Collaborating to Reduce Serious Harm: A Privacy Protective Roadmap for Situation Tables

Stephen McCammon
Legal Counsel
Office of the Information and Privacy Commissioner of Ontario

Toronto's Collaborative Risk Driven Approach

Toronto Police College

December 2, 2016

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: Respect for Privacy

- 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

IPC Oversight

- 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)

Situation Table Work

- Participated in Law Reform Commission of Ontario workshop on integrated approaches to community safety (2013), Waterloo Region Crime Prevention Council dialogue on privacy and information sharing (2014) and *Economics of Policing Workshop* (Ottawa, 2015)
- Observed and commented on three Situation Tables: Cambridge, North Bay, & Rexdale FOCUS (2015)
- Continuing to respond to queries about Situation Table-related privacy issues and solutions, as well as to speak at forums and Situation Tables
- Worked closely with the Ministry of Community Safety and Correctional Services (Ministry) and the OPP on the development of new provincial guidance documents (2015-2016)

New Privacy Guidance

- The IPC provided detailed comments on:
  - The Ministry's August 2016 Guidance on *Information Sharing in Multi-Sectoral Risk Intervention Models:*
    - 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 privacy requirements
  - The roadmap is designed to allow agencies to collaborate to reduce significant risks of serious bodily harm
  - 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 shared and services are delivered in a privacy compliant manner

Taking Another Route: Proceed with CAUTION

- Consider conducting a privacy impact assessment
- 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)
- **RISK:** Disclosure of name/address/DOB (e.g. to the entire table at Filter 3) links the individual to the information disclosed at Filter 2
- **RISK:** A disciplined discussion is necessary, but is likely to be insufficient if disclosure is made to those who have no reasonably foreseeable role to play in planning or carrying out the required intervention
- **RISK :** The wider the disclosure of PI/PHI (e.g. at Filter 3 or during the Report back), 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 its actions and decisions**
- 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, 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 **handle** specific PI / PHI, under what circumstances and for what purpose(s)
  - outlines measures that must be implemented for the protection of PI / PHI

… Provides for Oversight …

- Situation Tables require **policies, procedures 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:
  - methods to ensure that information is **accurate and up-to-date**
  - the right to access and correct one's own record of PI / PHI
  - **record keeping requirements**, including those relating to the secure retention, transfer, and disposal of PI/PHI
  - periodic **auditing** of information handling practices
  - regular review of which agencies should participate
  - **training** requirements
  - **transparency** requirements

… is Guided by *Need-to-Know* Rules

- **Data-minimization is essential to compliance** (i.e. refrain from handling PI /PHI when other information will serve the purpose, do not collect, retain, use or disclose more PI/PHI than is necessary and do not disclose PI/PHI to more agencies than is necessary)

- At every stage, limit the handling of PI / PHI to those who have the legal authority to collect, use and disclose that information, and who have a **legitimate need** to know the information

- Situation Table chairs should facilitate a privacy compliant discussion while helping to identify risk factors, Filter 4 agencies, etc.

Best Practice - Seek Consent

- Whenever possible, PI /PHI should be collected, used and disclosed with the **individual's express consent** *[but remember, institutions must also comply with 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)

Moving from Filter 1 to Filter 2

- While an agency must use PI/PHI in selecting a case at Filter 1, it is **essential** that **only de-identified information be shared at Filter 2** (i.e. during the group's assessment of risk and the need for a multi-agency intervention)
- 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 age or location are relevant, refer to age in broad ranges like "minor", "adult" or "senior", and a neighborhood or street rather than a person's address)

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. If, for example, 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 Four.
- At this point, identifying information – information such as 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**.

Filter 4: A Separate Meeting

- 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
- If, during the Filter 4 meeting, 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**.
- A further agency may be added to the Filter 4 part of the meeting if it becomes clear that its involvement is **necessary**

The Intervention and Report Back Stages

- During the intervention, **consent should drive any further information sharing.** This consent should be sought at the first reasonable opportunity.
- If the individual declines the offer of service, further sharing of personal information 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.

Record keeping

- The agency that brings an individual case forward, as well as the planning and intervening agencies, may need to **record** some information about the case, including some personal information.
- 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.
- Any other notes captured by any of the other agencies should be **securely destroyed**, particularly any notes that may contain personal information.

Notice

- Individuals should **receive written notice shortly after** their PI/PHI is disclosed and contact information for each agency to whom their PI/PHI was disclosed or a contact number or website that allows the individual to readily access such contact information
- Written notice may be provided by, for example, the lead agency during the first in-person intervention using **a card, letter or pamphlet**
- If it becomes evident that the risks are already being mitigated (e.g. the individual is already connected to sufficient services), no further information sharing should occur at the Situation Table. However, the individual should still receive notice of any disclosure of their personal information from the disclosing agency. Such notice should also reveal the names of the agencies to which disclosure was made, and where to obtain further information.

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

Save the Date!

The IPC is hosting a Situation Tables Webinar

- Date: December 6, 2016
- Time: 11a.m. – 12 p.m.
- The presentation will be followed by an interactive question and answer session.

To register, see our “What’s New” page or look for us on Twitter, Facebook or LinkedIn

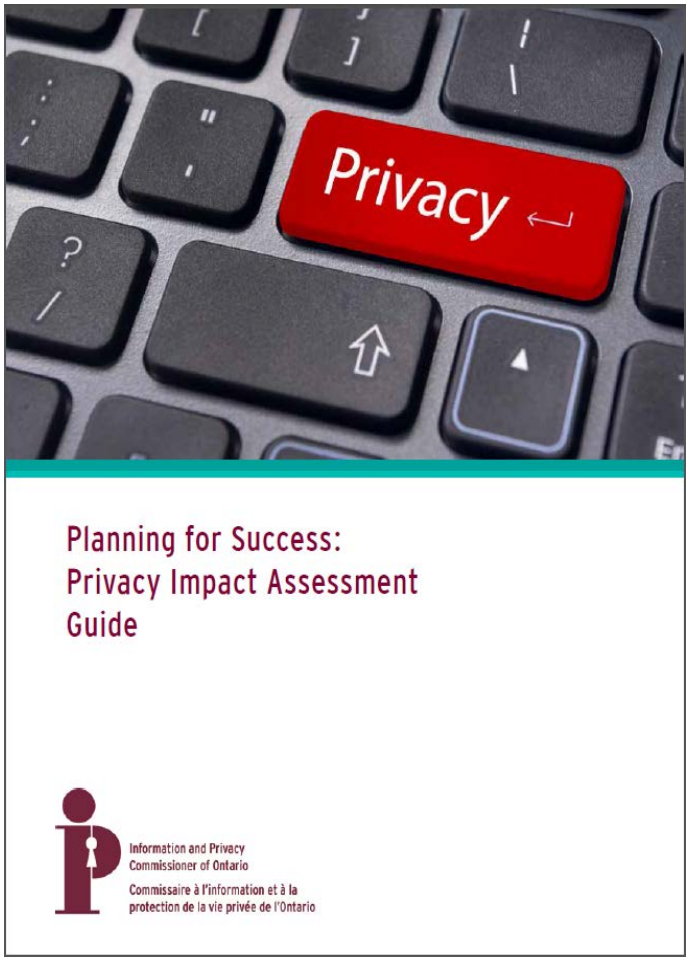
How to Contact Us

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

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