Best Practices for Privacy Protection

Renee Barrette

Director of Policy

Information and Privacy Commissioner of Ontario

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

City of Brampton
Privacy Event

November 23, 2017

Agenda

- Who We Are
- Legislative Requirements for Privacy
- Privacy Risks and How to Mitigate Privacy Risks
- Recent Privacy Investigations

Who We Are

IPC Mandate and Role

Established in 1988

Commissioner is appointed by and reports to Legislative Assembly

MISSION: We champion and uphold the public's right to know and 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

IPC's Legislation

- *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

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

Legislative Requirements for Privacy

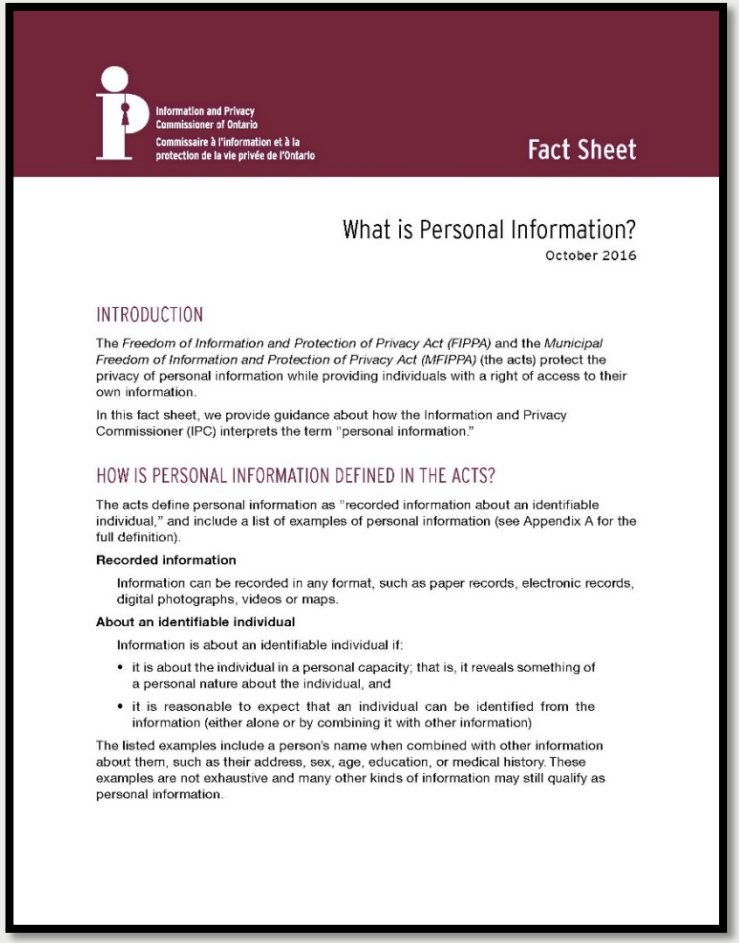
Fair Information Practices

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Key Obligations under *MFIPPA*

- legal authority to collect
- data minimization
- notice to data subjects
- retention
- safeguards
- give person access to their own PI

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 act lists examples of personal information
- This fact sheet provides guidance about how the IPC interprets the term "personal information"

What is a record?

A record is any record of information however recorded, whether in printed form, on film, by electronic means or otherwise and includes, for example:

- correspondence
- memorandum
- plans
- maps
- drawings, diagrams, pictorial or graphic work
- photographs, film, microfilm, sound records, videotape

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

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

- the purpose it was collected
- a consistent purpose or with consent (preferably in writing)

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

Privacy Obligations Under *MFIPPA*

Cont'd

Security of Personal Information rules

Information must be **retained**

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

No **use** unless

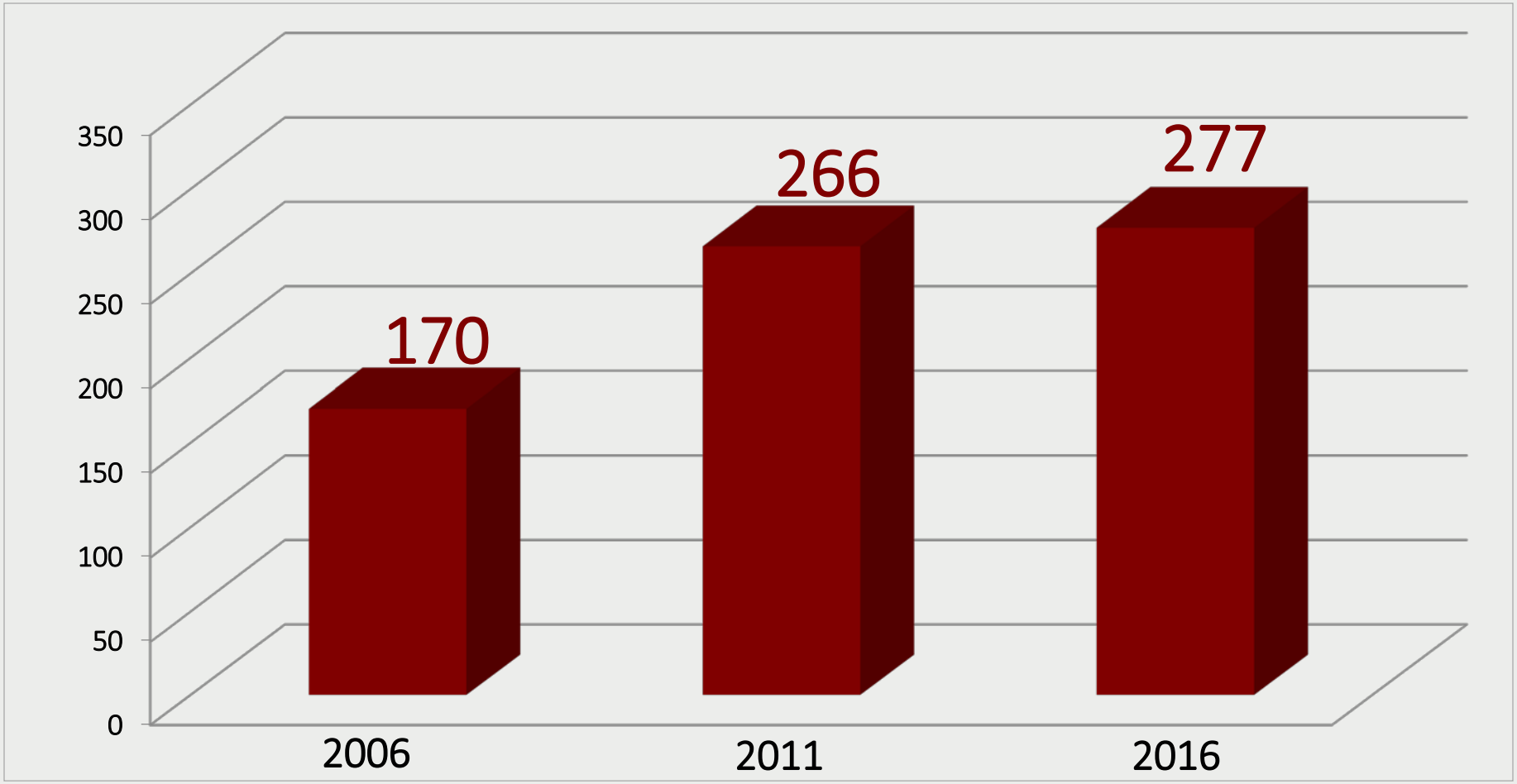
- accurate
- up to date

Information must be **protected**

- it must be protected from inadvertent disclosure and unauthorized access

Privacy Risks and Risk Mitigation

Total Privacy Complaints Opened Per Year



Privacy Breach

A privacy breach occurs when personal information is collected, retained, and used or disclosed in ways that are not in accordance with *MFIPPA*

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 electronic devices, such as laptop computers, digital cameras, or portable storage devices (USB sticks)
- unauthorized access (snooping, hacking)

Snooping into records

Harms caused by personal information snooping:

- discrimination, stigmatization, psychological or economic harm
- individuals withholding or falsifying information
- loss of trust or confidence in the public system
- cost and time in dealing with privacy breaches
- legal liabilities and proceedings

Sanctions for unauthorized access can include:

- investigation by privacy oversight bodies
- prosecution for offences
- statutory or common law actions
- discipline by employers
- discipline by regulatory bodies

What are PIAs

PIA refers to a process/approach for identifying and analyzing privacy risks when changing or developing programs or systems

A good PIA analysis provides senior management and program and system designers with sufficient information to reduce, mitigate or avoid different types of privacy risks

PIAs Benefits

ETHICAL: respond to FIPs and transparent PI handling practices.

RISK MITIGATION: Best tool to identify privacy risks, document countermeasures and implement mitigation strategies

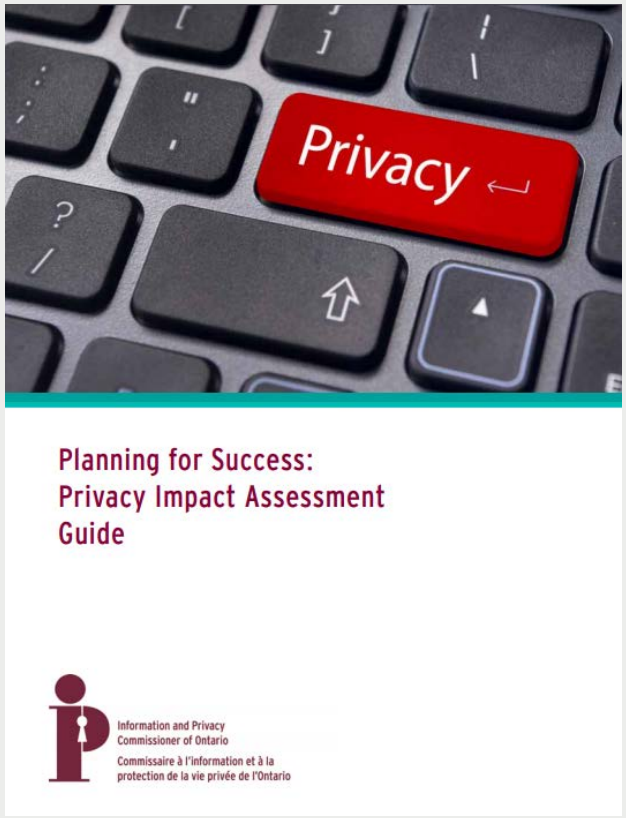
COMPLIANCE: directives, policies, legal, legislative requisites

SAVE TIME AND MONEY: avoid re-designs, delays, risk of project cancellation

PIA Guide

IPC PIA Guide (May 2015)

- tool to identify privacy effects, and mitigate risks, of any given project
- intended for *FIPPA* and *MFIPPA* institutions
- simplified 4-step methodology with tools
- basis for developing internal PIA policies and procedures



Reducing Risk of Privacy Breaches

1. Administrative

- privacy and security policies and procedures
- auditing compliance with rules
- privacy and security training
- data minimization ("need to know" limit)
- confidentiality agreements (alone or part of broader contracts)
- other means of communicating privacy messages (privacy notices, warning flags)
- privacy impact assessments

Reducing Risk of Privacy Breaches

2. Technical

- strong authentication and access roles
- detailed logging, auditing, monitoring
- strong password, encryption (devices, documents, email)
- patch and change management
- firewalls, hardened servers, intrusion detection and prevention, anti-virus anti-spam, anti-spyware
- protection against malicious and mobile code
- threat risk assessments, ethical hacks

Reducing Risk of Privacy Breaches

3. Physical

- controlled access to premises
- controlled access to locations within premises where identifying information is stored
- access cards and keys
- identification, screening, logging and supervision of visitors

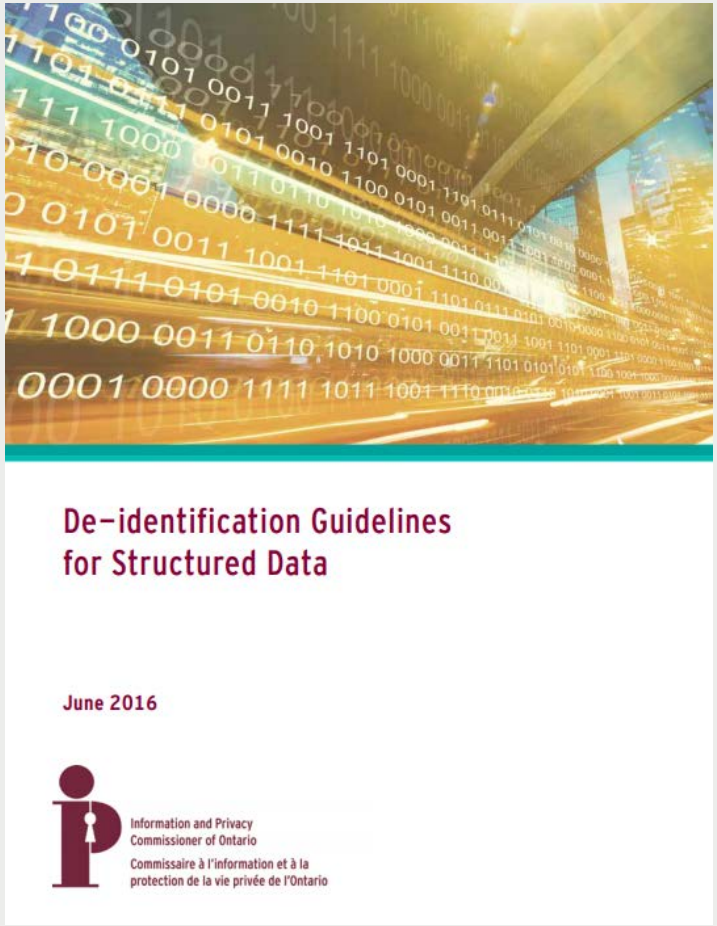
De-identification – Guidelines for Structured Data

De-identification is the process of removing personal information from a record or a data set

It is a risk based, step-by-step process to assist institutions in de-identifying data sets containing personal information

Key issues to consider when publishing data:

- release models
- types of identifiers
- re-identification attacks
- de-identification techniques



Responding to a Privacy Breach

STEP 1: IMMEDIATELY IMPLEMENT PRIVACY BREACH PROTOCOL

- Notify all relevant staff of the breach
- Develop and execute plan designed to contain the breach and notify those affected
- Recommend that you contact the IPC and provide our office with details of what happened

Responding to a Privacy Breach

STEP 2: STOP AND CONTAIN THE BREACH

- Identify the scope of the breach and take the necessary steps to contain it, including:
  - retrieve and secure any personal information that has been disclosed
  - ensure that no copies of the personal information have been made or retained by the individual who is not authorized to receive the information
  - determine whether the privacy breach would allow unauthorized access to any other personal information and take the necessary steps, such as changing passwords, identification numbers and/or temporarily shutting your system down

Responding to a Privacy Breach

STEP 3: NOTIFY THOSE AFFECTED BY THE BREACH

- You must take the necessary steps to notify those individuals whose privacy was breached at the first reasonable opportunity
- *MFIPPA* does not specify the manner in which notification must be carried out. There are numerous factors that may need to be taken into consideration when deciding on the best form of notification
- When notifying individuals affected by a breach:
  - provide details of the breach to affected individuals, including the extent of the breach and what personal information was involved
  - advise of the steps you are taking to address the breach and that they are entitled to make a complaint to the IPC. If you have reported the breach to the IPC, advise them of this fact
  - provide contact information for someone within your organization who can provide additional information and assistance.

Responding to a Privacy Breach

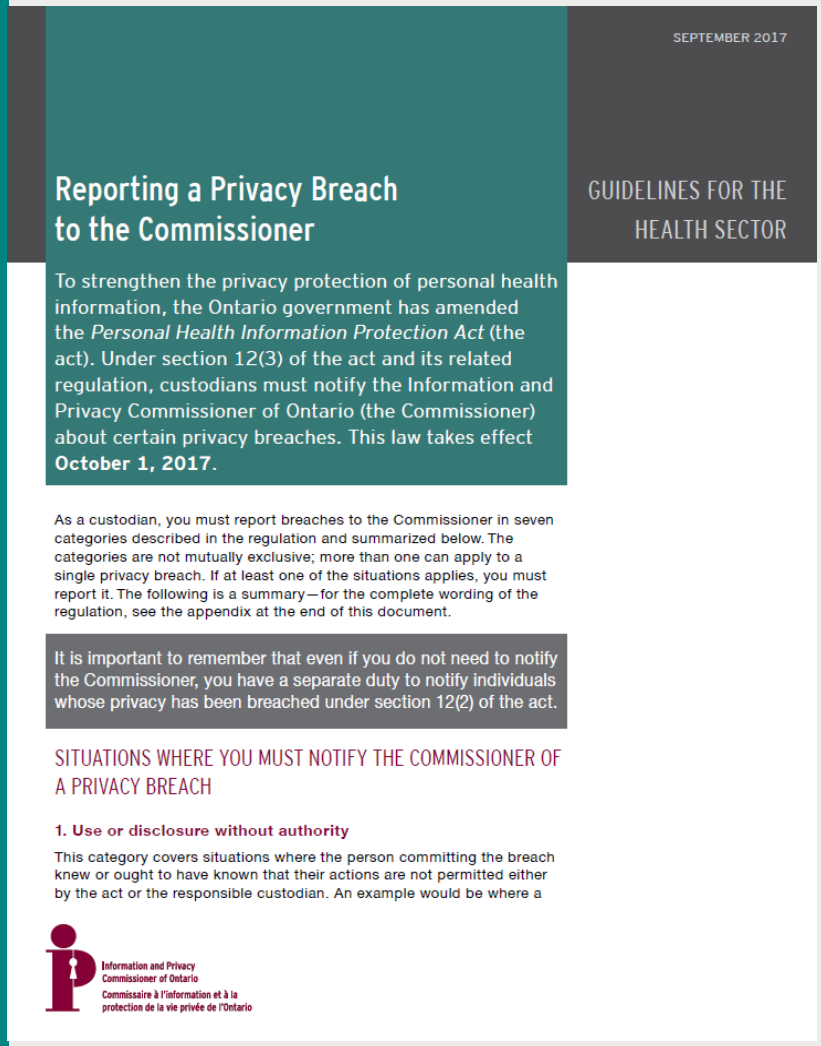
STEP 4: INVESTIGATION AND REMEDIATION

- You will be expected to conduct an internal investigation, including:
  - ensuring that the immediate requirements of containment and notification have been met
  - reviewing the circumstances surrounding the breach
  - reviewing the adequacy of your existing policies and procedures in protecting personal information
  - ensuring all staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of *MFIPPA*.

Reporting a Health Privacy Breach to the IPC

You must notify the IPC in cases of:

- unauthorized use or disclosure
- stolen information
- further use or disclosure after a breach
- pattern of similar breaches
- disciplinary action against a college or non-college member
- significant breach



SEPTEMBER 2017

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.

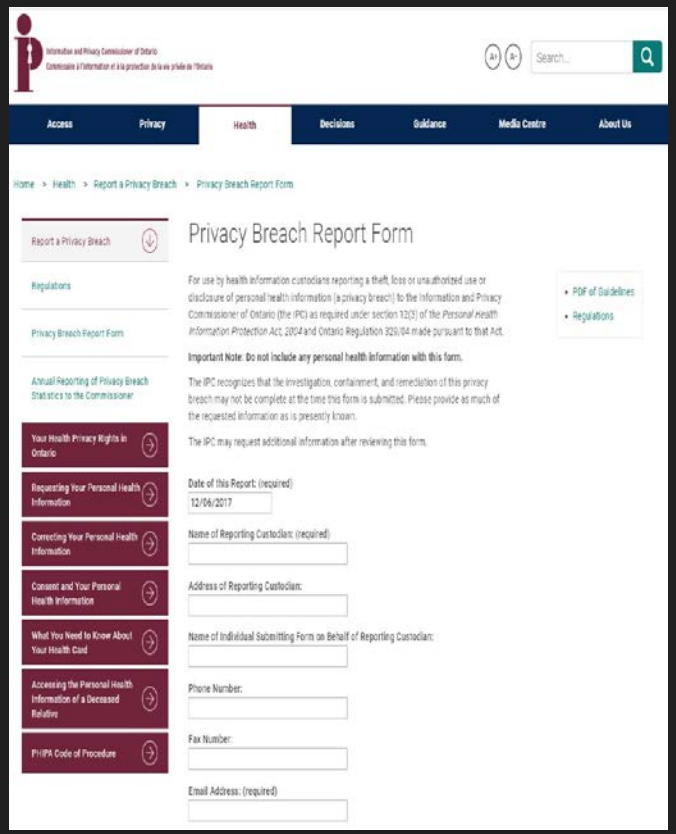
SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

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

Reporting a Health Privacy Breach to the IPC



Breaches can be reported online and by mail, fax or telephone

You will be asked to provide:

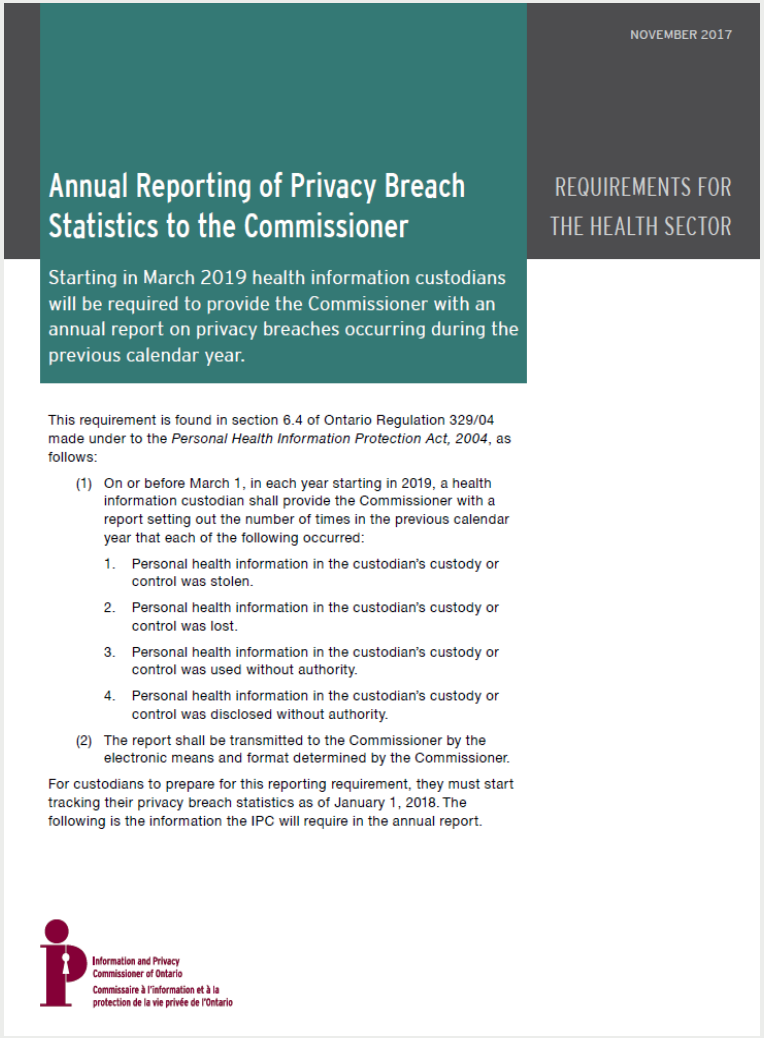
- a description of the breach
- steps taken to contain the breach
- steps taken to notify affected individuals
- steps taken to investigate or remediate

Health Information Custodians must provide breach statistics starting in 2019.

They must track incidents where personal health information is:

- stolen
- lost
- used without authority
- disclosed without authority

Begin tracking January 1, 2018



NOVEMBER 2017

Annual Reporting of Privacy Breach Statistics to the Commissioner

REQUIREMENTS FOR THE HEALTH SECTOR

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.

(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

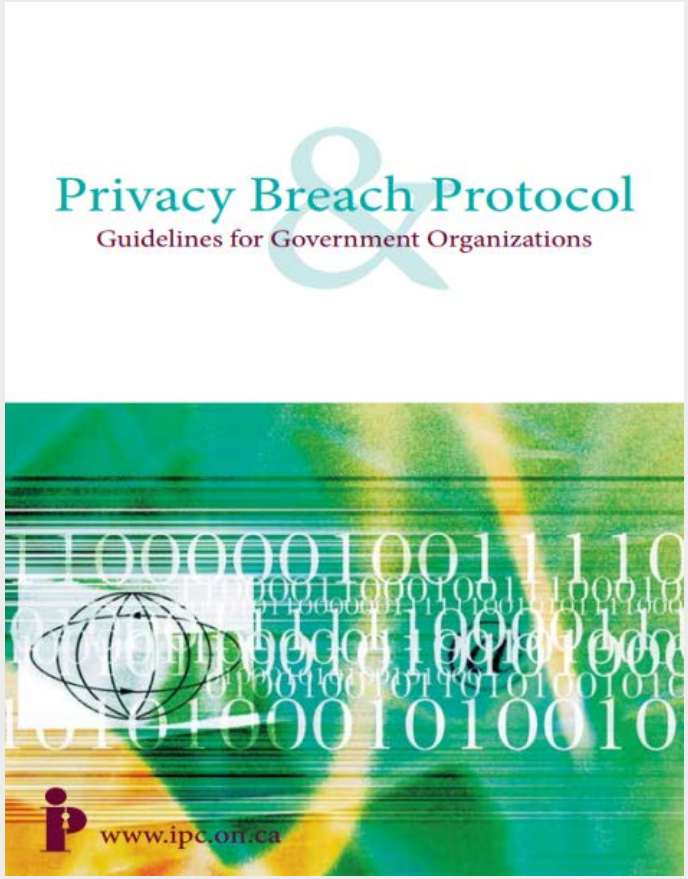
For custodians to prepare for this reporting requirement, they must start tracking their privacy breach statistics as of January 1, 2018. The following is the information the IPC will require in the annual report.

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

Privacy Breach Protocol Guide

Implementing a privacy breach protocol as a **best practice**, helps identify privacy risks, and potential and actual breaches

Guidance on what organizations should do when faced with a breach



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, the 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 investigation

Recent Privacy Investigations

Video Surveillance and Privacy (MC13-60)

In MC13-60, the complainant lived beside a public school and expressed concern with the use of video surveillance operated by the school board

IPC investigated and found that the board's collection of personal information through video surveillance within the school property was in accordance with section 28(2) of *MFIPPA*

IPC also found that the collection of personal information via video surveillance from outside the school's property was not in accordance with section 28(2) of *MFIPPA*

IPC's recommendations to the school board:

- to cease collection of personal information obtained by video surveillance systems from outside of the school property
- to revise its Notice of Collection in accordance with section 29(2) of *MFIPPA*
- to revise its policies, procedures, and guidelines to reflect the recommendations in the *Guidelines* and to provide clear and detailed information regarding the implementation and operation of video surveillance within its schools and provisions for periodic review of the continuing necessity for the video surveillance

Guidance for Video Surveillance

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

Technology Fact Sheet

Video Surveillance

November 2016

INTRODUCTION

This fact sheet provides institutions subject to the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act* (*FIPPA*, *MFIPPA* or the acts) with basic information about how to use video surveillance in a way that protects individual privacy. More detailed guidance can be found in the IPC's **Guidelines for the Use of Video Surveillance**.

DOES YOUR INSTITUTION HAVE THE AUTHORITY TO INSTALL A VIDEO SURVEILLANCE SYSTEM?

Institutions can collect personal information through the use of a video surveillance system if the collection is authorized under *MFIPPA* or *FIPPA*. Video surveillance may be authorized in cases where the system is used for the purposes of law enforcement, for example the use of temporary cameras by police for planned protests. It may also be authorized when necessary for the administration of your institution's lawful activities.

Video surveillance may be considered *necessary* if:

- the goals or purposes of the collection cannot be achieved by less privacy intrusive means, and
- the surveillance is more than merely helpful

For instance, circumstances may justify a school board's or a public transit authority's use of video surveillance to ensure safety on school property or on buses and subway systems.

ARE THERE LIMITS TO THE NUMBER AND PLACEMENT OF CAMERAS?

Yes. The video surveillance system should use as few cameras as possible. Cameras should be placed only in those locations where they are needed.

Guidelines for the Use of Video Surveillance

October 2015

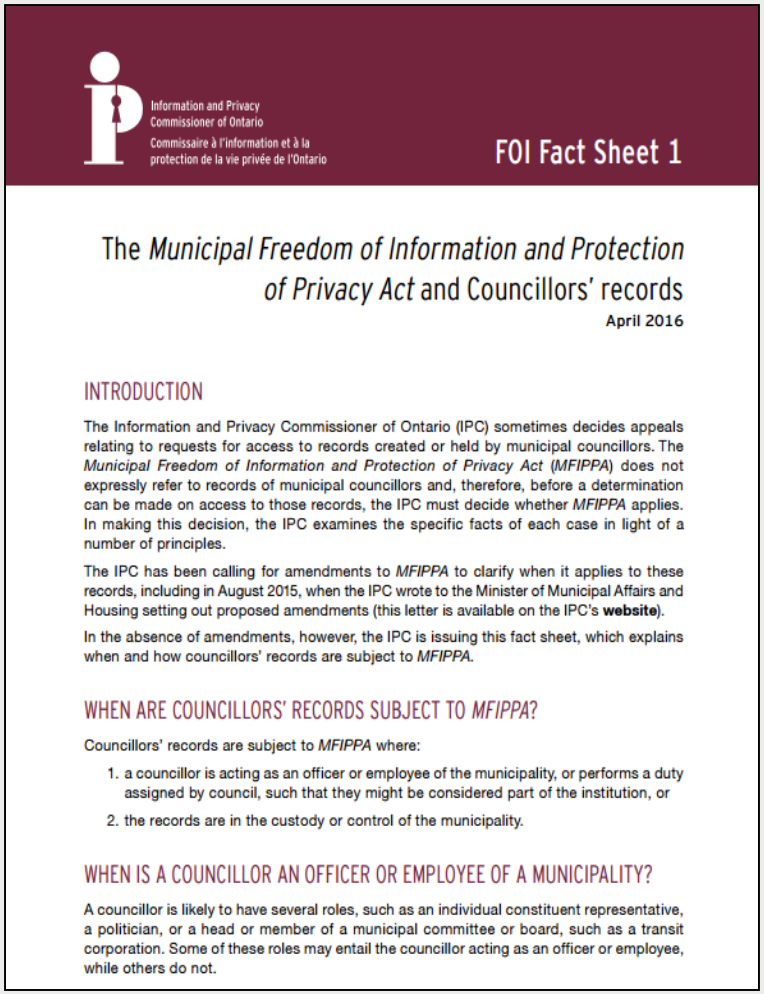
Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

IPC Resources

New IPC Fact Sheet Series

- Published to provide information in response to frequently asked questions about access to information, privacy and technology

- Series includes:
  - Councillors' Records
  - What is Personal Information?
  - Reasonable Search
  - Video Surveillance
  - Ransomware



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

FOI Fact Sheet 1

The *Municipal Freedom of Information and Protection of Privacy Act* and Councillors' records

April 2016

INTRODUCTION

The Information and Privacy Commissioner of Ontario (IPC) sometimes decides appeals relating to requests for access to records created or held by municipal councillors. The *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) does not expressly refer to records of municipal councillors and, therefore, before a determination can be made on access to those records, the IPC must decide whether *MFIPPA* applies. In making this decision, the IPC examines the specific facts of each case in light of a number of principles.

The IPC has been calling for amendments to *MFIPPA* to clarify when it applies to these records, including in August 2015, when the IPC wrote to the Minister of Municipal Affairs and Housing setting out proposed amendments (this letter is available on the IPC's **website**).

In the absence of amendments, however, the IPC is issuing this fact sheet, which explains when and how councillors' records are subject to *MFIPPA*.

WHEN ARE COUNCILLORS' RECORDS SUBJECT TO *MFIPPA*?

Councillors' records are subject to *MFIPPA* where:

1. a councillor is acting as an officer or employee of the municipality, or performs a duty assigned by council, such that they might be considered part of the institution, or
2. the records are in the custody or control of the municipality.

WHEN IS A COUNCILLOR AN OFFICER OR EMPLOYEE OF A MUNICIPALITY?

A councillor is likely to have several roles, such as an individual constituent representative, a politician, or a head or member of a municipal committee or board, such as a transit corporation. Some of these roles may entail the councillor acting as an officer or employee, while others do not.

IPC Webinars

- New series on timely, in-demand topics about access to information and privacy issues.
- First two presentations are now available at ipc.on.ca:
  - Situation Tables
  - Understanding Exemptions in *FIPPA* and *MFIPPA*

Questions?

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

Media: media@ipc.on.ca / 416-326-3965