PHI than is reasonably necessary to meet the purpose of the collection, use or disclosure

40(1): "A health information custodian **may** disclose personal health information about an individual **if** the custodian **believes on reasonable grounds** that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons."

Assessing risk of harm using the significant risk of serious bodily harm threshold

- The section 40(1) standard is an objective standard based on **reasonable grounds** in terms of the assessment of both the **harm element** and the **necessity of the disclosure element**
- Requisite **harm** includes serious psychological harm
- Mere inconvenience to the individual or a service provider would not satisfy the **serious harm** test
- Questions and subjective concerns do not provide reasonable grounds for believing that disclosure of personal health information is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm." [Queensway Carleton Hospital (Re), 2016 CanLII 930 (ON IPC)]
- In assessing whether the **significant risk of serious harm** threshold has been met, consideration should be given to both the degree of risk that a particular harm will be realized and the degree of the harm should it be realized
- As the severity of the realizable harm grows, the requisite probability of its realization may fall well below certainty. However, "no risk" of a very serious harm would never be sufficient, any more than a "high risk" or certainty of a mere inconvenience
- Consider whether there is an objectively realistic possibility of a harm occurring that will interfere in a substantial way with the integrity, health or well-being of a person

The *necessity of the disclosure* element and the impact of the section 30 based data-minimization

- Data-minimization – also referred to as a "need-to-know" approach – is critical
- Assuming the disclosing agency has determined that the section 40(1) significant risk of serious harms standard has been met, before any disclosure is made consideration must be given to:

  - **The character of the disclosure:** Do not disclose PI/PHI if other information will serve the harm reduction purpose

  - **The content of the disclosure:** Do not disclose more PI/PHI than is reasonably necessary to meet the harm reduction purpose

  - **The scope of the disclosure:** Do not disclose PI/PHI to more agencies than is necessary to meet the harm reduction purpose

Seek Consent

- Whenever possible, seek the individual's express consent to collect, use and disclose their information
- Consent must be **from the individual** to whom the information relates, knowledgeable, related to the particular information, and never obtained through deception or coercion
- Continue to respect the **data-minimization** standard
- **Inform the individual** what information will be shared, which agencies will receive it, and for what purpose
- **Respect** the individual's choices (e.g. re: the purpose, content and scope of the disclosure, the withdrawal of consent)
- **Document** the consent
- Note, when collecting PI, institutions cannot rely solely on consent

Reviewing the Four Filter process …

	Agencies involved	Information used	Function performed	Guidance
#1	The originating agency (OA)	Relevant, accessible PI /PHI from the OA's files	**Preliminary assessment by the OA**: is there a significant risk of serious bodily harm that requires a multi-agency response? Has consent been sought and obtained? Identify and respect its limitations	Requisite harm includes: serious psychological harm; harms that constitutes substantial interference with the health or well-being of a person; does not include mere inconvenience to the individual or a service provider
#2	The full table	De-identified information only	OA presents the case, **group assessment** of risk and the need for a multi-agency intervention	Discuss relevant risk factors, avoid discussing factors in needlessly precise terms (e.g. use age range rather than DOB)
#3	The full table	De-identified information only	**Group identification** of the agencies reasonably believed to be necessary to the planning and implementation of the intervention	Focus on the identified risks and how the services provided by specific agencies might be employed to reduce or eliminate those risks
#4	Those agencies reasonably believed to be necessary to plan and implement the intervention, + "consent" agencies	Name/identity of the individual reasonably believed to be at risk, other PI/PHI reasonably believed to be necessary to plan and implement the intervention	**Sub-group planning** of the intervention and **refinement** of the make-up of the intervention group (+ / -). Note: sub-group meets apart from the full group	Focus on the risks that require mitigation, the role intervening agencies are expected to play, and the PI/PHI reasonably believed to be necessary to assess the situation and plan the intervention

De-identified information

- Information is **de-identified** if it does not identify an individual, and it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual

- The removal of direct identifiers may not be sufficient to prevent re-identification

- "**Quasi-identifiers**" can be used for re-identification (e.g. gender, marital status, location, date of previous incident, diagnosis, profession, ethnic origin, race, or profession)

- Quasi-identifiers can be used either by themselves or in combination with other available information to uniquely identify individuals

Tips for keeping it de-identified

- Determine what classes of de-identified information are **required** to effectively assess risk and focus the discussion on those factors
- **Avoid** the discussion of any quasi-identifiers that are not relevant
- **Zero in** on the factors you will need to discuss in order to mitigate harm
- Even when it comes to relevant factors, avoid discussing an individual's circumstances in **unnecessarily** precise terms (e.g. if only general age, location and mental health status are relevant, refer to age in broad ranges like "minor", "adult" or "senior"; a neighborhood or street rather than a person's address; the fact a person has a mental illness rather than their specific diagnosis)

Filter 4: look ups and add ons

- During the Filter 4 meeting, if individual agency representatives of this sub-group decide to perform a ‘look up’ on their respective systems, any further information sharing must also comply with **data minimization requirements**

- Further agencies may be added to the Filter 4 part of the meeting if it becomes clear that their specific involvement is **necessary**

The intervention and report back

- During the intervention, consent should be sought at the first reasonable opportunity for **any further information sharing at the situation table**
- If the individual declines the offer of service, further sharing of PI **at the situation table** should **cease**
- During the **report back stage**, unless the individual has expressly consented to being identified to the entire group, the report back to the table should be strictly limited to **de-identified information** that reflects, for example, that the individual in case # 1XA was connected with services, declined further service, or that the intervening agencies need to discuss further action

Participating in a situation table meeting by teleconference

Policies, procedures or protocols should require that:

- Agencies provide a list of remote participants to the situation table chair prior to the meeting
- Remote participants log into the meeting with a business e-mail address or phone number
- At the outset of the meeting, all participants re-affirm their recognition of the sensitive nature of the items being discussed and that only authorized Filter One (the initiating agency) and Filter Four participants are permitted to collect, record or transcribe personal information in relation to the meeting
- Accessing or downloading of any confidential material only be done on authorized computer equipment on a secure internet connection

Record keeping

- Newly assigned **unique pseudo-anonymous numbers** should be used to keep track of individual cases at the Situation Table, rather than identifying or quasi-identifying information such as an individual's initials, address or telephone number
- **Careful management** of this tracking responsibility is vital
- The agency that brings an individual case forward, as well as the planning and intervening agencies, should **record** some information about the case, including some PI
- Any other notes that contain any PI as captured by any of the other agencies, should be **securely destroyed**

Notice of disclosure

- Individuals should **receive written notice shortly after** their PI is disclosed
- Written notice may be provided by, for example, the lead agency during the first in-person intervention using **a card, letter or pamphlet**
- An agency should document the date, time and manner that the notice was provided
- **NOTE**: if, for example, during the Filter 4 discussion, it becomes evident that the risks are already being mitigated (e.g. the individual is already connected to sufficient services), the individual should still receive notice of any disclosure of their PI from the disclosing agency.
- **NOTE**: notice of disclosure and any associated documents **should not** characterize this disclosure as involving a "limited“ or “minimal” amount of PI

Can notice be delayed?

- In circumstances where providing notice at the “door knock” could reasonably be expected to cause a significant risk of serious harm to the mental or physical health of an individual, the notice may be delayed
- In such cases, provide the written notice at the first reasonable opportunity after the risk of serious harm associated with the provision of notice is reasonably believed to have abated

Notice: the details

- Notice to the individual should:
  - Indicate that the individual's PI was disclosed
  - Indicate the purpose of the disclosure (e.g. PI was disclosed for the purpose of reducing a significant risk of serious harm)
  - Indicate that the disclosure included PI such as the individual's name, address and risk-related circumstances
  - Identify the name of the agency that disclosed the individual's PI (e.g. the originating agency, which may be different from the “lead agency”) and the names of each of the agencies to which the disclosure was made
  - Include contact information for each of these agencies or contact information that would allow an individual to readily access contact details, as well as any other information about the situation table

Access & correction requests, privacy complaints and proactive disclosure

- Direct requestors/complainants to **the applicable institution, service provider or HIC**; **provide contact information** as needed
- **Institutions, service providers and HICs** must comply with the applicable access and privacy legislation
- The IPC encourages institutions and other situation table participants to **be transparent** about their situation table policies, procedures and activates
- The **benefits associated with open government** and transparency may lead a situation table or one of its institutional members to decide to **proactively disclose** a situation table MOU (e.g. without waiting for or relying on an access to information request)

Situation table story telling

- Use de-identified language or made-up names and ages to refer to clients' stories
- Do not mention the names of involved agencies
- Do not mention the area of the city involved
- Do not tell stories that are unique or appear to be unique
- Create a storytelling de-identification protocol that describes the steps you and your colleagues will take to protect the privacy of individual situation table clients
- Periodically evaluate your protocol and storytelling practices to assess whether your approach to storytelling needs to be updated
- Review the IPC's June 2016 paper, De-identification Guidelines for Structured Data to assess whether any additional steps may be required to minimize the risk of a breach associated with your public data release practices

Concluding words

- Properly understood, access and privacy legislation helps discipline rather than prevent the effective delivery of vital public services
- With sufficient planning and governance, situation tables can function in compliance with Ontario privacy legislation, including *PHIPA*
- Use of the privacy protective roadmap will help foster a strong sense of responsibility amongst all participants to maintain confidentiality, comply with privacy legislation and work together
- Respecting clients' privacy is essential to ensuring public trust and providing effective service delivery
- The IPC encourages government bodies to conduct periodic evidence-based evaluations of programs with significant privacy impacts

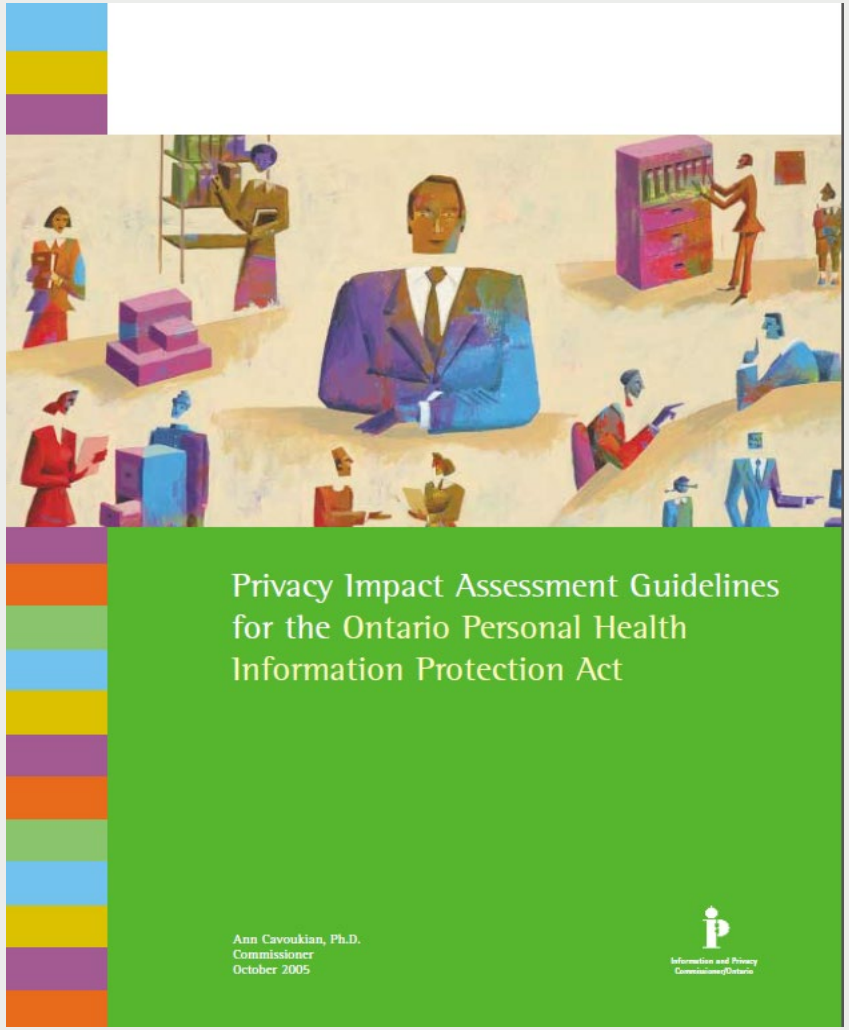
Additional IPC resources

IPC Webinar:
Privacy Protective Roadmap for Situation Tables

- Situation tables may help to ensure safer, stronger communities, but come with privacy risks
- IPC guidance helps community partners implement situation tables, while respecting the personal privacy of individuals

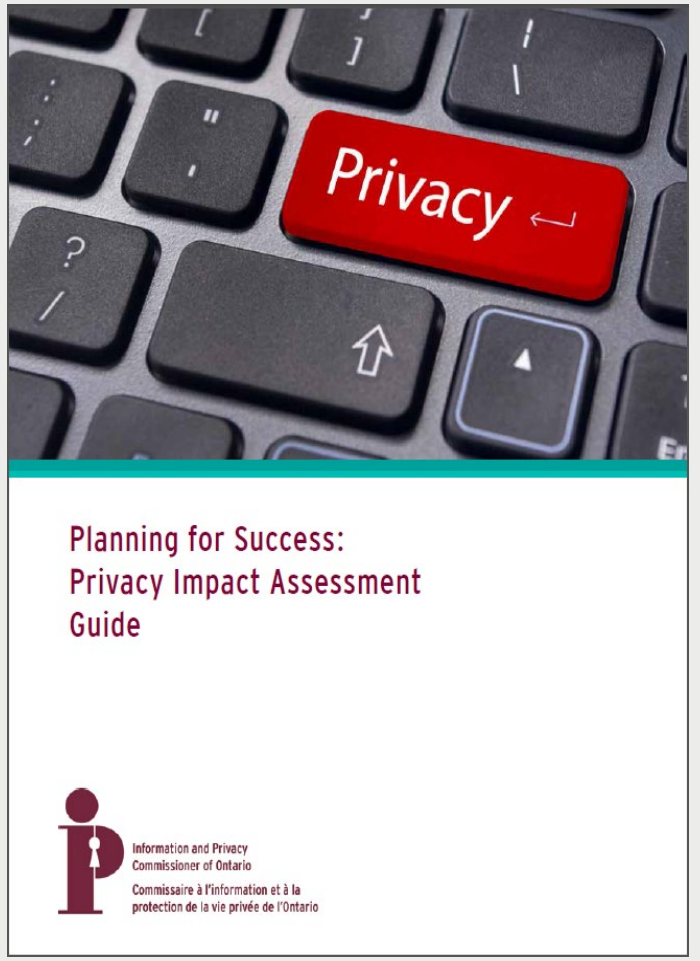
PIA Guidelines (*PHIPA*)

- Participating health information custodians should conduct a PIA to facilitate compliance with *PHIPA*
- These Privacy Impact Assessment Guidelines also include a self assessment tool



Privacy Impact Assessment Guide

- PIAs are tools to identify privacy impacts and **risk mitigation** strategies
- Widely recognized as a privacy best practice
- IPC developed a simplified **4 step methodology** and tools for M/FIPPA institutions
- Participating institutions should conduct a PIA on their own or in **collaboration** with other participants



Breach Notification under PHIPA

- Regulations prescribing when HICs must notify the IPC of a theft, loss or unauthorized use or disclosure came into force October 1, 2017
- The IPC recently published a guidance document explaining when we expect that a PHI-related privacy breach will be reported to the IPC.
- The IPC has also published guidance on the related duty to provide an annual statistical report to the IPC

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

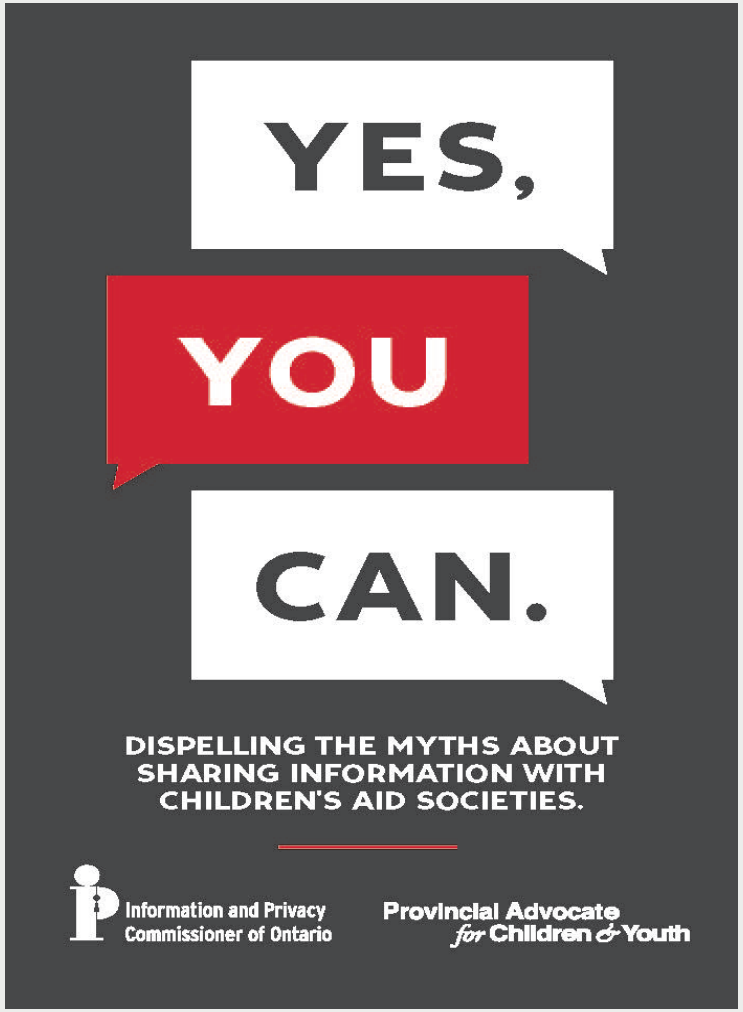
1. Use or disclosure without authority

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

Yes, You Can

- IPC collaborated with the Provincial Advocate for Children and Youth to develop this guide about privacy and Children's Aid Societies
- This guide dispels myths and explains that privacy legislation is not a barrier to sharing information about a child who may be at risk



- For recent guidance on compelling circumstances disclosures under FIPPA and MFIPPA:
  - See pages 4-5 of the IPC's November 2019 Fact Sheet, Disclosure of Personal Information to Law Enforcement

IPC fact sheets on working remotely while addressing privacy

- Working from home during the COVID-19 pandemic

- Privacy and security considerations for virtual health care visits

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