PRIVACY

Privacy Breaches

Guidelines for Public Sector Organizations

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

TABLE OF CONTENTS

INTRODUCTION

Ontario's privacy laws set out the rules for how public sector organizations should manage and protect information about identifiable individuals – namely, personal information.[1]

This guide explains what to do in the event of a privacy breach. It can also help you develop your own privacy breach response plan.

Effective July 1, 2025, the *Freedom of Information and Protection of Privacy Act* (FIPPA) explicitly requires provincial institutions to report certain privacy breaches to the Information and Privacy Commissioner of Ontario (IPC) and notify affected individuals of those breaches, as soon as feasible after the institution determines that the breach occurred.

Be aware that different privacy laws in Ontario have different reporting and notification requirements.

- If you are an institution subject to Ontario's FIPPA, **this guidance applies to you**.
- If you are an institution subject to Ontario's *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), **you should also follow this guidance**. While MFIPPA has not been amended to expressly include the same breach-related requirements as FIPPA, following this guide will help you develop or strengthen your privacy breach response plans, support compliance with your other legal requirements, and ensure you are ready if similar amendments are made to MFIPPA.
- If you are dealing with a breach under Ontario's health privacy law, **this guidance does not apply to you**. Instead, refer to our guidance, ***Responding to a Health Privacy Breach: Guidelines for the Health Sector***.
- If you are dealing with a breach under Part X of the *Child, Youth and Family Services Act*, **this guide does not apply to you**. Instead, refer to page 28 of our guidance, ***Part X of the Child, Youth and Family Services Act: A Guide to Access and Privacy for Service Providers***.
- If you are dealing with a breach as a data integration unit designated under Part III.1 of FIPPA, **this guidance does not apply to you**. Instead, refer to the specific breach requirements under **FIPPA Part III.1** in addition to the steps set out in your practices and procedures.

Note: depending on what type of institution you are, you may have mandatory breach reporting obligations under other laws as well.

1 Please see the IPC's Interpretation Bulletin on "**personal information.**"

WHAT IS A PRIVACY BREACH?

A privacy breach occurs when personal information is collected, retained, used, disclosed, stolen, lost or disposed of in ways that do not comply with Ontario's privacy laws. FIPPA section 40.1 (1) generally refers to a breach of privacy safeguards as "a theft, loss or unauthorized use or disclosure of personal information."

The most common privacy breaches occur when unauthorized persons gain access to personal information. For example, personal information may be seized in a cyberattack, stolen (such as through theft of a portable electronic device) or accessed by an employee for improper purposes (for example, snooping).

RESPONDING TO A PRIVACY BREACH

When a privacy breach occurs, you should take immediate steps to respond to the breach.

All public sector institutions should have a documented privacy breach response plan or protocol in place. This will help ensure that the institution can respond effectively to breaches.

The breach response plan or protocol should clearly set out:

- **Who does what**. Specify key roles and responsibilities of certain designated management and staff on the breach response team. This may include information technology and security staff, the institution's FOI and privacy coordinator, legal services, communications, human resources, senior executives, and external experts, on an as-needed basis.
- **Who to contact and when**. Include current contact information for internal personnel who must be immediately notified, the order in which they should be contacted, and backups in the event of absence.
- **How to stay prepared**. Practice your plan or protocol periodically through simulated exercises to ensure everyone involved knows what to do in the event of a privacy breach and is prepared to act in a timely and coordinated manner.

The breach response steps outlined below are presented in a general chronological sequence; however, each breach is different. In some cases, your institution may determine that certain steps need to occur simultaneously, or in a different order, for the breach response to be effective.

1) ASSESS AND CONTAIN THE SCOPE OF BREACH

ASSESS

- Identify the scope of the breach, including what personal information is likely involved, the nature of the information, and how much personal information was potentially exposed.
- Assess how many people may have been affected by the breach and who they are.
- Identify which systems were or may have been compromised by the breach and when.
- While a full investigation will reveal further details over time, it's essential to conduct a preliminary assessment as soon as possible to determine the next steps, including whether notification and reporting are required.

CONTAIN

- Ensure that no personal information has been retained by an unauthorized recipient. If it has, contact the recipient to ensure the secure return or destruction of personal information, obtain documented assurance that no copies have been retained by them, and follow-up as needed.
- Prevent further unauthorized access to any other personal information by taking appropriate action, such as changing passwords and identification numbers or temporarily shutting down a system.
- In the case of unauthorized access by staff, consider suspending their access rights until a full investigation is complete.

2) ASSESS REAL RISK OF SIGNIFICANT HARM (RROSH)

Institutions are required to apply the real risk of significant harm (RROSH) threshold to determine when breaches **must** be reported to the IPC and whether individuals affected by the breach **must** be notified. Whether a privacy breach meets the RROSH threshold depends on a number of factors. Not all factors need to be satisfied before notification is required. Likewise, additional factors may be relevant to the particular facts of a breach scenario.

The factors relevant to determining whether a breach creates a real risk of significant harm to affected individuals include:

- the sensitivity of personal information involved
- the probability that the personal information has been, is being, or will be, misused
- the availability of steps the individual could take to reduce the risk of the harm occurring or mitigate the harm should it occur

Note that institutions must also consider any direction, recommendation or guidance provided by the IPC, and additional factors that may be prescribed in the future.

Assessing these factors will help you decide whether it is reasonable in the circumstances to believe that there is a real risk of significant harm to the affected individual(s) because of the breach. Under FIPPA, the definition of significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property.

2.1 SENSITIVITY OF PERSONAL INFORMATION

Is the personal information that was stolen, lost, or used or disclosed without authority sensitive?

Key things to determine	• What type(s) of personal information were impacted? • Could the compromise of this type of personal information cause significant harm to the individual (for example, identity theft, financial loss, humiliation, damage to reputation, etc.)?
Examples	• A breach of an individual's name and credit card number could result in identify theft and financial fraud. • A breach of professional or academic misconduct records could lead to reputational damage and negatively impact future employment opportunities.

Relevant considerations	• It is important to examine not only the nature of the personal information involved, but also the context and the circumstances of the breach.
	• In general, breaches of sensitive personal information are more likely to result in significant harm. Examples of personal information which could be sensitive include:
	  o health information
	  o government-issued identifiers (SIN, driver's licence number, passport number)
	  o financial information (credit card number, banking information, income records)
	• Along with health and financial information, certain types of information will generally be considered sensitive because of the specific risks to individuals when this information is collected, used, or disclosed. This may include information such as:
	  o ethnic and racial origins
	  o political opinions
	  o genetic and biometric data
	  o sex life or sexual orientation
	  o geolocation data
	  o religious/philosophical beliefs
	  o disciplinary records
	• The number of data elements involved in a breach can also affect sensitivity. There is a greater likelihood of significant harm to an individual when there are more data elements about the individual involved in the breach.
	  o For example, a first and last name may not be considered sensitive on their own, but when paired with birth date, home address, and financial information, the sensitivity of a name may increase because more is known about the individual. This could result in a risk of significant harm, including identity theft.
	• Consideration should also be given to whether the exposed data elements could be combined with other publicly available identifying information to cause significant harm.

	• Certain information may not initially seem sensitive, but the context and circumstances of the breach (to whom the information was exposed and how) may make the information much more sensitive. o For example, a person's name and address may be publicly available information in most cases, but for witnesses, informants or undercover agents, or for vulnerable individuals at risk of domestic abuse, releasing this type of information could put their safety and even their lives in danger (see below).

2.2 PROBABILITY OF MISUSE

What is the probability that the personal information that was stolen, lost, or used or disclosed without authority has been, is being, or will be misused?

Key things to determine	• What are the facts/circumstances of the breach? o What do you know about the person(s) who caused the breach or stole, received, used, or disclosed the breached information? Was there evidence of malicious intent? (ransomware, phishing, hacking, theft, snooping). o What is the relationship, if any, between the person(s) who caused the breach and/or stole, received, used, or disclosed the breached information and the individual(s) whose information was breached? • Do the facts/circumstances of the breach make it or more or less likely that the personal information will or could be used to cause significant harm to the affected individuals?
Relevant considerations	• Circumstances of the breach: o Was the breach intentional or accidental? o Who caused the breach or stole, received, used, or disclosed the breached information (or could have done so)? Are their identities known? What is their relationship to the affected individuals? o When did the breach first occur and for how long was the information exposed? o Was the information exposed to limited or known entities who have destroyed it and confirmed that they did not further disclose the information? o Has the personal information otherwise been recovered or securely destroyed? o Was the information adequately encrypted, de-identified, or otherwise not easily accessible?

	○ Is there evidence of malicious intent (for example, theft, hacking, malware, snooping)? ○ Is the breached information in the hands of an individual or entity that represents a safety or reputational risk to the individual(s) (for example, an ex-spouse)? ○ Is the information known to be exposed to entities or individuals who are likely to attempt to cause harm with it (for example, cybercriminals)? ○ Has the information been further used or disclosed for unauthorized or malicious purposes (for example, was the information published on the internet or dark web or is there a real threat that this may happen)? ○ Were potentially vulnerable individuals affected (for example, children or youth, individuals with disabilities, the elderly)? ○ Were multiple pieces of personal information breached, thus raising the risk of misuse? ○ Has harm already materialized for any affected individuals?

2.3 AVAILABILITY OF STEPS TO REDUCE RISK OR MITIGATE HARM

Could the individual take steps to reduce the risk of the harm occurring or mitigate the harm should it occur?

Key things to determine	• If the individuals were notified of the breach, could they take steps to reduce the risk of harm occurring or mitigate the harm should it occur? • If yes, this factor weighs in favour of notifying so that the affected individuals can take these steps.
Examples	• Changing passwords • Enrolling in credit monitoring • Notifying their bank • Monitoring their accounts for suspicious activity • Notifying relevant government offices that their ID was compromised • Preventing reputational harm by taking legal or other proactive means to mitigate such harm
Relevant considerations	• Would credit or other monitoring by the individual reduce the risk of harm or mitigate the harm? • Is the individual able to recover or prevent further use or disclosure of their personal information through legal or other means?

	• Could the individual change their passwords or other credentials to reduce the risk of harm or mitigate the harm? Conversely, have the individual's passwords or other credentials already been changed? • If the individual notified their family, colleagues, etc. of the breach, would it reduce the risk of harm or mitigate the harm (for example, by informing them of a compromised account sending messages)? • Could the individual take steps to reduce the risk of reputational damage or humiliation or mitigate this harm should it occur? • Are there any other steps the individual could take to reduce the risk of harm or mitigate harm?

3) NOTIFY THOSE AFFECTED BY THE BREACH

If it is reasonable in the circumstances to believe that the breach poses a real risk of significant harm to individuals whose personal information was affected by the breach, you **must** notify them as soon as feasible after you determine the breach occurred.

When evaluating the need to notify individuals, you should also consider:

- Legislative requirements: Whether you or your institution are subject to laws that either require or prohibit notification of affected individuals.
- Contractual obligations: Whether you or your institution have a contractual obligation to notify affected individuals in the case of a data loss or privacy breach.
- Third-party contractors: If the breach occurs at a third-party entity that you have contracted to store or process personal information on your behalf, you must ensure (contractually or otherwise), that they inform you of the breach immediately, since you, as the institution, have the primary responsibility for notifying affected individuals if there is a real risk of significant harm.

Where notifying individuals is otherwise prohibited by law, provincial institutions are not required to notify affected individuals of a breach but **are still required to report the breach to the IPC, as required under FIPPA**.

3.1 WHEN AND HOW TO NOTIFY AFFECTED INDIVIDUALS

Notification should occur as soon as feasible following a breach. If law enforcement is involved, advise them of your notification plans.

Direct notification to affected individuals

Direct notification, such as a telephone call, letter, email, or in person, is the preferred form of notice to individuals impacted by a privacy breach.

Indirect notification to affected individuals

Indirect notice to individuals may be used by an institution in specific situations, such as where one or more of these circumstances apply:

- You are unable to determine the identities of affected individuals despite taking reasonable steps to do so.
- There are questions as to the reliability or accuracy of contact information.
    - Note: Outdated contact information for a portion of the affected individuals does not mean that all the affected individuals should be notified indirectly. In cases involving a mix of outdated and current contact information, a hybrid approach to notification involving both direct and indirect elements may be appropriate.
- Direct notification would unreasonably and significantly interfere with the operations of your institution.
    - Note: All breach notification processes will involve the expenditure of time and resources. Indirect notice should only be considered when the time and resources required to provide direct notice would cause unreasonable and significant interference with your operations.
- Direct notification would be reasonably likely to be harmful or detrimental to the affected individuals, for example where it could cause emotional distress or result in risk to personal safety.
- The breach affects a significantly large number of individuals, making direct notification impractical.
    - Note: context should be considered to determine what constitutes a significantly large number of individuals, including the total number of individuals affected, the sensitivity, scope and impact.
- For voluntary notifications where RROSH has not been met, institutions may also consider indirect notification when the risk of harm to affected individuals has reasonably been determined to be low.

The indirect notice must be distributed in a way that could reasonably be expected to reach the affected individuals. Using multiple methods of public notification is generally most effective and considered a best practice. Examples may include:

- A prominent notice on your institution's website or a dedicated website containing details about the breach.
    - Ensure you take reasonable steps to bring the digital notice to the attention of affected individuals. Affected individuals may be unlikely to visit your website or breach notice unless specifically prompted to go there by media announcements, social media posts, or other means.
- Other public outreach activities to bring the notice to the attention of the affected individuals, such as:
    - posting notices or posters in high traffic areas of your facility for a length of time that will allow affected individuals to read the notice
    - placing notices in national or local newspapers
    - creating social media posts on relevant platforms
    - purchasing radio or TV announcements and advertising targeted to affected individuals
    - issuing news releases and community notices targeted to affected individuals
    - hosting town halls or webinars to provide information
    - any other case-specific public communication strategies that would be effective for reaching individuals affected by the breach

3.2 WHAT TO INCLUDE IN THE NOTIFICATION TO AFFECTED INDIVIDUALS

The information in the notice should be written in plain language and help affected individuals reduce or prevent any risk of significant harm that could be caused by the breach.

Direct and indirect notifications to affected individuals should include:

- the date of the notice
- a statement that the individual is entitled to **make a complaint to the IPC** and how they may do so (NOTE: this is mandatory under section 40.1 (4) of FIPPA if notice is being provided in accordance with that section)

- a statement that the complaint needs to be filed within one year (NOTE: this restriction only applies to FIPPA institutions if notice is being provided in accordance with section 40.1 (4) of FIPPA)
- mailing address for the IPC (2 Bloor Street East, Suite 1400 Toronto, ON, M4W 1A8)
- enough information about the breach to enable someone reading the notice to easily understand how they may have been impacted
- a description of the circumstances of the breach
- the cause of the breach, if known
- the date or period when the breach occurred
- the date when your institution became aware of the breach
- a description of the personal information affected by the breach, with as much detail as possible
- a description of how the personal information was affected by the breach (for example accessed, encrypted, exfiltrated, posted online, etc.)
- any risk of harm to affected individuals, if known
- steps your institution has taken to contain the breach and reduce and mitigate any risk of harm to affected individuals
- steps individuals can take to mitigate harm and protect themselves, if applicable, such as but not limited to:
    - contacting their bank, credit card company, and appropriate government departments to advise them of the breach
    - monitoring and verifying all bank account, credit card, and other financial transaction statements for any suspicious activity
    - obtaining a copy of their credit report from a credit reporting bureau
- a statement advising whether you have reported the matter to the IPC and other appropriate regulatory bodies, if applicable
- contact information for someone within the institution who can provide additional information and assistance, and answer questions

4) REPORT THE BREACH TO THE IPC

Where it is reasonable in the circumstances to believe that there is a real risk of significant harm resulting from a privacy breach, you must report the breach to the IPC as soon as feasible after determining the breach has occurred.

In situations where you will be notifying a large number of affected individuals about a breach, it is strongly recommended that you report the breach to the IPC first so our office can work with you to refine your proposed notification plan. This will avoid having to re-notify affected individuals using a different method or having to add missing information later.

When reporting privacy breaches to our office, please use the **report a privacy breach at your organization** form. Please ensure to include all information that is available at that point. Even if you do not have all the details yet, the earlier you notify our office the better. You can send us further information as more becomes known through the course of your investigation.

You should also consider whether other authorities or organizations should be informed of the breach.

Authority or organization	Purpose of contacting
Law enforcement	If theft or other crime or offence is suspected. For additional information, please see the IPC's ***Disclosure of Personal Information to Law Enforcement guide***.
Professional or regulatory bodies	In the context of a breach that relates to professional or regulatory standards overseen by a regulatory or professional body.
Technology suppliers	If the breach was due to a technical failure and a recall or technical fix is required.
Canadian Centre for Cyber Security	If there has been a cyber incident, including those that may involve a breach of personal information.

4.1 WHAT HAPPENS WHEN A BREACH IS REPORTED TO THE IPC?

When responding to a report or complaint of a privacy breach, or initiating our own investigation, the IPC may, among other things:

- assess whether the breach has been contained and affected individuals adequately notified
- interview individuals involved

- review and provide recommendations on your institution's policies and any other relevant documents
- require the production of information or records relevant to a review
- issue a report or decision after an investigation or review, which may include recommendations and orders
- in the context of a review under FIPPA:
    - issue an order to
        - discontinue an information practice
        - change an information practice
        - return, transfer, or destroy personal information
        - implement a different information practice
    - make a recommendation as to how an information practice could be improved
- in the context of an investigation under MFIPPA, make a recommendation and issue an order to:
    - cease a collection practice that contravenes MFIPPA
    - destroy collections of personal information that contravene MFIPPA

Institutions subject to a review or investigation have a duty to cooperate and assist the IPC.

5) INVESTIGATE

In general, an investigation, whether carried out internally or with the assistance of external forensic experts, should aim to determine what happened, why it happened, and how to prevent it from happening again. It should include:

- identifying and analyzing the events that led to the breach
- determining the source of the breach (internal or external) and its root cause
- determining key facts in relation to the breach and its impact on individuals and your institution
- determining whether the breach was an isolated incident or a systemic issue, and if the latter, reviewing your program-wide or institution-wide procedures

- examining the adequacy of your relevant security measures, such as your access privileges, system auditing capabilities, regular monitoring and implementation of software updates, etc.
- examining the adequacy of your relevant organizational privacy measures, such as existing policies and procedures, and the adequacy and frequency of your staff training programs relating to privacy and security
- in cases involving unauthorized access to electronic systems by a malicious actor, determining the series of actions taken by threat actor in your environment and the impact of the attack on records of personal information, typically through a forensic investigation and e-discovery analysis (for example, were records accessed, encrypted, or exfiltrated
- taking steps to investigate whether any stolen information was further used or disclosed without authority, such as posted on the dark web (for example, conducting dark web monitoring)
- in addition to assessing and evaluating the adequacy of security measures, reviewing the adequacy of the organization's information management practices in relation to the circumstances of the breach (including backup practices, information storage, and retention)
- confirming if retention schedules were followed for records containing personal information, and if the institution audits or reviews their implementation at least annually
- determining what (if any) contributing factors led to the breach or exacerbated it (for example, insufficient patch practices or the retention of records beyond the timelines established in retention schedules)
- maintaining a record of audit logs and any other information gathered during the investigation
- in cases involving real risk of significant harm, continuing to advise the IPC of your investigation findings as they become known
- cooperating with any investigation the IPC undertakes into the incident, including by answering our questions to the best of your knowledge and providing us with requested information in a timely manner

Please note that the facts gathered in an investigation must still generally be provided to the IPC, even if legal counsel is involved.

6) REDUCE THE RISK OF FUTURE PRIVACY BREACHES

Institutions are accountable for privacy breaches that involve personal information under their custody or control.

6.1 IMPLEMENT A PRIVACY MANAGEMENT PROGRAM

Regardless of the size of the institution, it is important to develop and maintain a privacy management program to protect personal information under the institution's custody or control from privacy breaches. An effective privacy management program includes:

- approval and support from the institution's senior leadership
- a designated privacy officer responsible for the development and implementation of the privacy program and its day-to-day operation
- clearly defined roles and responsibilities
- dedicated staff and funding resources appropriate to the volume and sensitivity of personal information under the institution's custody or control
- annual and up-to-date privacy and security training for all staff about Ontario's privacy laws and the institution's practices and procedures (see IPC guidance on **phishing** and **ransomware**)
- annual confidentiality undertakings for staff
- clear disciplinary measures for non-compliance
- good record keeping practices, including a framework to document what personal information is collected, used, retained, disclosed, secured and disposed of by your institution, and whose personal information it is
- a program to conduct privacy impact assessments to ensure privacy and security risks are identified and addressed before collecting personal information and updated before making any significant changes to the purpose for which personal information is used or disclosed
- robust information security practices and procedures, for example:
    - limiting access privileges
    - regularly monitoring software updates and retiring legacy systems
    - monitoring and auditing of systems containing personal information

- strong/multifactor authentication
- vulnerability management
- endpoint protection
- data backup and recovery
- encryption
- incident response planning
- completing threat risk assessments for new technologies

- processes to confirm alignment with record retention schedules to ensure personal information is not retained for longer than necessary
- regular auditing of employees' access to systems containing personal information
- privacy warning flags on electronic systems containing personal information
- strong procurement practices when outsourcing activities that involve personal information to third parties (see **IPC Guidance: Privacy and Access in Public Sector Contracting with Third Party Service Providers**)

6.2 REMEDIATE VULNERABILITIES

Privacy breaches typically uncover weaknesses in an institution's privacy management or security framework. It is critical that institutions promptly address these weaknesses and vulnerabilities as soon as possible following a breach incident. Remediation is a crucial process for preventing the recurrence of similar breaches by addressing the root causes of the breach. This involves reviewing the breach from a systemic perspective and may require a broader review of program or institution-wide procedures. The IPC will work actively with institutions to recommend remedial steps to strengthen their information practices and reduce the risk of privacy breaches recurring in the future.

In most cases, institutions follow these recommendations in the early resolution or investigation stages of our Tribunal dispute resolution process, and the matter is successfully resolved. In much rarer instances, these cases may proceed to adjudication, where the IPC may issue binding orders against institutions to act, modify or cease certain information practices.

RECORD KEEPING AND ANNUAL REPORTING

FIPPA institutions must maintain a record of the total number of privacy breaches that met the RROSH threshold and were reported to the IPC. These breaches must be provided to the IPC in an annual privacy breach report. For FIPPA institutions, annual privacy breach reports must be submitted to the IPC by **March 31** of the following year.

The annual report must include:

- the number and type of reported breaches and
- the number of individuals affected by each breach

For more information on tracking and submitting breach statistics, see ***Annual Reporting of Privacy Breach Statistics***.

MFIPPA does not include a similar requirement to submit privacy breach statistics to the IPC, however it is a best practice for all institutions to document and maintain records of their breaches, regardless of the need to report.

ADDITIONAL RESOURCES

The IPC has guidance that can assist your organization in meeting its privacy responsibilities and avoiding a privacy breach. You can find these documents in the guidance section of the IPC's website (**www.ipc.on.ca**).

About the IPC

The role of the Information and Privacy Commissioner is set out in five statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act, 2004*, *Part X of the Child, Youth and Family Services Act, 2017*, and the *Anti-Racism Act*.

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

www.ipc.on.ca
info@ipc.on.ca

September 2025