MARCH 2021

GUIDELINES FOR THE HEALTH SECTOR

Reporting a Privacy Breach to the IPC

If you are a health information custodian under Ontario's health privacy law, the *Personal Health Information Protection Act* (*PHIPA*) and you experience a privacy breach, you may be required to notify the Information and Privacy Commissioner of Ontario (IPC). This guidance explains what types of breaches must be reported to the IPC.

Custodians are only required to notify the IPC if the breach falls into the categories explained below.[1]

The categories are not mutually exclusive; more than one can apply to a single incident. You must report the breach to the IPC at the first reasonable opportunity if at least one of the situations applies. These categories are set out in the regulation, and you can find the complete wording in the appendix of this document..

It's important to remember that even if you don't need to report the breach to the IPC, you have a duty to notify individuals whose privacy has been breached. You must also count every breach in your annual statistics report to the IPC.

1 A coroner to whom Ontario Health provides personal health information under subsection 55.9.1 (1) of *PHIPA* must, with respect to that information, comply with a number of obligations as if the coroner were a custodian, including the obligation to notify the IPC of the breaches described here.

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

SITUATIONS WHERE YOU MUST NOTIFY THE IPC

1. Use or disclosure without authority

There may be situations where you or another person uses or discloses personal health information in your custody or control without authority. You must report such breaches to the IPC where the person committing the breach either knew or should have known that their actions were not permitted under the law. That person could be your employee, a health care practitioner with privileges, a third party (such as a service provider), or even someone with no relationship to you.

One example is where an employee looks at the personal health information of their neighbour, a friend's child, or a 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 information. Regardless of the motive, you must report this type of breach to the IPC.

By contrast, you generally do not need to notify the IPC when the breach is accidental, for example, if information is inadvertently sent by email or courier to the wrong person, or a letter is placed in the wrong envelope. Also, you do not need to notify the IPC when a person who is permitted to access patient information accidentally accesses the wrong patient record. 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 health information was stolen you must report it to the IPC.

A typical example would be where someone has stolen paper records, a laptop, a USB drive, or other electronic device. Another example would be where personal health information is subject to a ransomware or other malware attack. You must report these types of breaches to the IPC.

You do not need to notify the IPC if the stolen information was de-identified or encrypted.

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 this is the case, you must report it to the IPC.

For example, an employee accidentally sends a letter containing a patient's personal health information to the wrong person. Although the person returned the letter to you, you learn that they kept a copy and are threatening to make the information public. Even if you did not report the initial incident, you must notify the IPC of this situation.

Another example is where you learn an employee wrongfully accessed a patient's personal health information and subsequently used this information to market products or services or to commit fraud (for example, health care or insurance fraud). You would also need to report this breach.

4. Pattern of similar breaches

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

For example, you discover that a letter to a patient inadvertently included information relating to a different patient. Over a few months, the same mistake is repeated several times because an automated process for generating letters has been malfunctioning for some time. 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 uniform way can help you identify patterns.

5. Disciplinary action against a college member

If you are required to report an employee or another agent to a health regulatory college because of a breach, you must also report the breach to the IPC.

Where the agent is a member of a college, you must notify the IPC of a privacy breach if:

- you terminate, suspend or discipline them as a result of the breach
- they resign, and you believe this action is related to the breach

Where a health care practitioner with privileges or otherwise affiliated with you is a member of a college, you must notify the IPC of a privacy breach if:

- you revoke, suspend or restrict their privileges or affiliation as a result of the breach
- they give up or voluntarily restrict their privileges or affiliation with you, and you believe this action is related to the breach

For example, a doctor reveals on social media that a well-known individual is receiving services from your hospital. You formally discipline the doctor by placing a written reprimand in their personnel file. Or, an employee resigns, and you suspect the resignation relates to their recent breach of patient privacy. You should report these breaches to the IPC.

Similar requirements apply to health care practitioners who are employed to provide health care for a board of health.

6. Disciplinary action against a non-college member

Not all agents of a custodian are members of a college. If an agent is not a member, you must still notify the IPC in the same circumstances that would have triggered notification to a college.

For example, a registration clerk has an unpleasant encounter with a patient and posts information about the patient on social media. You suspend the clerk for a month. Although the clerk is not a member of a college, you must still report this privacy breach.

7. Significant breach

Even if none of the above 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 custodian or agent was responsible for the breach

For example, you are a health care practitioner and you accidentally disclose a patient's mental health assessment to other practitioners through a group email, rather than to just the patient's physician. This information is highly sensitive and you disclosed it to a number of persons to whom you did not intend to send the information. Or, you post detailed information on a website about a group of patients receiving specialized treatment for an unusual health issue. It comes to your attention that while you did not use any patients' names, others can easily identify them. This breach involves many patients, 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. For example, the recipients of a misdirected group email that contains a patient's mental health assessment may, upon realizing the mistake, delete the email and successfully contain the breach. Containing the breach might minimize or eliminate the potential for harm to the patient, but the breach may still be significant in that it reveals an underlying problem in your information policies and practices.

UNAUTHORIZED COLLECTION BY MEANS OF THE EHR

Custodians may collect, use, and disclose personal health information by means of the electronic health record (EHR) according to the rules set out in Part V.1 of *PHIPA*.

In the EHR context, custodians must comply with the breach notification requirements set out elsewhere in *PHIPA*, as well as an additional

requirement: if personal health information is collected without authority by means of the EHR, the custodian responsible for the collection must, in certain circumstances, notify the IPC. That is, if the unauthorized collection by means of the EHR had been a use or disclosure under any of the seven circumstances described in this document, the custodian must notify the IPC at the first reasonable opportunity.

For example, one of the circumstances described in this document is that the use or disclosure is part of a pattern. This means that the custodian must notify the IPC if an unauthorized collection by means of the EHR is part of a pattern.

HOW TO REPORT A BREACH TO THE IPC

You must submit the report at the first reasonable opportunity, either by mail or online at **www.ipc.on.ca**.

You will need to describe:

- the circumstances of the breach (for example, how the 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 health information that was stolen, lost, used or disclosed without authority, or collected by means of the EHR without authority
- the steps you took to contain, investigate, and remediate the breach and prevent future breaches (with the understanding 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, while in other cases no further action will be taken.

ANNUAL STATISTICS

PHIPA requires custodians to submit statistics on the number of privacy breaches each year, including all thefts, losses, unauthorized uses or disclosures, or unauthorized collections by means of the EHR of personal health information.[2]

Note that these statistics include privacy breaches that did not meet the threshold for reporting the breach to the IPC. An accidental privacy breach that is isolated and limited in scope — misdirected correspondence, for example — may not have been reported to the IPC when it happened, but should still be counted for annual statistical

2 A coroner to whom Ontario Health provides personal health information under subsection 55.9.1 (1) of *PHIPA* must, in respect of that information, comply with this annual statistics requirement, with any necessary modification, as if the coroner were a custodian.

reporting. For more information about submitting annual statistics, please see **Annual Reporting of Privacy Breach Statistics to the Commissioner** available on the IPC's website.

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

APPENDIX

Excerpts from Ontario Regulation 329/04 under *PHIPA*

Section 6.3

(1) The following are the circumstances in which a health information custodian is required to notify the Commissioner for the purposes of subsection 12 (3) of the Act:

1. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority.
2. The health information custodian has reasonable grounds to believe that personal health information in the custodian's custody or control was stolen.
3. The health information custodian has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in the custodian's custody or control, the personal health information was or will be further used or disclosed without authority.
4. The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information in the custody or control of the health information custodian.
5. The health information custodian is required to give notice to a College of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.
6. The health information custodian would be required to give notice to a College, if an agent of the health information custodian were a member of the College, of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.
7. The health information custodian determines that the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances, including the following:
    i. Whether the personal health information that was lost or used or disclosed without authority is sensitive.
    ii. Whether the loss or unauthorized use or disclosure involved a large volume of personal health information.
    iii. Whether the loss or unauthorized use or disclosure involved many individuals' personal health information.

iv. Whether more than one health information custodian or agent was responsible for the loss or unauthorized use or disclosure of the personal health information.

(2) In this section,

"College" means a College as defined in subsection 17.1 (1) of the Act.

(3) A health information custodian shall notify the Commissioner of the existence of a circumstance set out in subsection (1) at the first reasonable opportunity.

Section 18.3

(1) A health information custodian is required to notify the Commissioner for the purposes of clause 55.5 (7) (b) of the Act under any circumstance where the custodian would be required to notify the Commissioner if the collection by means of the electronic health record had been for a use or disclosure to which section 6.3 of this Regulation applied.

(2) The health information custodian shall inform the Commissioner of an unauthorized collection to which subsection (1) applies at the first reasonable opportunity.

Subsection 18.10 (4)

If personal health information about an individual is collected without authority by a coroner by means of the electronic health record, the coroner shall,

…

(b) notify the Commissioner of the unauthorized collection at the first reasonable opportunity, if any circumstance exists where the coroner would be required to notify the Commissioner if the coroner were a custodian to which subsection 18.3 (1) of this Regulation applied.