2C: Information sharing and situation tables: a full course meal enabled by privacy compliance

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

PHIPA Connections Summit
Mississauga, Ontario

December 4, 2019

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

Legislation overseen by the IPC today

- *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 1,200 municipal organizations
- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - covers 300 provincial institutions

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

Coming soon – a new legislative mandate

Part X of the Child, Youth and Family Services Act (CYFSA)

- in force as of January 1, 2020
- big step forward for Ontario's child and youth sectors
  - closes a legislative gap for access to personal information and privacy protections
  - **modeled on *PHIPA***
  - promotes transparency and accountability

Ontario's privacy legislation – the broad strokes

- Institutions 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 information held by institutions
  - appeal access requests and privacy complaint decisions to the IPC

Looking at situation tables through the required privacy lens

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

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* 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

Key IPC guidance: ensure that table participants are working from the *same page*

- *Employ a single set of situation table privacy practices drawing on the highest relevant privacy standards*

- **Key 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

  - **Collection provisions:**
    - *PHIPA – ss. 30, 36*
    - *MFIPPA and FIPPA – ss. 28(2), 29(1); and 38(2), 39(1) respectively*

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 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

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** 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. Do not:
  - Handle PI/PHI when other information will serve the purpose
  - Collect, retain, use or disclose more PI/PHI than is necessary
  - Disclose PI/PHI to more agencies than is necessary
- **Transparency:** Participating agencies should be open with the public about their involvement in a situation table

The IPC's distillation of the Four Filter process

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
- **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 and scope of the disclosure, the withdrawal of consent)
- **Document** the consent
- Note, when collecting PI, institutions cannot rely solely on consent

	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?	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

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
- The IPC is available to provide general guidance to communities with respect to operating innovative service delivery models in a privacy compliant manner

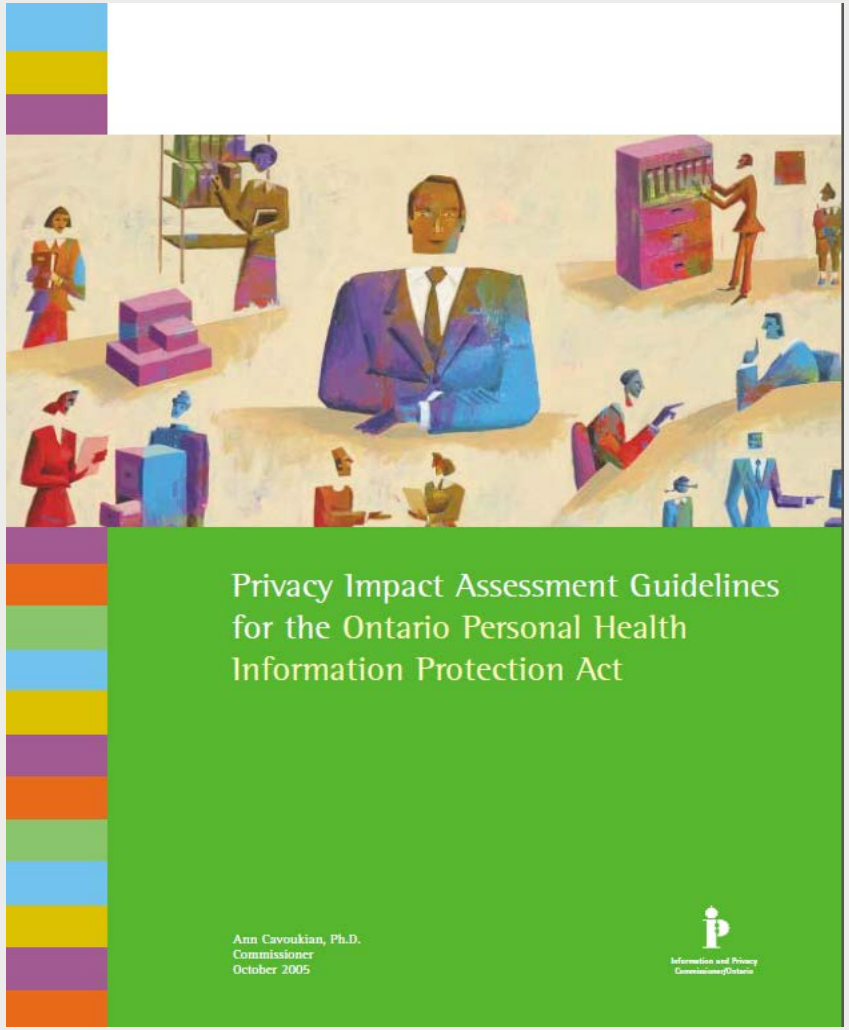
Additional IPC guidance

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

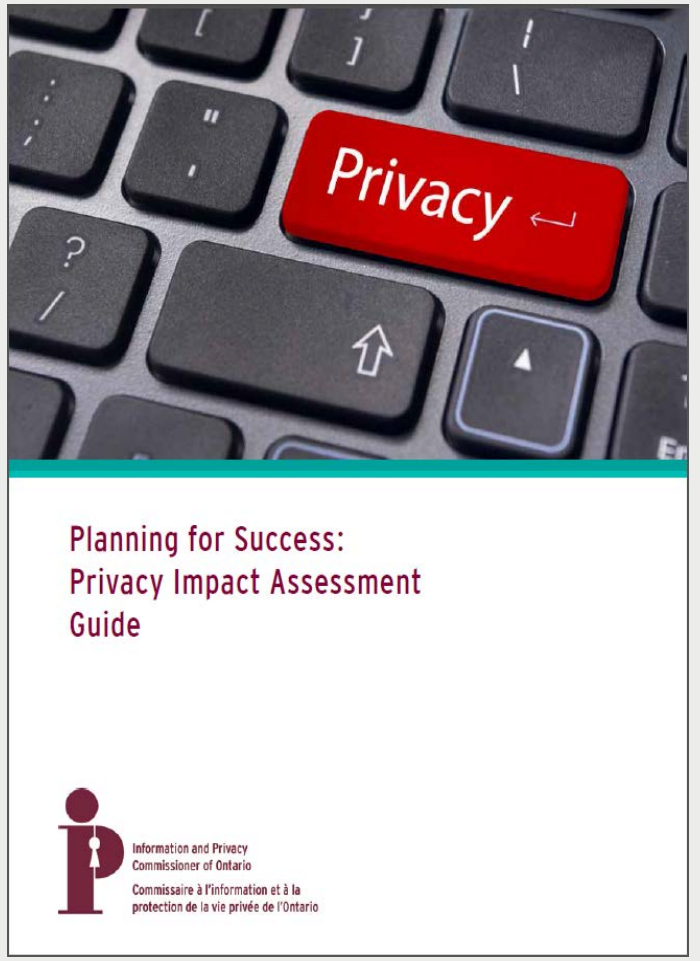
PIA Guidelines (*PHIPA*)

- 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



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