Collaborating to Prevent Harm: Privacy Issues and Solutions

Stephen McCammon
Legal Counsel
Office of the IPC of Ontario

Championing the Change Symposium
Pearson Convention Centre
October 28, 2015

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

Overview

- Background: Information and Privacy Commissioner Brian Beamish's (IPC) mandate, role, and recent activity

- Privacy issues and solutions in the context of a significant collaborative service delivery development: the situation table

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 mandate and role

The IPC ensures compliance with three privacy statutes:

FIPPA and ***MFIPPA which provide:***

- Right of access to information and appeal 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)

Championing the change & privacy …

- Increased focus on collaboration and information sharing to improve service delivery and reduce harm.
- Respecting privacy is essential to ensuring trust and providing effective service delivery.
- A roadmap for success accounts for privacy requirements and best practices.

… Ontario IPC involvement

- Staff participated in **Law Reform Commission of Ontario workshop** on integrated approaches to community safety (Nov. 2013), and **Waterloo Region Crime Prevention Council** dialogue on privacy and information sharing (June 2014)
- Commissioner participated in ***Economics of Policing Workshop*** (Ottawa, January 2015).
- IPC staff **observed and commented** on three situation tables in spring/summer, 2015: Cambridge, North Bay, & Rexdale FOCUS.
- IPC has **responded to queries** from various institutions interested in situation tables, as well as spoken at forums.
- **IPC continues to dialogue** with the Ministry of Community Safety and Correctional Services (MCSCS).

The Saskatchewan IPC HUB report

Nov. 2014, Saskatchewan IPC found necessary components of a privacy program were missing in Prince Albert, recommended changes to improve the program and comply with privacy legislation:

1. Destroy databases, spreadsheets linking case # and client names.
2. **Consent as the default** for use and disclosure of PI, collection, use and disclosure of PHI.
3. Use of a **standard referral form**.
4. Modify four filter approach (e.g. enforce **need-to-know access** past Filter 2, **delay** sharing PI until confirmation of "**acutely elevated risk**").
5. Comprehensive privacy **training** for participants.
6. Provide the public with **notice** and information re: complaint procedures.

Key privacy issues in Ontario

- Do participating agencies have adequate **legal authority** to collect, use and disclose PI / PHI at the situation table?
- Are you collecting, using and disclosing PI / PHI **with the individual's knowledge** (e.g. notice of indirect collection of PI)? Have you sought their **consent?**
- Are you disclosing PI /PHI when other information (e.g. de-identified information) will serve the purpose, or disclosing **more than necessary including** to **more agencies than necessary?**
- Do you have sufficient **governance, training, and oversight?**
- Are you employing adequate **de-identification** techniques?

Privacy solutions – legal authority

- Each participating agency must have legal authority for its information handling activities - **collection, use and disclosure of** PI / PHI (e.g. consent).
- Scope of authority determined vis a vis each agency's own mandate, duties, and powers and the applicable privacy statute.
- *In terms of non-consensual disclosure, FIPPA* and *MFIPPA* permit disclosure of PI, for example, "in **compelling circumstances** affecting the health or safety of an individual."
- Similarly, *PHIPA* permits the disclosure of PHI, for example, "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."
- *Receiving agencies must also have the authority to collect and use the PI or PHI.*

Privacy solutions – notice and consent

- Whenever possible, PI /PHI should be collected, used and disclosed with the **individual's 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.
- If consent is impractical, look to the **harm prevention disclosure** provisions in the privacy acts for authority to disclose PI or PHI (s. 32(h) of *MFIPPA*, s. 42(1)(h) of *FIPPA*, s. 40(1) of *PHIPA*).
- Individuals must still **receive notice** that their PI has been disclosed.

Privacy solutions – the recommended harm prevention disclosure framework

When disclosure of PI / PHI without consent is necessary, the following framework is *recommended* for determining if the disclosure is compliant with Ontario privacy acts:

1. It is reasonable for the disclosing agency to believe that the subject individual is at **significant risk** of serious bodily harm or poses a significant risk of serious bodily harm to others;
2. The disclosing agency is **unable to reduce or eliminate the risk** without disclosing PI or PHI;
3. It is reasonable for the disclosing agency to believe that disclosing the PI or PHI to one or more specific agencies **will reduce or eliminate** the risk posed to, or by, the individual;
4. The disclosure of PI or PHI is limited to that which is **reasonably necessary** to develop and implement an **effective strategy** to reduce or eliminate the risk; and
5. Each recipient agency has the authority to collect the PI or PHI and has a **role to play** in the development and implementation of an effective strategy to reduce or eliminate the risk.

Privacy solutions – 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.

- All institutions and HICs (not just situation table chairs) must be responsible for complying with privacy legislation and **accountable for their actions**.

- Part of that accountability must be to the public. Institutions and HICs should be **transparent about their participation** in a situation table.

Privacy solutions – avoiding excessive disclosure

- Handling of PI / PHI must be limited to those who have the legal authority to collect, use and disclose that information, and who have a **legitimate need** to know the information.
- To ensure appropriate disclosures, participating agencies should consider signing **information sharing agreements ,** particularly with agencies not covered by privacy legislation.
- **An information sharing agreement should**:
  - confirm who may access specific PI / PHI and under what circumstances and for what purpose;
  - ensure that adequate measures for the protection of PI / PHI are followed.

Privacy solutions – oversight

- Situation tables require consistent **oversight mechanisms** to ensure continued adherence to privacy legislation.

- Information management protocols will assist members in ensuring that all information is collected, used and disclosed appropriately. Protocols should be established for:
  - Effective **record keeping practices**
  - Methods to ensure **accuracy and currentness** of information
  - Ability to ensure access and correction of **one's own** record of PI / PHI
  - **Secure** retention and disposal
  - Regular **auditing** of information sharing practices and appropriateness of continued participation.

Privacy solution – de-identification

- De-identification of information is **essential (e.g. at Filter 2)**, but removal of direct identifiers may not be sufficient to prevent re-identification.
- 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.
- "**Quasi-identifiers**" can be used for **re-identification** (e.g. gender, marital status, location information, date, diagnosis information, profession, ethnic origin, visible minority status, and/or income.).
- These quasi-identifiers can be used either by themselves or in combination with other available information to uniquely identify individuals.

General observations

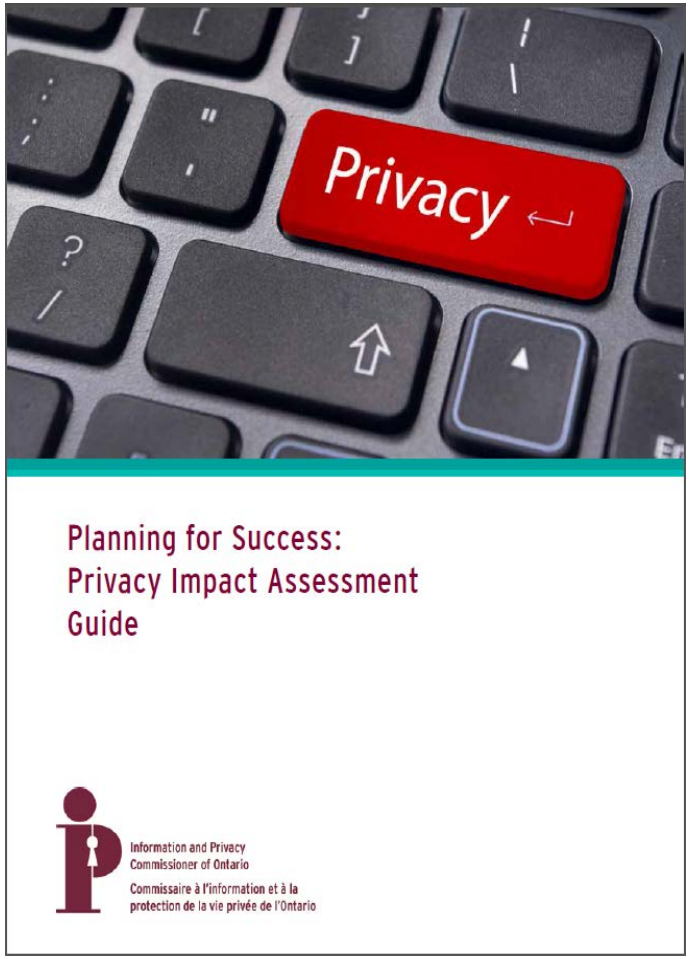
- Excellent work is being done in Ontario to create new service delivery models that respond to urgent needs of vulnerable populations.
- Situation tables and other innovative models can operate in a privacy protective manner with **sufficient planning and governance**.
- IPC continues to provide comments to the MCSCS to **facilitate compliance with privacy acts, including on the four filter approach**.
- B**est practices** for situation tables include:
  - De-identification
  - Strong sense of responsibility of all participants to maintain confidentiality and comply with the privacy acts
  - Looking to consent 1st for the collection, use and disclosure of PI and PHI
  - Collection, use and disclosure limited to a need-to-know basis

Next Steps

- MCSCS has committed to **developing tools and guidance** for communities interested in establishing situation tables.
- The IPC has committed to supporting MCSCS as it works to develop these tools by providing it with **privacy guidance**.
- Communities working to develop and improve on other innovation service delivery models can approach the IPC for privacy guidance at any time.

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.



https://goo.gl/9gM1x6

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.