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

person looks at an ex-spouse's medical history for no work related purpose—the "snooping" case. 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.

This includes situations where the unauthorized use or disclosure is not done for a personal or malicious motive. For example, it might include where employees of a hospital are curious about why a local celebrity or a co-worker was treated at the hospital, and access that individual's medical records.

You generally do not need to notify the Commissioner when the breach is accidental, for example, when 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 Commissioner when a person who is permitted to access patient information accidentally accesses the wrong patient record. However, even accidental privacy breaches must be reported if they fall into one of the other categories below.

2. Stolen information

A typical example of this would be where someone has stolen paper records, or a laptop or other electronic device. Another example would be where patient information is subject to a ransomware or other malware attack, or where the information has been seized through use of a portable storage device. You should report cases like these to the Commissioner.

You do not need to notify the Commissioner if the stolen information was de-identified or properly 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; you must report this to the Commissioner.

For example, your employee inadvertently sends a fax containing patient information to the wrong person. Although the person returned the fax 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 incident, you must notify the Commissioner of this situation.

Other examples include where you learn that an employee wrongfully accessed patient information and subsequently used this information to market products or services or to commit fraud (e.g., health care or insurance fraud).

4. Pattern of similar breaches

Even if a privacy breach is accidental or insignificant by itself, it must be reported to the Commissioner 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.

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

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. This should be reported to the Commissioner.

5. Disciplinary action against a college member

A duty to report an employee or other agent to a health regulatory college also triggers a duty to notify the Commissioner.

Where an *employee* is a member of a college, you must notify the Commissioner 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 Commissioner of a privacy breach if:

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

Similar requirements apply to *health care practitioners employed by a board of health*.

6. Disciplinary action against a non-college member

Not all employees or other agents of a custodian are members of a college. If an agent is not such a member, you must still notify the Commissioner in the same circumstances that would have triggered notification to a college, had the agent been a member.

For example, one of your registration clerks 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 report this privacy breach.

7. Significant breach

Even if none of the above six circumstances apply, you must notify the Commissioner if the privacy breach is significant. In deciding whether a breach is significant, you must consider all the relevant circumstances, including whether

i. the information is sensitive

ii. the breach involves a large volume of information

iii. the breach involves many individuals' information

iv. more than one custodian or agent was responsible for the breach

For example, you are a health care practitioner who accidentally discloses a patient's mental health assessment to other practitioners on a group email distribution list, rather than to just the patient's physician. This information is highly sensitive and has been disclosed 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 a novel 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. These types of breaches should be reported to the Commissioner. Note that even breaches that cause no particular harm may still be significant.

ANNUAL REPORT TO THE COMMISSIONER

Custodians will be required to start tracking privacy breach statistics as of January 1, 2018, and will be required to provide the Commissioner with an annual report of the previous calendar year's statistics, starting in March 2019.

The Commissioner will release detailed guidance on this statistical reporting requirement in fall 2017.

APPENDIX

Ontario Regulation 329/04 under the *Personal Health Information Protection Act*, 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 section 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.

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