Privacy Standards and Best Practices for Situation Tables: A Roadmap for Success

Stephen McCammon, Legal Counsel

Office of the Information and Privacy Commissioner of Ontario

Northumberland Situation Table
Cobourg, Ontario
November 1, 2018

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

Presentation overview

- Background regarding the Information and Privacy Commissioner's (IPC) mandate, role, and recent activity
- The **Privacy Protective Roadmap** - issues and solutions in the context of a collaborative service delivery development: the Situation Table

Key message: respecting privacy is essential to ensuring trust

- Increased focus on collaboration and information sharing to improve service delivery and reduce significant risks of serious harms
- A **roadmap** for innovation and success accounts for privacy requirements and best practices (e.g. data minimization)
- Respecting personal privacy of clients is essential to ensuring trust and providing effective service delivery

IPC mandate and role

- Office established by statute in 1988
- IPC appointed by and **reports to the Legislative Assembly of Ontario**
- Provides **independent and impartial** review of access and privacy decisions and practices
- Provides **guidance**; conducts inquiries, investigations and reviews; issues orders and makes recommendations

Key privacy legislation

The IPC ensures compliance with three privacy statutes

- *FIPPA and MFIPPA* which provide:
  - Right of access to information in the custody or control of institutions and appeal of access decisions to the IPC
  - Privacy rules for **government institutions'** collection, retention, use and disclosure of personal information (PI)
- *PHIPA* which provides:
  - Comprehensive privacy protections for personal health information (PHI) in the custody or control of "**health information custodians**" (HICs) (including rights of access, correction, and complaint)

IPC also interprets and applies other intersecting legislation

IPC's Situation Table work

- Participated in Ontario Law Reform Commission workshop on integrated approaches to community safety (2013), Waterloo Region Crime Prevention Council dialogue (2014) and *Economics of Policing Workshop* (Ottawa, 2015)
- Observed and commented on three Situation Tables: Cambridge, North Bay, & Rexdale FOCUS (2015)
- Worked with the Ministry of Community Safety and Correctional Services (Ministry) and the OPP on guidance papers (2015-2016)
- Hosted a Webinar on Situation Tables (2016)
- Met with and provided comments to SPIDER (Toronto, 2017)
- Participated in Durham Connect Summit on Information and Data Sharing (October 2018)
- Continuing to present on and respond to queries about Situation Table-related privacy issues and solutions

Privacy guidance

The IPC provided detailed comments on:

- The Ministry's August 2016 Guidance on *Information Sharing in Multi-Sectoral Risk Intervention Model*
  - Provides a **roadmap** for information sharing at Situation Tables using a privacy protective version of the four-filter approach that has the support of the IPC
- Chapters VI & VII of a *Situation Table Guidance Manual*
  - An April 2016 manual produced by Dr. Hugh Russell with a grant from the Ministry and guidance from the OPP's Community Safety Services

A roadmap for success

The IPC's key contribution to this Guidance:

- A **roadmap** for compliance with Ontario privacy requirements
  - The roadmap is designed to allow agencies to collaborate to reduce significant risks of serious bodily harm
  - Wide range of agencies (e.g. police, health, schools, etc.) and privacy requirements involved
  - The IPC recommends the use of the roadmap as outlined in the August 2016 Guidance
  - If another route is chosen, you must still ensure that services are delivered in a privacy compliant manner

Taking another route: proceed with CAUTION

- Consider conducting a privacy impact assessment (PIA)
- Each agency must have and is advised to map out the legal authorities for its own **information handling activities** (e.g. collection, retention, use, disclosure)
- A disciplined discussion at the table is necessary, but may not be sufficient for the purpose of compliance with privacy legislation
- Disclosure of name, address, DOB – e.g. to the entire table at Filter 3 – links an individual to the information disclosed at Filter 2
- **RISK:** The wider the disclosure, the greater the risk of a **privacy breach**

The roadmap for success starts with planning and governance ...

- **Strong governance** is necessary to ensure that all participants understand their responsibilities and are able to participate in the Situation Table in a privacy protective manner
- Each participating agency is responsible for complying with privacy legislation and being **accountable for the actions and decisions of its representatives**
- To be accountable, institutions and HICs need to be **transparent about their participation** in a Situation Table, including by providing contact information of an individual who can provide further information or receive a complaint

… Includes an information sharing agreement …

- To ensure appropriate **handling** of PI/PHI (hereafter "PI"), participating agencies should sign an **information sharing agreement,** especially when agencies not covered by privacy legislation are involved

- **Among other things, an information sharing agreement**:
  - confirms who may be involved in **sharing** specific PI, under what circumstances and for what purpose(s)
  - outlines measures that must be implemented for the protection of PI

… Provides for oversight …

- Situation Tables require **policies, procedures, agreements and practices** to ensure continued adherence to privacy legislation
- These mechanisms will help agencies ensure that all information is collected, retained, used and disclosed in a compliant and appropriate manner. They should address:
  - measures to ensure that information is **accurate and up-to-date**
  - intake of access and correction **requests** and **privacy complaints**
  - **record handling requirements**, including those relating to the secure retention, transfer, and disposal of PI
  - the periodic **audit or review** of information handling practices
  - regular review of **which agencies should participate** and how
  - **training** requirements
  - **transparency** requirements

… Is guided by *need-to-know* rules

- **Data-minimization is essential to compliance** (refrain from handling PI when other information will serve the purpose, do not collect, retain, use or disclose more PI than is necessary and do not disclose PI to more agencies than is necessary)
- At every stage, limit the handling of PI to those who have the legal authority to collect, use and disclose that information, and who have a **legitimate need** to know the information
- Consensus at the Situation Table can be valuable but should not be mistaken for compliance with privacy legislation
- Situation Table chairs should facilitate a privacy compliant discussion while helping to identify risk factors & Filter 4 agencies

Best practice - seek consent

- Whenever possible, PI should be collected, used and disclosed with the **individual's express consent** *[but remember, institutions must also comply with* s. 38(2) of *FIPPA / s. 28(2) of MFIPPA]*
- **Consent must be**: from the individual to whom the information relates, knowledgeable, related to the particular information, and never obtained through deception or coercion
- In seeking consent, **inform the individual** what specific information will be shared, which agencies will receive the information, and for what purpose
- An individual may agree to disclose their information to some agencies, but not to others. To the extent that disclosure relies on consent, those choices for must be **respected**.
- A disclosing agency should **document the consent** (e.g. the date of the consent, the information to be disclosed, the organizations to whom the information will be disclosed, for what specific purpose(s), and subject to what restrictions or exceptions)

The Four Filter Process for Disclosure

(Where consent is unavailable or insufficient)

Filter 1: initial agency screening

- **Before** a situation is brought to the table, the originating agency uses PI to determine if the case meets the threshold
- **Key question**: is there a significant risk of serious bodily harm that the originating agency can't handle on its own?
- Significant risk of serious bodily harm includes a significant risk of both **serious physical** as well as **serious psychological harm**
- Relevant factor - whether that harm constitutes **substantial interference** with the health or well-being of a person and not mere inconvenience to the individual or a service provider
- If, after evaluating the risks, the originating agency concludes that the risk can **only** be addressed effectively by a multi-agency intervention, the agency may proceed to the next filter

Filter 2: assessing the risks; a de-identified discussion

- The originating agency presents the situation to the table in a **de-identified format**
- The group works together to further assess the risks and the need for a multi-agency intervention
- While an agency must use PI in selecting a case at Filter 1, it is **essential** that **only de-identified information be shared at Filter 2**

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 3: identifying the interveners

- If the Filter 2 thresholds are met, the next step is to identify the agencies reasonably believed to be **necessary** to the planning and implementation of the intervention
- Further review of the risk factors in a **de-identified Q & A driven discussion** will help reveal which agencies need to be involved
- For example, if it appears that the risk factors are tied to housing and education issues, consider whether agencies that provide housing, shelter or educational services should be involved at Filter 4

Filter 4: the full discussion: a separate meeting

- At this point, identifying information – e.g. the name and address of the individual – may be shared, but **only with the sub-group of intervening agencies**
- Only these agencies may remain for the Filter 4 part of the meeting where they will 1st learn **the identity of the individual**
- Limit the Filter 4 part of the meeting to:
  - those agencies reasonably believed to be **necessary** to the planning and implementation of the intervention
- Limit the Filter 4 discussion to:
  - the information reasonably believed to be **necessary** to plan and implement the intervention

The Filter 4 discussion

The assessment and decision to disclose PI should involve the thoughtful exercise of discretion. The agency making the disclosure should be able to articulate its rationale for the nature and scope of the disclosure in terms of factors including:

- What are the specific risks that require mitigation?
- What role is each agency expected to play in the intervention?
- What kind of PI is required to mitigate the identified risks?
- To what extent will the provision of general information (e.g. non-identifying information and/or less-specific personal information) permit the agencies to mitigate the risks?

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

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

New legislation on the horizon...

The *Child, Youth and Family Services Act*

- As of January 2020, Part X will provide for comprehensive privacy protections with respect to the handling of PI by children's aid societies and other child, youth and family service providers
- Individuals will have rights of access, correction, and complaint, with oversight by the IPC
- These protections and rights are modelled on provisions in *PHIPA*

The *Safer Ontario Act;* includes the *Police Services Act, 2018*

- As of January 2020, the PSA, 2018 will: (i) mandate community safety and well being planning; and (ii) facilitate the establishment of First Nations police service boards (with the consequent application of *MFIPPA)*

Concluding observations

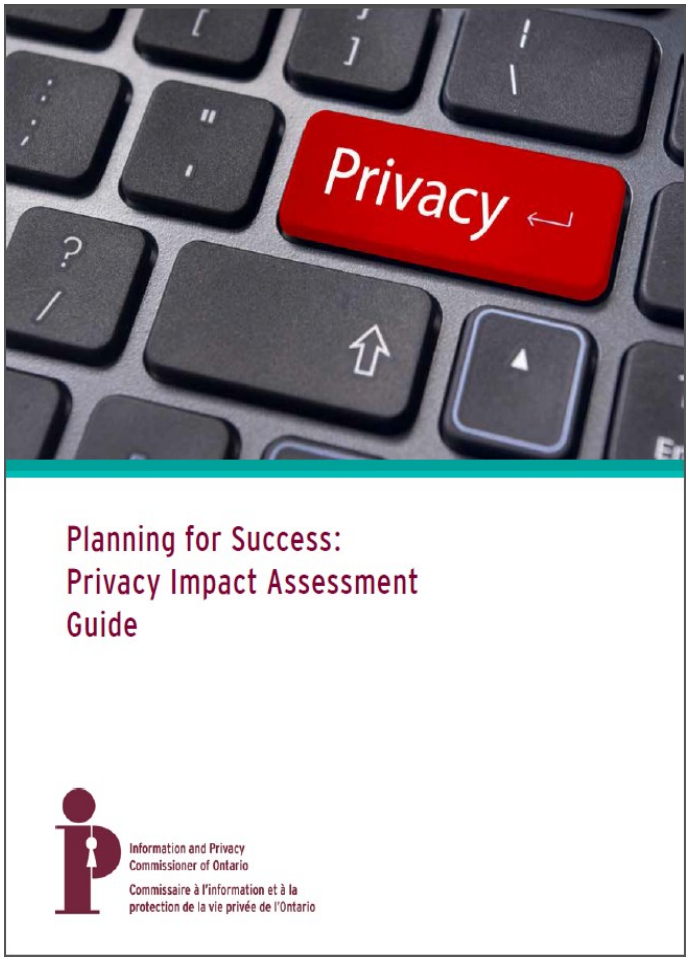
- Important work is being done to create new service delivery models designed to respond to significant risks of serious harms faced by vulnerable individuals
- Situation Tables and other innovative models can operate in a privacy protective manner with sufficient planning and governance
- Use of the privacy protective **roadmap** will help foster a strong sense of responsibility amongst all participants to maintain confidentiality and comply with privacy legislation
- The IPC is available to provide general guidance to communities with respect to operating innovative service delivery models in a privacy compliant manner

The IPC's Situation Tables webinar

- The IPC hosted a Situation Tables webinar on December 2, 2016
- The webinar can be used as a **training tool**
- It includes:
  - A presentation entitled "The Privacy Protective Roadmap for Situation Tables"
  - An interactive Q & A
- The complete webinar is available on our website at www.ipc.on.ca

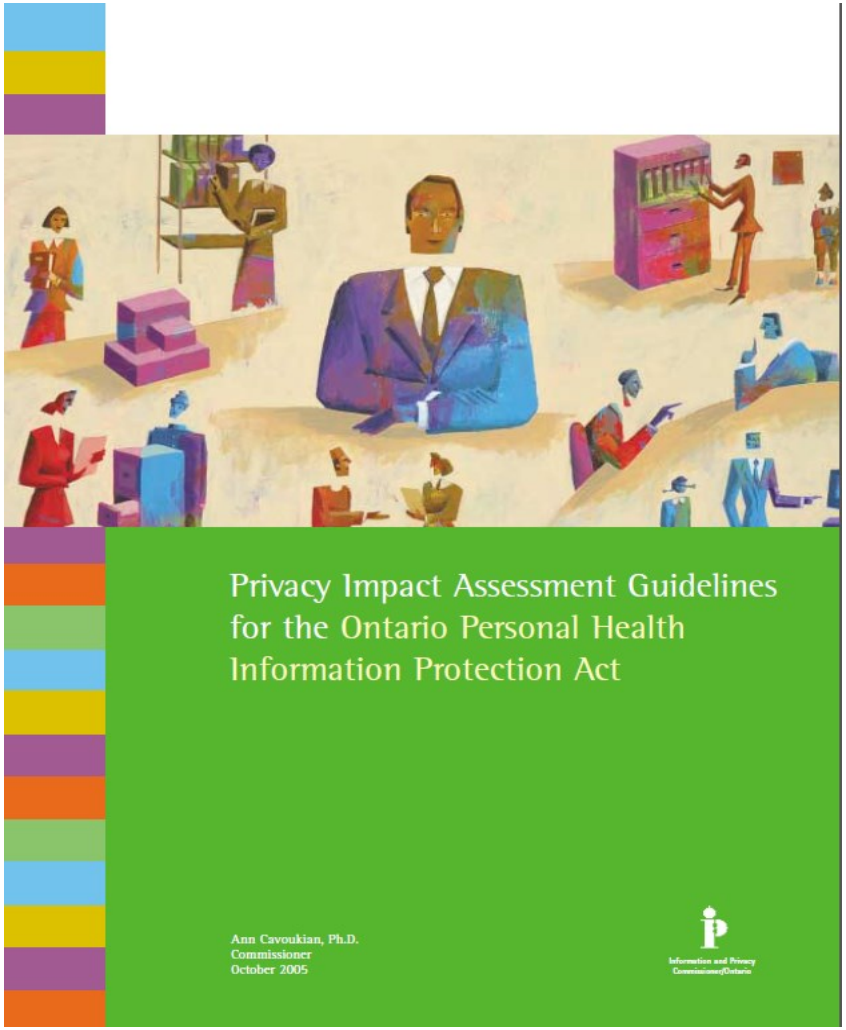
Privacy Impact Assessment Guide

- 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



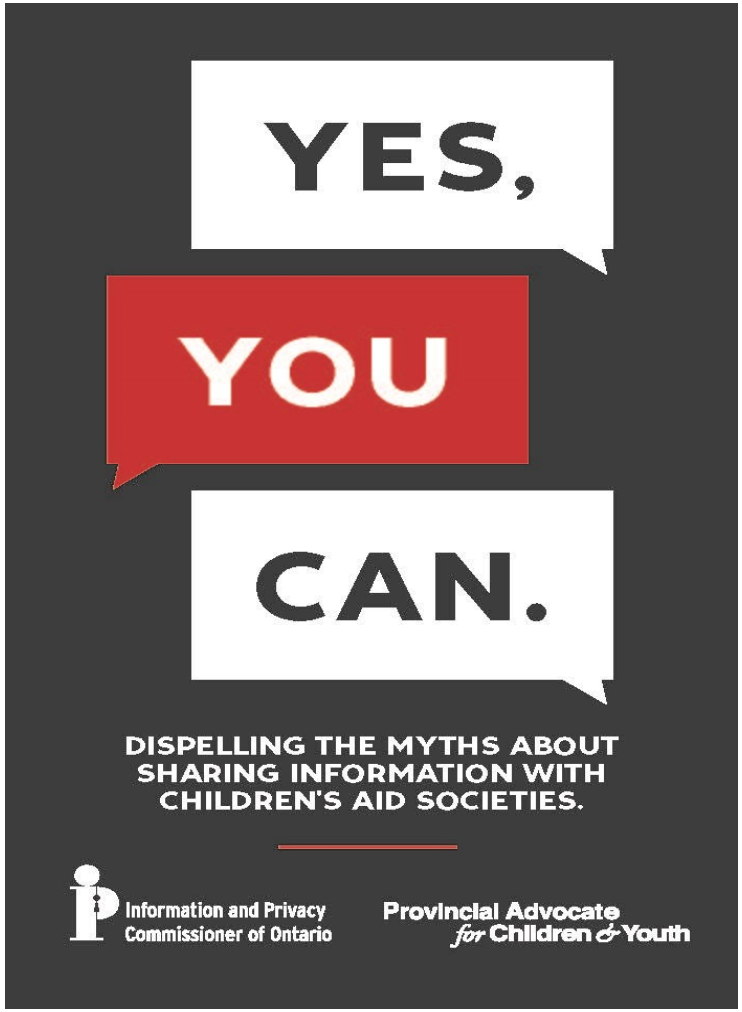
PIA Guidelines (*PHIPA*)

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



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



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

How to 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