

# Data Sharing Among Public Institutions

## *Balancing Privacy and Service Delivery*

Brian Beamish

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

Durham Connect  
Summit

October 11, 2018

# Our Office

- Information and Privacy Commissioner (IPC) provides **independent** review of government decisions and practices on access and privacy
- Commissioner is appointed by, and reports to the Legislative Assembly, to ensure **impartiality**

## Our Mandate

- *resolve* access to information appeals
- *investigate* privacy complaints – public sector and health
- *research* access and privacy issues
- *comment* on proposed government legislation and programs
- *educate* the public and government on issues of access and privacy



# The Legislation

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



# New Mandates

## *Child, Youth and Family Services Act*

- effective January 1, 2020
- big step forward for Ontario's child and youth sectors
  - closes a legislative gap for access and privacy
  - promotes transparency and accountability

## *Anti-Racism Act*


- passed June 2017
- requires public sector organizations in child welfare, education and justice sectors to collect information about Indigenous identity, race, religion and ethnic origin
- includes requirements to protect collected information

# Ontario's Privacy Laws

- Institutions must:
  - follow rules on how they collect, use, retain, disclose and dispose of personal information
  - collect, use or disclose information only for legitimate, limited and specific purposes
  - inform individuals how they intend to use their personal information
  - provide the name of their Freedom of Information and Privacy Coordinator
- Individuals have the right to file a privacy complaint with the IPC
- private-sector privacy law
  - *PIPEDA* – overseen by the Privacy Commissioner of Canada – applies to commercial businesses in Ontario

# What is Personal Information?

- It is recorded information about an individual such as:
  - name, address, sex, age, education, and medical or employment history
  - social insurance number
  - personal views or opinions
- Business information is not personal information



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

Fact Sheet

## What is Personal Information?

October 2016

### INTRODUCTION

The *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* (the acts) protect the privacy of personal information while providing individuals with a right of access to their own information.

In this fact sheet, we provide guidance about how the Information and Privacy Commissioner (IPC) interprets the term "personal information."

### HOW IS PERSONAL INFORMATION DEFINED IN THE ACTS?

The acts define personal information as "recorded information about an identifiable individual," and include a list of examples of personal information (see Appendix A for the full definition).

**Recorded information**

Information can be recorded in any format, such as paper records, electronic records, digital photographs, videos or maps.

**About an identifiable individual**

Information is about an identifiable individual if:

- it is about the individual in a personal capacity; that is, it reveals something of a personal nature about the individual, and
- it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information)

The listed examples include a person's name when combined with other information about them, such as their address, sex, age, education, or medical history. These examples are not exhaustive and many other kinds of information may still qualify as personal information.



# Situation Tables



# FIPPA/MFIPPA/PHIPA Collection and Disclosure Rules

- *M/FIPPA* participants are authorized to **collect** personal information, when it is necessary to provide a service
- *M/FIPPA* participants are authorized to **disclose** personal information if:
  - ✓ individual consents
  - ✓ disclosure is for a consistent purpose
  - ✓ to comply with another law (e.g. *CFSA* duty to report)
  - ✓ in compelling circumstances (risk of harm)
- *PHIPA* participants are authorized to collect and disclose:
  - ✓ consent
  - ✓ risk of harm



# Situation Tables and Privacy Concerns

Situation tables create an **information-sharing environment** to enable local agencies to develop intervention strategies in cases involving “acutely elevated risks of harm”

- Key privacy issues under *FIPPA*, *MFIPPA* and *PHIPA* include:
  - legal authority to collect, use and disclose personal information
  - consent
  - personal information being used when de-identified information will serve the purpose
  - insufficient governance, training and oversight

# Privacy Guidance on Situation Tables

- The Ministry of Community Safety and Correctional Services (MCSCS), *Guidance on Information Sharing in Multi-Sectoral Risk Intervention Model*
  - provides a **roadmap** for information sharing at situation tables in a way that protects individual privacy, using a four-filter approach
- Chapters VI and VII of a *Situation Table Guidance Manual*
  - produced in April 2016, by Dr. Hugh Russell, with a grant from the MCSCS and guidance from the OPP

# Success with Situation Tables

- **strong governance** to ensure all participants understand their responsibilities and are able to participate in the situation table
- appropriate handling of personal information through an **information sharing agreement**, especially if not covered by privacy legislation
- **policies, procedures and practices** to ensure continued adherence to privacy legislation
- **data-minimization** is essential to compliance. Do not:
  - handle personal information when other information will serve the purpose
  - collect, retain, use or disclose more information than is necessary
  - disclose personal information to more agencies than necessary



# Best Practice – Seek Consent

- If possible, seek the individual's express consent to collect, use and disclose their information
- Institutions must also comply with *FIPPA* and *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
  - **inform the individual** what information will be shared, which agencies will receive it, and for what purpose
  - **respect** the individual's choices regarding their specific disclosure requests
  - **document** the consent



# Disclosure for Planning and Analysis

# Data Integration in and Between Public Institutions

- **Sharing, linking, analyzing data** across agencies can result in new insights for:
  - policy development
  - system planning
  - resource allocation
  - performance monitoring
- *FIPPA/MFIPPA* **does not** permit disclosure for these purposes



# S. 42(1)(d) of *FIPPA*

- *FIPPA* is outdated and does not permit disclosure of PI among institutions except in limited circumstances
- Section 42(1)(d) provides that  
An institution shall not disclose personal information except  
[...]  
where disclosure is made to an officer, employee, consultant or agent **of the institution** who needs the record in the performance of their duties and where disclosure is necessary and proper in the discharge of the institution's functions;

# Privacy Risks of Data Integration

- not based on consent – lack of transparency
- replication of massive government databases of linked and identifiable personal information
- surveillance and profiling of individuals
- increased cybersecurity risks
- potential discrimination based on inaccurate data/flawed algorithms

# *PHIPA* – A Modern Approach to Privacy

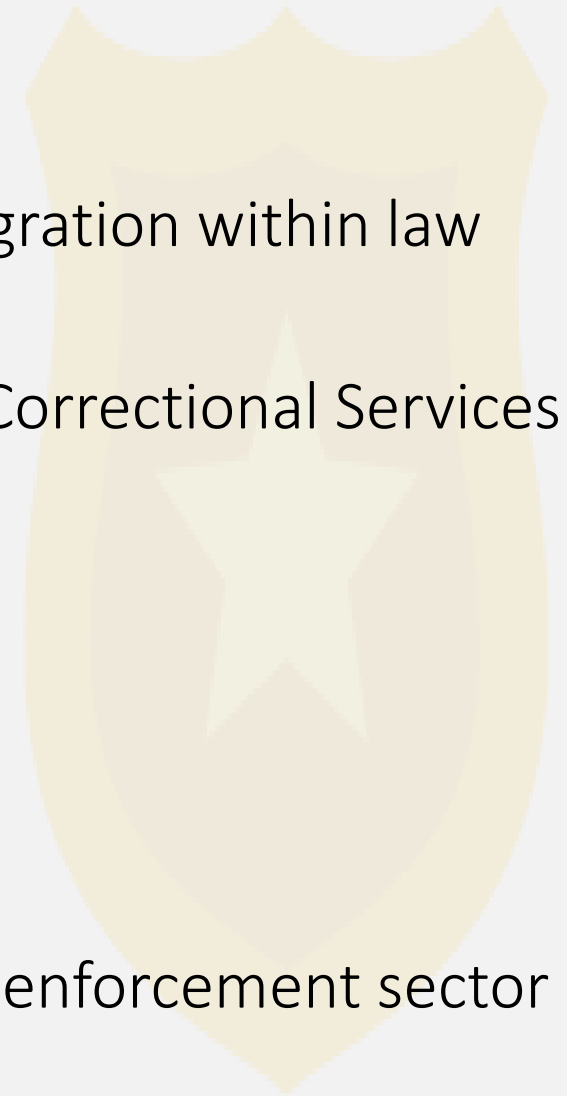
- Ministry of Health and Long-Term Care can collect and link personal health information from health providers, for:
  - funding, planning or allocating resources
  - detecting, monitoring or preventing fraud
- Must have controls to protect privacy
  - prescribed unit to perform data integration
  - de-identification
  - IPC review of unit's practices and procedures
  - independent oversight
- IPC has strong investigative/audit powers under *PHIPA*





# Bill 175 – *Police Services Act, 2017*

- Includes measures to protect privacy while enabling data integration within law enforcement sector:
  - designated unit within Ministry of Community Safety and Correctional Services to perform data integration
  - de-identification
  - IPC review of unit's practices and procedures
  - IPC order-making powers
  - offence provisions
- Does not allow for unrestricted data sharing from outside law enforcement sector



# IPC and Ontario Government Working Group

- IPC and Ontario Government staff are working to design a legislative framework to enable a centralized approach to data integration to ensure:
  - no replication of linked datasets across multiple government agencies
  - consistent application of privacy controls
  - independent oversight
  - public trust and accountability

# IPC's Proposed Amendments to *FIPPA*

- enable **inter-ministerial data integration**
- require a single dedicated unit within the OPS to:
  - collect and link personal information on behalf of ministries
  - de-identify information
  - make only de-identified information available to ministries for system planning, analysis and evaluation
- establish framework for privacy controls – section 55.9 of *PHIPA* model
- enhance investigative/audit/order making powers of the IPC

# IPC's Proposed Amendments to *FIPPA*

Cont'd

- enable **sector-specific data integration**
- require a dedicated unit within a ministry to:
  - collect and link personal information from prescribed service providers and other agencies within a specific sector
  - de-identify the information
  - make only de-identified information available to ministry staff for system planning, analysis and evaluation
- establish framework for privacy controls – section 55.9 of *PHIPA* model
- enhance investigative/audit/order making powers of the IPC



# Guidance Materials



# 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



TECHNOLOGY

MAY 2017

## Big Data Guidelines



## De-identification Guidelines for Structured Data

June 2016



## Planning for Success: Privacy Impact Assessment Guide



# Our Open Door Policy

- Any public institution or agency considering programs which may impact privacy can approach IPC for advice
- Most privacy challenges can be addressed through collaboration
- Privacy protections can be developed and can be implemented
- It is best to address privacy concerns from the outset
- Success depends on involvement of other agencies and stakeholders

“A democratic society relies upon the participation of an informed citizenry. A city cannot be truly innovative and respect the rights of its residents if only a sliver of public officials have the power to speak for — or to ignore — the broader community. Every resident has the right to participate in decision-making processes that impact their constitutional rights.”

— American Civil Liberties Union





# 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](http://www.ipc.on.ca)

E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)

Media: [media@ipc.on.ca](mailto:media@ipc.on.ca) / 416-326-3965