CHILD, YOUTH, AND FAMILY SERVICES

Reporting a Privacy Breach to the Information and Privacy Commissioner

Guidelines for Service Providers

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

If you are a service provider under Part X of the *Child, Youth and Family Services Act* and you experience a privacy breach, you may be required to notify the Information and Privacy Commissioner.

Under Ontario's child and family services law, service providers are required to protect personal information in their custody or control against theft, loss, and unauthorized use or disclosure. If a privacy breach does occur, the service provider must notify any affected individual at the first reasonable opportunity.

Service providers are also required to notify the IPC, and the Minister of Children, Community and Social Services, but only if the breach falls into certain categories. These categories are set out in the legislation. You can find the complete wording in the appendix of this document.

SITUATIONS WHERE YOU MUST NOTIFY THE IPC OF A PRIVACY BREACH

Categories of breaches are not mutually exclusive; more than one can apply to a single incident. If at least one applies, you must report the breach to the IPC.

1. USE OR DISCLOSURE WITHOUT AUTHORITY

This category covers situations where the person committing the breach **knew** or should have known that the use or disclosure was not permitted. This person could be your employee, a volunteer, a consultant, or even someone with no relationship to you.

For example, an employee intentionally reads the personal records of their neighbour, a friend's child, or a local celebrity for a non work-related purpose. This is called "snooping." Whether done maliciously, or out of curiosity or even concern, snooping is a type of unauthorized use of personal information that you must report to the IPC.

By contrast, you generally do not need to notify the IPC if a breach is **accidental**; for example, when an employee accidentally views the wrong client record or inadvertently emails information to the wrong person. However, you must report even accidental privacy breaches if they fall into one of the other categories below.

2. STOLEN INFORMATION

If you believe personal information was stolen, you must notify the IPC. A typical example is a situation in which someone has stolen paper records, or a laptop or other electronic device. Another example is where client information is subject to a ransomware or other malware attack. However, if the information was de-identified or encrypted, you do not need to notify the IPC.

3. FURTHER USE OR DISCLOSURE WITHOUT AUTHORITY AFTER A BREACH

Following an initial privacy breach, you may become aware that the information was or will be **further** used or disclosed without authority. If so, you must report it to the IPC.

For example, your employee inadvertently sends a letter containing client information to the wrong person. Although the person returned the letter to you, you learn that he kept a copy and is threatening to make the information public. Even if you did not report the initial, accidental breach, you must notify the IPC of this situation. Another example is where an employee wrongfully accesses a client's file and then discloses their personal information on social media.

4. PATTERN OF SIMILAR BREACHES

Even if a privacy breach is accidental or insignificant, it must be reported to the IPC if it is part of a pattern of similar breaches. Such a pattern may reflect systemic issues that you need to address, such as inadequate training or procedures.

For example, you discover that correspondence to a client inadvertently included information relating to a different client. Over a few months, the same mistake is repeated several times

because an automated process has been malfunctioning. You should report this to the IPC.

Use your judgment in deciding if a privacy breach is an isolated incident or part of a pattern. Consider, for instance, the time between the breaches and their similarities. Keeping track of privacy breaches in a standard format will help you identify patterns.

5. BREACH BY PRESCRIBED ENTITY

Under the *CYFSA*, service providers may disclose personal information to certain prescribed entities for analysis related to planning, managing, and evaluating services. The Canadian Institute for Health Information and the Institute for Clinical Evaluative Sciences are currently prescribed. Service providers may also disclose information, for the same purposes, to Indigenous persons or entities that are not prescribed, if certain conditions are met. For more information, see *CYFSA* Regulation 191/18.

If you learn that personal information you disclosed to a prescribed or non-prescribed person or entity has been stolen, lost, or used or disclosed without authority, you must report it to the IPC.

As the service provider who disclosed the information, it is **your** responsibility to report the breach to the IPC, even if it was caused by the entity and not by any actions on your part. For example, if a prescribed entity notifies you that their employee lost some of the records you disclosed to them for statistical analysis, you must notify the IPC.

6. DISCIPLINARY ACTION AGAINST AN EMPLOYEE, OR RELATED RESIGNATION

You must report any breach to the IPC that leads to the termination, suspension, or discipline of an employee whose actions resulted in the breach. Similarly, if an employee resigns and you believe their resignation is related to a breach, you must report it to the IPC.

For example, one of your intake workers reveals on social media that a well-known individual is receiving services from your

organization. You formally discipline the employee by placing a written reprimand in their personnel file. Or an employee resigns, and you suspect the resignation relates to your investigation into their unauthorized use of client information. You should report these breaches to the IPC.

7. SIGNIFICANT BREACH

Even if none of the previous six circumstances apply, you must notify the IPC if the privacy breach is significant. To decide whether a breach is significant, you must consider all the relevant circumstances, including whether:

- the information is sensitive
- the breach involves a large volume of information
- the breach involves many individuals' information
- more than one service provider was involved in the breach

For example, an employee accidentally sends an email intended for one particular supervisor to your whole organization. The email contains a large volume of sensitive information about a child in care. Or, you post information on your website about the progress made by families in your programs. It comes to your attention that while you did not use any names, others can easily identify some of the families described. This breach involves many clients, whose information has potentially been made widely available. You should report these types of breaches to the IPC. Note that even breaches that cause no particular harm may still be significant.

HOW TO REPORT A BREACH TO THE IPC

Submit your breach report online at **www.ipc.on.ca**, as soon as reasonably practical.

You will need to describe:

- the circumstances of the breach (for example, how the personal information came to be stolen, lost, or disclosed without authority, how many individuals were affected, how the breach was discovered)

- whether and how you notified the affected individuals
- the nature of the personal information that was stolen, lost, or used or disclosed without authority
- the steps you took to contain, investigate, and remediate the breach and prevent future breaches (some of this work may still be ongoing)

The IPC will review the information you provide and may request additional information. In some cases, the IPC may decide to conduct an investigation. In other cases, the IPC will take no further action, such as when it is satisfied that the breach is contained, and you have addressed its cause and taken steps to prevent further breaches.

ANNUAL STATISTICS

The *CYFSA* requires that service providers submit annual statistics on the number of privacy breaches each year, including all thefts, losses, or unauthorized uses or disclosures of personal information.

This count includes privacy breaches that did not meet the threshold for reporting to the IPC. An accidental privacy breach that is isolated and limited in scope, such as misdirected correspondence, may not have been reported to the IPC when it happened, but should still be counted for annual statistical reporting. For more information about submitting annual statistics, see *Guidelines for Submitting Statistics to the IPC*, at **www.ipc.on.ca**.

Service providers should have a system in place to record all privacy breaches. This helps to track ongoing issues, patterns and changes, and will help you meet your annual statistics reporting obligations.

APPENDIX

CHILD, YOUTH AND FAMILY SERVICES ACT, SECTION 308

(1) A service provider shall take reasonable steps to ensure that personal information that has been collected for the purpose of providing a service and that is in the service provider's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

(2) Subject to any prescribed exceptions and additional requirements, if personal information that has been collected for the purpose of providing a service and that is in a service provider's custody or control is stolen or lost or if it is used or disclosed without authority, the service provider shall,

a) notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or unauthorized use or disclosure; and

b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under section 316.

(3) If the circumstances surrounding the theft, loss or unauthorized use or disclosure meet the prescribed requirements, the service provider shall notify the Commissioner and the Minister of the theft, loss or unauthorized use or disclosure.

ONTARIO REGULATION 191/18 UNDER THE *CYFSA*, SECTION 9:

Each of the following circumstances is prescribed for the purposes of subsection 308 (3) of the Act:

1. The service provider has reasonable grounds to believe that the personal information was used or disclosed without authority by a person who knew or ought to have known that the person was using or disclosing the information without authority.
2. The service provider has reasonable grounds to believe that the personal information was stolen.

3. The service provider has reasonable grounds to believe that the personal information that was stolen or lost or used or disclosed without authority was or will be further used or disclosed without authority.
4. The loss or unauthorized use or disclosure of the personal information is part of a pattern of similar losses or unauthorized uses or disclosures of personal information in the custody or control of the service provider.
5. The service provider has reasonable grounds to believe that personal information that the service provider disclosed, to a prescribed entity or a person or entity that is not a prescribed entity under subsection 293 (1), (2) or (3) of the Act, has been stolen or lost or used or disclosed without authority by the prescribed entity or the person or entity that is not a prescribed entity.
6. An employee of the service provider is terminated, suspended or disciplined as the result of the theft, loss or unauthorized use or disclosure of personal information by the employee.
7. An employee of the service provider resigns and the service provider has reasonable grounds to believe that the resignation is related to an investigation or other action by the service provider with respect to the theft, loss or unauthorized use or disclosure of personal information by the employee.
8. The service provider determines that the loss or unauthorized use or disclosure of the personal information is significant after considering all relevant circumstances, including,
    i. the sensitivity of the personal information that was lost or used or disclosed without authority,
    ii. the volume of the personal information that was lost or used or disclosed without authority,
    iii. the number of persons whose personal information was lost or used or disclosed without authority, and
    iv. whether one or more service providers were involved in the loss or unauthorized use or disclosure of the personal information.

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 at **www.ipc.on.ca**.

About the IPC

The Information and Privacy Commissioner of Ontario is appointed by the Legislative Assembly of Ontario and is independent of the government of the day. The IPC's mandate includes resolving access to information appeals and privacy complaints, educating the public about access and privacy issues, reviewing information practices and commenting on proposed legislation, programs, and practices.

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

October 2019