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

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

This guide explains what a privacy breach is and how to respond to one. It can also help you develop your own privacy breach response plan.

If you are an organization subject to Ontario's health privacy law, you should refer to our guidance, *Responding to a Health Privacy Breach: Guidelines for the Health Sector*.

WHAT IS A PRIVACY BREACH?

A privacy breach occurs when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws. 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 device) or accessed by an employee for improper purposes.

RESPONDING TO A PRIVACY BREACH

When a privacy breach occurs, you should do the following:

IMMEDIATELY ALERT APPROPRIATE PARTIES

Alert all relevant staff of the breach, including your freedom of information and privacy coordinator, and determine who else within your organization should be involved in addressing the breach.

CONTAIN THE BREACH

Identify the nature and scope of the breach and the action you need to take to contain it:

- determine what personal information is involved
- take corrective action, for example:
    - ensure that no personal information has been retained by an unauthorized recipient and get their contact information in case follow-up is required
    - ensure that the breach does not allow unauthorized access to any other personal information by taking appropriate action (for example, changing passwords or identification numbers, or temporarily shutting down a system)
    - in a case of unauthorized access by staff, consider suspending their access rights
    - retrieve hard copies of any personal information that has been disclosed

NOTIFY THOSE AFFECTED BY THE BREACH

You should notify those affected as soon as reasonably possible if you determine that the breach poses a real risk of significant harm to the individual, taking into consideration the sensitivity of the information and whether it is likely to be misused. If law enforcement is involved, ensure that notification will not interfere with any investigations.

Notification should be direct, such as by telephone, letter, email or in person. Indirect notification can be used in situations where direct notification is not possible or reasonably practical, for instance, when contact information is unknown or the breach affects a large number of people.

Notification to affected individuals should include:

- details of the extent of the breach and the specifics of the personal information that was compromised
- the steps taken and planned to address the breach, both immediate and long-term

- a suggestion, if financial information or information from government-issued documents is involved, to:
    - contact their bank, credit card company, and appropriate government departments to advise them of the breach
    - monitor and verify all bank account, credit card and other financial transaction statements for any suspicious activity
    - obtain a copy of their credit report from a credit reporting bureau
- contact information for someone within your organization who can provide additional information and assistance, and answer questions
- a statement that they have a right to make a complaint to the IPC and how to do so

INVESTIGATE

- Identify and analyze the events that led to the breach
- Review your policies and practices in protecting personal information, privacy breach response plans and staff training to determine whether changes are needed
- Determine whether the breach was a result of a systemic issue and if so, review your program-wide or institution-wide procedures
- Take corrective action to prevent similar breaches in the future and ensure your staff are adequately trained
- If you have contacted the IPC, advise us of your findings and remedial measures, and cooperate with any further investigation we undertake into the incident

NOTIFYING THE IPC

You should notify the IPC of significant breaches, such as those that may involve sensitive personal information or large numbers of individuals, or when you are having difficulties containing the breach. In these situations, you should notify the IPC as soon as reasonably possible.

In situations where you will be notifying a large number of individuals, it is important to contact the IPC before you begin the notification process, so that we are prepared to respond to inquiries.

The IPC can assist you with your breach response plan.

WHAT HAPPENS WHEN THE IPC INVESTIGATES?

When responding to a report or complaint of a privacy breach, or initiating our own investigation, we may:

- assess whether the breach has been contained and affected individuals adequately notified
- interview individuals involved
- review and provide advice on your organization's policies and any other relevant documents
- issue a report after the investigation, which may include recommendations
- issue an order

The purpose of the IPC investigation is future-oriented — that is, if there was a privacy breach, the IPC will assist the institution in taking steps to prevent similar occurrences.

HOW TO REDUCE THE RISK OF FUTURE PRIVACY BREACHES

You should consider the following measures to prevent privacy breaches:

- educate your staff about Ontario's privacy laws and your organization's policies and practices governing the collection, retention, use, security, disclosure and disposal of personal information
- conduct privacy impact assessments before introducing or changing technologies, information systems, and processes to ensure privacy risks are identified and addressed
- seek input from appropriate parties such as your legal counsel and security units, your freedom of information and privacy coordinator, the Ontario ministry responsible for information and privacy matters, and our office, as necessary

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 the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, and the *Personal Health In-formation Protection Act*. The commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day.

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 2019