

OSBIE

Risk Management Seminar

**Managing Privacy, Security and
Access to Information
Compliance Risks**

Renee Barrette / Fred Carter

Policy Director / Senior Advisor

Toronto

October 20, 2017



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

Agenda

IPC Mandate and Role

MFIPPA

Privacy and Access Risks

Risk Mitigation Strategies

New Developments

Questions?



IPC

Mandate and Role



IPC Mandate and Role

- Established in 1988
- Commissioner appointed by and reports to Legislative Assembly
- *MISSION*: We champion and uphold the public's right to know and right to privacy
- *MANDATE*:
 - resolve access to information appeals and privacy complaints
 - review and approve information practices
 - conduct research, deliver education and guidance on access and privacy issues
 - comment on proposed legislation, programs and practices



Legislation

The IPC oversees compliance with:

- ***Freedom of Information and Protection of Privacy Act (FIPPA)***
 - over 300 provincial institutions such as ministries, provincial agencies, boards, commissions, community colleges and universities
- ***Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)***
 - over 1,200 organizations such as municipalities, police, school boards, conservation authorities, transit commissions
- ***Personal Health Information Protection Act (PHIPA)***
 - individuals and organizations involved in delivery of health care services, including hospitals, pharmacies, laboratories, doctors, dentists and nurses



MFIPPA



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

MFIPPA

The purposes of *MFIPPA* are:

- to provide a **right of access to information** under the control of institutions in accordance with the principles that
 - information should be available to the public
 - access exemptions should be limited and specific
 - access decisions should be reviewed independently of government
- to **protect the privacy of individuals** with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information



Institutions

- *MFIPPA* applies to “**institutions**” regarding the general records and records of personal information in their custody and control
- Institutions under *MFIPPA* include **school boards**
- School boards remain responsible for the information practices of educators and **third-party service providers**



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.

- Personal information is **any recorded information that is identifiable to an individual**
- The acts list examples of personal information
- This fact sheet provides guidance about how the IPC interprets the term "personal information"



Privacy Obligations Under *MFIPPA*

MFIPPA sets out rules for the **collection**, **use**, and **disclosure** of personal information

To **collect** personal information, it must be:

- Expressly authorized by statute
- Used for the purposes of law enforcement, or
- Necessary to the proper administration of a lawfully authorized activity

Example:

Government institutions must have a legitimate reason and purpose for collecting personal information, such as a school board installing cameras to protect the safety and security of its students

You can only **use** personal information for:

- The purpose it was collected
- A consistent purpose or with consent (preferably in writing)

Example:

Video footage collected by a security camera cannot be used to monitor student attendance, but it may be used in relation to a security incident

You can only **disclose** personal information:

- With consent
- For a consistent purpose
- To comply with legislation
- For law enforcement
- For health and safety reasons
- For compassionate reasons

Example:

A video capturing evidence of a crime can be shared with law enforcement, even if it contains personal information



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Privacy Obligations under *MFIPPA*

Security of Personal Information rules

Information must be **retained**

- if used by an institution, it must be retained for at least one year

Retention rules allow time for individuals to access their personal information

No **use** unless

- accurate
- up to date

Reasonable measures must be taken to make sure that the information being used is accurate

Information must **protected**

- it must be protected from inadvertent disclosure and unauthorized access

IPC expects administrative, technical and physical measures to be in place to protect personal information



Yes, You Can

YES,

YOU

CAN.

DISPELLING THE MYTHS ABOUT
SHARING INFORMATION WITH
CHILDREN'S AID SOCIETIES.

 Information and Privacy
Commissioner of Ontario

 Provincial Advocate
for Children & Youth

- Collaboration with Provincial Advocate for Children and Youth
- Professionals sometimes cited privacy as the reason for refusing to disclose information to child protection workers
- Dispels myths - privacy legislation is not a barrier to sharing information about a child who may be at risk

Access Rights

Under *MFIPPA* every person has a **right** to access a record or a part of a record in the **custody or under the control** of an institution unless:

- contents fall within exemptions
- the request is frivolous or vexatious
- the record is specifically excluded, or
- another act overrides the legislation

Right of access applies to **records** which is broadly defined to include:

- correspondence, working notes (notebooks), photos,
- expense accounts, videos, e-mails, appointment books and schedules,
- draft documents, voicemails and texts



Access Requests

- Requests can be made by anyone, for any reason - no obligation on the requestor to provide a reason for making the request
- Once an access request is received **all responsive records must be retained** – they cannot be altered, deleted, or shredded



Exemptions: Limited and Specific

There are two separate categories of exemptions under Ontario's access laws:

- 1) mandatory exemption – Head of an institution **must** withhold the record
- 2) discretionary exemption – Head of an institution **may choose** to withhold the record

DISCRETIONARY EXEMPTIONS

- Draft by-laws, record of closed meetings (*MFIPPA* only)
- Advice or recommendations
- Law Enforcement
- Economic and other interests
- Solicitor-client Privilege
- Danger to safety or health
- Species at risk (*FIPPA* only)
- Information soon to be published
- Requester's own personal information

MANDATORY EXEMPTIONS

- Relations with other governments
- Cabinet records (*FIPPA* only)
- Third party information
- Someone else's personal information



PRIVACY and ACCESS RISKS



What is a Privacy Breach?

- A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the act
- Among the most common breaches of personal privacy is the **unauthorized disclosure** of personal information, such as:
 - sending communications to the wrong recipient due to human error
 - improper records destruction procedures
 - loss or theft of unsecured assets, such as laptop computers, digital cameras, or portable storage devices (USB sticks)
 - unauthorized access (snooping, hacking)



IPC Privacy Investigations

The IPC may:

- receive privacy complaints from the public or investigate on its own accord
- investigate privacy complaints and report publicly on them
- order the institution to cease and destroy a collection of personal information
- make recommendations to safeguard privacy



IPC Privacy Investigations

Depending on circumstances, IPC may:

- ensure adequate containment, notification
- interview appropriate individuals
- obtain and review the organization's position on the breach
- ask for status report of any actions taken by the organization
- review and provide input and advice on current policies and procedures and any other relevant documents and recommend changes
- issue a report or order at the conclusion of the review



Privacy Class Action

Jones vs Tsige (2012)

- New common law right of action for invasion of privacy, tort of “intrusion upon seclusion”
- Conditions:
 - unauthorized intrusion
 - matter intruded upon was private
 - highly offensive to a reasonable person, causing distress, humiliation or anguish



Privacy Class Action

Casino Rama

- Cyberattack discovered November 2016
- Confidential data of employees, customers and vendors stolen
- National class action lawsuit commenced 4 days after the breach was publicly announced
- Plaintiffs claiming \$60 million in damages, plus legal costs and paid credit monitoring for the plaintiffs



MFIPPA Offense Provisions



FIPPA and MFIPPA: Bill 8 – The Recordkeeping Amendments

December 2015



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

- Bill 8, *Public Sector and MPP Accountability and Transparency Act*
- Requires institutions to take **reasonable measures** to protect their records in accordance with recordkeeping requirements
- Makes it an **offence** to alter, conceal or destroy a record with the intention of denying a right to access the record, with a penalty of up to \$5,000



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

Ransomware



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

Technology Fact Sheet

Protecting Against Ransomware

July 2016

Ransomware has become an increasingly common and dangerous threat to the security of electronic records. This fact sheet provides information on how public institutions and healthcare organizations in Ontario can protect themselves against it.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or "malware," that encrypts files on your device or computer, including any mapped or network drives, and then demands payment in exchange for the key needed to decrypt the files. It essentially locks you out of your data and holds the means of regaining access for ransom.

HOW DO COMPUTERS GET INFECTED?

Hackers use different techniques to install ransomware on computers. In general, these fall into two categories: "phishing" attacks and software exploits.

Phishing Attacks

Phishing is a type of online attack in which a hacker sends one or more individuals an unsolicited electronic communication—email, social media post or instant messenger chat—designed to trick or deceive a recipient into revealing sensitive information or downloading malware.

In the case of ransomware, the hacker will often try to impersonate an "official" correspondence relating to a common business transaction, such as a shipping notice or invoice from a delivery company. The hacker may also try to fake an "urgent matter," such as an unpaid invoice or notice of audit. More advanced versions (also known as "spear phishing") target specific individuals or places of business.

Ransomware may be installed if the recipient opens a file attachment or clicks on a link in the body of the message.

- IPC Fact Sheet released in July 2016
- What is ransomware?
- How do computers get infected?
 - phishing attacks
 - software exploits
- Protecting your organization
- Responding to incidents
- Available at www.ipc.on.ca



Risk Mitigation



Privacy Impact Assessments (PIAs)



Planning for Success:
Privacy Impact Assessment
Guide

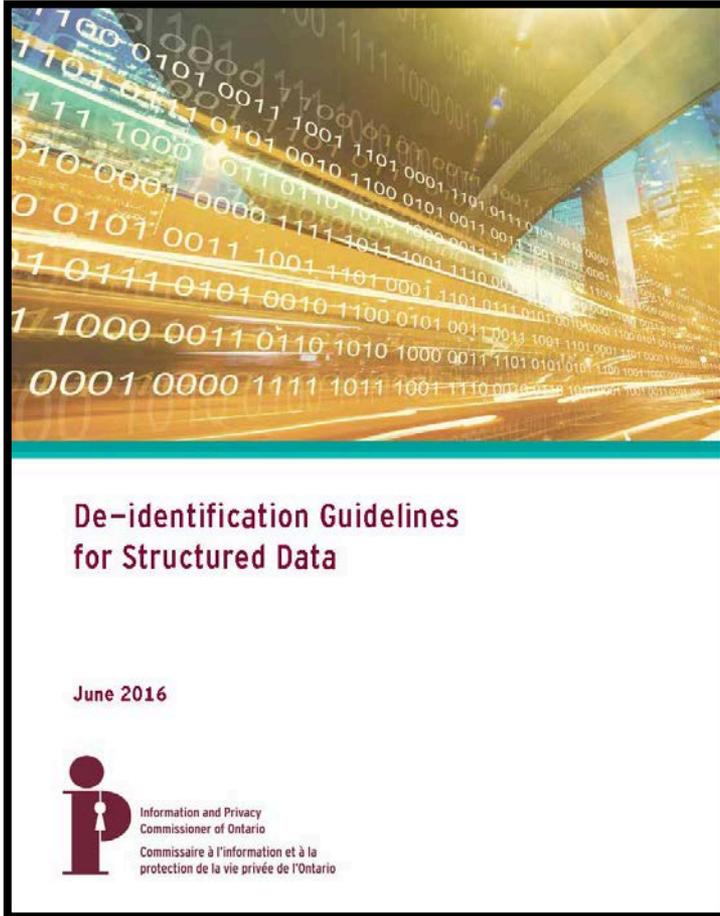
- A PIA is a formal risk management tool used to **identify the actual or potential risks** that a proposed or existing information system, technology or program may have on individuals' privacy
- A PIA should be conducted during the design phase and **prior to implementation**
- IPC **highly recommends** a PIA

PIA Benefits

- A PIA will help:
 - identify **privacy and security risks**
 - develop mitigation strategies
 - **reduce costs** by providing “early warnings” of challenges
 - determine necessary **roles and responsibilities**
 - foresee problems in merging technologies and systems
 - **set standards** for new data handling practices and existing systems handling new information



De-identification



- **De-identification is the removal of personal information from a record or data set**
- This guide outlines a risk-based, step-by-step process to assist institutions in de-identifying data sets containing personal information
- Covers key issues to consider when publishing data

Records & Information Management



Improving Access and Privacy with Records and Information Management

November 2016



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

- Effective RIM practices help institutions **meet legal requirements and better serve the public**
- This paper provides guidance to help institutions understand the relationship between strong RIM practices and compliance with the acts



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

RIM Best Practices

- Improve ability to respond to FOI requests in a timely manner
- **Reduce costs** to organization and requester by making searches more efficient
- Facilitate responses to requests for **correction** of personal information
- **Reduce risk of a privacy breach** and improve privacy breach response
- **Reduce reputational risks** by improving statistical reports and relationships with requesters



Security Best Practices

Reducing Risk of Breaches

Administrative

Technical

Physical



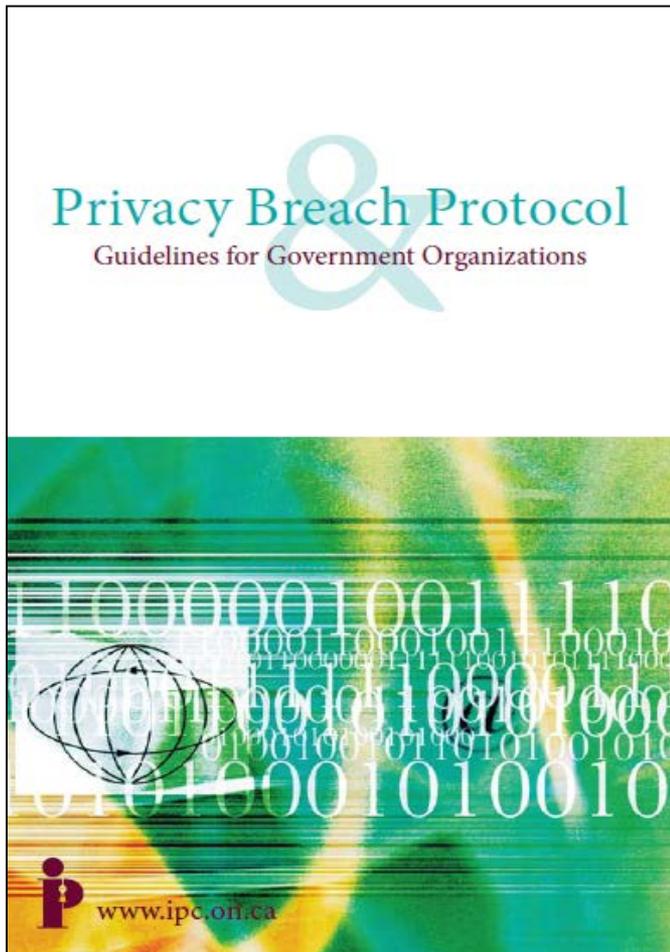
Responding to a Privacy Breach

Key Steps:

- Implement / identify
- Contain
- Notify
- Investigate / remediate



Privacy Breach Protocol



- privacy breach protocol helps identify privacy risks, potential and actual breaches
- ensure training on protocol
- ensure staff know their responsibilities when a breach occurs



New Developments



Privacy Breach Reporting

- No mandatory breach reporting to IPC under *MFIPPA*
- Mandatory breach reporting to IPC for health information as of October 1, 2017
- We receive voluntary breach reports under all three statutes
 - 102 public sector self-reported (2016)
 - 233 health sector self-reported (2016)
 - more learned from complainants, media



Health Sector Privacy Breach Reporting

- Health information custodians are required to report privacy breaches to the IPC in seven categories described in the regulations
- Each category is discussed, examples provided

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

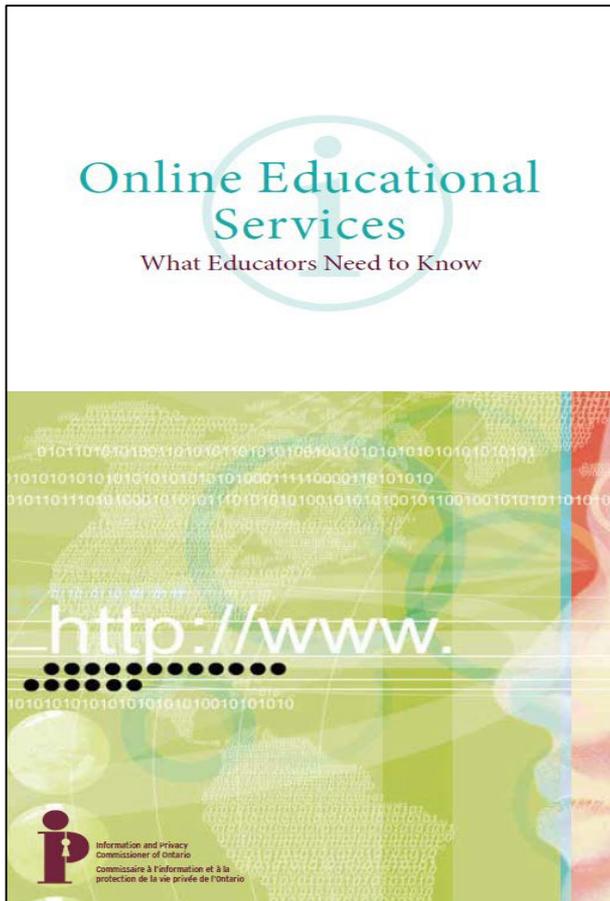
This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Online Educational Services



- Teachers use online educational services for learning, communication, evaluation
- While innovative and inexpensive, they could risk privacy of students
- School boards must ensure online services used by teachers are compliant with *MFIPPA*
- IPC and Ontario Association of School Board Officials (OASBO) created fact sheet about privacy risks of online educational services

Best Practices for Using Online Educational Services

- Consult with school board, principal and/or administrators before selecting an online education service
- Read and understand privacy policies and terms of service
- Minimize the identifiability of students, where feasible
- Involve parents and guardians, where appropriate
- Provide timely and ongoing guidance to students on appropriate uses of online educational services



Online Educational Services

- **IPC workshop “Privacy in the Networked Classroom”**
 - Co-sponsors: eQuality Project, Big Data Institute, OASBO
 - Bring IT Together (BIT17) Conference, Niagara Falls
 - Full day: November 8, 2017
- **Ministry of Education “Decision Tree” Tool**
 - Working Group of education stakeholders
 - Goal: create an online tool for educators to use when considering online educational services
 - Tool features series of questions, guidance and information
 - Beta launch at BIT17



Video Surveillance Guidelines



Guidelines for the Use of Video Surveillance

October 2015

- The IPC first published guidelines on the use of video surveillance in public places in 2001 and then on the use of video surveillance in schools in 2003.
- This guide consolidates previous advice and presents some new issues and factors to consider, including **retention periods** and **notices of collection**.
- It also provides **key messages** and **examples** for clarity.

Video Surveillance Guidelines

- **Best practices** include conducting a **privacy impact assessment**, consulting the public and establishing policies and procedures.
- Institutions must be prepared to process requests for information from the public including developing protocols for the **redaction of personal information** from the video footage where appropriate.
- Updated guidance on **retention period for unused footage** to a “reasonableness” standard:
 - “...limited to the **amount of time reasonably necessary** to discover or report an incident that occurred in the space under surveillance.”



Video Surveillance Guidelines

Policies and Procedures

- Comprehensive policies and procedures should be in place to address privacy and security issues including:
 - when **recording will be permitted**, required, prohibited
 - retention, use, disclosure and destruction of recordings
 - privacy/security **safeguards** for cameras, servers, and other systems (e.g. encryption, role-based access, audit processes)
 - responding to access requests



Questions?



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Contact

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

