HEALTH

OCTOBER 2018

Responding to a Health Privacy Breach: Guidelines for the Health Sector

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

CONTENTS

WHAT TO DO WHEN A PRIVACY BREACH OCCURS 1

- STEP 1: NOTIFY STAFF AND OTHER CUSTODIANS 1
- STEP 2: IDENTIFY THE SCOPE OF THE BREACH AND TAKE STEPS TO CONTAIN IT 1
- STEP 3: NOTIFY THE INDIVIDUALS AFFECTED BY THE BREACH, THE IPC, AND/OR THE REGULATORY COLLEGES 2
- STEP 4: INVESTIGATE AND REMEDIATE 3

HOW TO MINIMIZE THE RISK OF A PRIVACY BREACH 4

OTHER RELEVANT PUBLICATIONS 5

In Ontario, health information custodians (custodians) have a duty under the *Personal Health Information Protection Act* (*PHIPA*) to protect personal health information (PHI) against privacy breaches. A privacy breach occurs when PHI is collected, used or disclosed without authorization. This can include theft, loss, or unauthorized copying, modification or disposal.

As a custodian, you should have a privacy breach protocol in place so that there is a process to follow in the event of a privacy breach. The protocol should be flexible enough to cover a wide range of possible breaches, such as:

- cyberattacks
- loss or theft of portable devices
- misdirected faxes, and
- collection of PHI without authority by means of the electronic health record.

Having a privacy breach protocol can help you meet your obligations under *PHIPA* by:

- enabling a quick, coordinated response
- clarifying roles and responsibilities
- establishing processes to investigate, contain and remediate the breach, and
- preparing for the possible involvement of the Information and Privacy Commissioner of Ontario (IPC).

WHAT TO DO WHEN A PRIVACY BREACH OCCURS

On learning of a privacy breach, you must take immediate action. The following steps may need to be carried out simultaneously or in quick succession. You may need to return to and repeat some of the steps.

STEP 1: NOTIFY STAFF AND OTHER CUSTODIANS

- Notify appropriate staff of the breach, including the chief privacy officer or other staff member responsible for privacy.
- Depending on the nature or seriousness of the privacy breach, you may need to contact senior management, the patient relations representative, and technology and communications staff.
- If the breach involves PHI on an electronic system shared between multiple custodians, notify all affected custodians.

STEP 2: IDENTIFY THE SCOPE OF THE BREACH AND TAKE STEPS TO CONTAIN IT

- Identify the scope of the breach, including individuals or organizations who may have been involved with or are responsible for the breach, and the nature and quantity of PHI that is affected.
- Retrieve any copies of PHI that have been disclosed.
- Ensure that no copies of PHI have been made or retained by anyone who was not authorized to receive the information. Record the person's contact information in case follow-up is required.

Determine whether the breach would allow unauthorized access to any other PHI, for instance if it is on a shared system. Take whatever steps are appropriate, such as changing passwords and identification numbers and/or temporarily shutting down your computer system.

- In a case of unauthorized access by an agent, consider suspending their access rights

STEP 3: NOTIFY THE INDIVIDUALS AFFECTED BY THE BREACH, THE IPC, AND/OR THE REGULATORY COLLEGES

DIRECT NOTIFICATION TO AFFECTED INDIVIDUALS

- *PHIPA* requires custodians to notify individuals affected by a breach at the first reasonable opportunity. Notification can be by telephone or in writing. Depending on the circumstances, you can make a notation in the individual's file to discuss at their next appointment.
- There are many factors to consider when deciding on the best form of notification (e.g., the sensitivity of the PHI). If unsure, contact the IPC to discuss the most appropriate form of notification.
- When notifying individuals affected by a privacy breach, you should provide the following information:
    - where appropriate, the name of the agent responsible for the unauthorized access
    - the date of the breach
    - a description of the nature and scope of the breach
    - a description of the PHI that was subject to the breach
    - the measures implemented to contain the breach, and
    - the name and contact information of the person in your organization who can address inquiries
- Notice to affected individuals must include a statement letting them know they are entitled to make a complaint to the IPC.
- If financial information or information from government-issued documents, such as health card numbers, are involved, the following statements can be included in the notice:

> As a precautionary measure, we strongly suggest that you contact your bank, credit card company, and relevant government offices to advise them that you may have been affected by this breach.
>
> We recommend you monitor and verify all your bank accounts, credit card and other financial transaction statements for any suspicious activity.
>
> If you suspect misuse of your personal information, you can obtain a copy of your credit report from a credit reporting bureau to verify the legitimacy of the transactions listed.
>
> - Equifax at 1-800-465-7166 or **www.equifax.ca**
> - TransUnion at 1-800-663-9980 or **www.transunion.ca**

If you are concerned that you may be a victim of fraud, you may request these bureaus place a fraud alert on your credit files instructing creditors to contact you before opening any new accounts.

If your health card number has been affected by the breach, you should call ServiceOntario INFOline at 1-866-532-3161 or 1-800-387-5559 to report your lost or stolen health card number. If you suspect misuse of your health card number, you can report suspected cases of fraud by calling the Ministry of Health and Long-Term Care at 1-888-781-5556 or e-mail at **reportohipfraud@moh.gov.on.ca**.

You may also wish to review this publication from the Information and Privacy Commissioner of Ontario, ***Identity Theft: A Crime of Opportunity***.

INDIRECT NOTIFICATION TO AFFECTED INDIVIDUALS

- Direct notification is the standard form of notice that health information custodians should provide to individuals impacted by a privacy breach. However, there are exceptional circumstances where custodians may consider providing indirect notification to affected individuals.
- Notification to affected individuals should occur as soon as possible following the breach, even if providing indirect notice.
- If your organization is considering indirect notification, you should consult with the IPC. You should be prepared to explain why you believe indirect notice is reasonable in the circumstances and your plans for it. This includes the content of your proposed notice and your strategies for distribution.
- Indirect notice to individuals may be considered by your organization where one or more of these exceptional circumstances apply:
    - The breach affects a significantly large number of individuals, making notifying the affected individuals directly impractical.
    - The risk of harm to affected individuals has reasonably been determined to be low.
    - You are unable to determine the identities of affected parties despite taking reasonable steps to do so.
    - There are questions as to the reliability/accuracy of contact information.
        - ◊ Note: Outdated contact information for a portion of the affected parties does not mean that all the affected parties 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 organization.
        - ◊ Note: All breach notification processes will involve the expenditure of time and resources. It is only when the time and resources required to provide direct notice cause unreasonable and significant interference with your operations that indirect notice may be an option.
    - Direct notification would be reasonably likely to be harmful or detrimental to the affected individuals.

CONTENT OF AN INDIRECT NOTICE

- After assessing the specific circumstances of the breach and determining in consultation with the IPC that indirect notice is a reasonable approach, the notice should:
    - Be written in plain language.
    - Provide enough information to enable someone reading the notice to easily understand how they may have been impacted by the breach.
    - Describe the circumstances of the breach.
    - Describe the cause of the breach, if known.
    - Indicate the date or period when the breach occurred.
    - Note the date when your institution became aware of the breach.
    - Describe the personal information/personal health information that is impacted in as much detail as possible.
    - Describe how the personal information/personal health information was affected by the breach (for example accessed, encrypted, exfiltrated, posted online, etc.).
    - Describe the risk of harm to affected individuals, if known.
    - Identify steps your institution has taken to contain the breach and reduce/mitigate the risk of harm to affected individuals.
    - Identify additional steps individuals can take to further reduce/mitigate the risk of harm.
    - Inform affected individuals that they can file a complaint with the Information and Privacy Commissioner of Ontario (as required under PHIPA and CYFSA and as of July 1, 2025, FIPPA) and provide a link to the IPC's website.
    - Provide contact information of an individual within the institution who can answer questions and provide additional information about the breach.
    - State whether you have reported the matter to the IPC and other appropriate regulatory bodies, as applicable.

DISTRIBUTION OF AN INDIRECT NOTICE

- The indirect notice must be distributed in a way that could reasonably be expected to reach the affected individuals.
- Thought and care should be put into deciding what strategy will be most effective to reach affected individuals. Multiple methods of public notification are generally most effective and are considered a best practice.
- A multi-channel public notice strategy should include a combination of some, or all, of the following methods to bring the notice to the attention of the affected individuals:
    - A prominent notice on your organization's website or a dedicated website containing details about the breach.

- ◊ If you are using your organization's website to provide notice, ensure the notice or a link to the notice is displayed prominently on the main page of your organizations' website and that it is clearly visible without the need for scrolling or searching.
- ◊ If you are using a dedicated breach website to provide notice, you should place a link to the breach website on the main page of your organization's website so it is clearly visible, and visitors can click through to access the breach website.
- ◊ All digital notices should remain posted for a reasonable period that will allow affected parties to read the notice.

- Ensure you take reasonable steps to bring the digital notice to the attention of affected parties. Affected parties 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 parties to read the notice.
  - ◊ Placing notices in national or local newspapers.
  - ◊ Creating social media posts on relevant platforms.
  - ◊ Purchasing radio and/or TV announcements and advertising targeted to affected individuals.
  - ◊ Issuing news releases and community notices targeted to affected individuals.
  - ◊ Hosting town halls and/or webinars to provide information.
  - ◊ Any other case-specific public communication strategies that would be effective for reaching individuals affected by the breach.

IPC

Under PHIPA, custodians must report certain privacy breaches to the IPC at the first reasonable opportunity and cooperate with the IPC, as described in ***Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector***.

REGULATORY COLLEGES

- You are required to notify a health care practitioner's regulatory college within 30 days if any of the following applies:
  - The practitioner was an employee or agent of the custodian and was terminated, suspended, or subject to disciplinary action as a result of a breach.
  - The practitioner's privileges or affiliation is revoked, suspended, or restricted as a result of a breach.
  - The practitioner resigns and the custodian has reason to believe that the resignation is related to an investigation or other action carried out as a result of an alleged breach.

- The practitioner relinquishes or voluntarily restricts their privileges or affiliation and the custodian has reasonable grounds to believe that it is related to an investigation or other action carried out as a result of an alleged breach.

STEP 4: INVESTIGATE AND REMEDIATE

- Conduct an internal investigation to:
  - ensure the immediate requirements of containment and notification have been met
  - review the circumstances surrounding the breach, and
  - review the adequacy of existing policies and procedures in protecting PHI
- Address the situation from a systemic basis; in some cases, program-wide procedures may warrant a review. For example, administrative or security controls on an electronic system may be insufficient and need to be updated or augmented.
- If you have notified the IPC of a breach, you will be asked to provide the details of your investigation and work with the IPC to identify and commit to any necessary remedial action.
- Keep a log of all privacy breaches and identify a person responsible for maintaining the log. For each privacy breach, record:
  - the name of the employee or agent that caused the breach, where it is determined to be relevant, such as in the case of unauthorized access
  - the date of the breach
  - the nature, scope and cause of the breach
  - the number of individuals affected by the breach
  - a description of the PHI that was subject to the breach, and
  - a summary of the steps taken to respond to the breach.
- You may also be required to cooperate in any IPC investigation related to the breach.

You must keep track of and report privacy breach statistics to the IPC, as required by *PHIPA*. The publication, ***Annual Reporting of Privacy Breach Statistics to the Commissioner***, describes what statistical information must be tracked and reported to the IPC.

HOW TO MINIMIZE THE RISK OF A PRIVACY BREACH

- Educate staff about the privacy rules in *PHIPA* governing the collection, use, disclosure, retention, transfer and disposal of PHI.
- Make sure policies and procedures are in place that comply with the privacy protection provisions of *PHIPA* and that staff are properly trained.
- Safeguard PHI when it is physically removed from the office or facility. Ensure that all laptops and personal devices are password protected and that data is encrypted.

- Ensure that no more PHI is collected, used or disclosed than is reasonably necessary to proactively lessen the impact of any privacy breaches.
- Ensure that you do not collect, use or disclose PHI if there is other information that will serve the intended purpose.
- Ensure that logging and auditing is in place on electronic systems containing health records. Make staff aware that the systems will be regularly audited.

Conduct a privacy impact assessment (PIA), where appropriate. The PIA helps determine whether new technologies, information systems and proposed programs or policies meet basic privacy requirements. For further information, see the IPC publication, ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act***.

When in doubt, seek advice from your organization's legal department and chief privacy officer.

Custodians may also consult with the IPC for comments on actual or proposed information practices.

OTHER RELEVANT PUBLICATIONS

For information about a custodian's legal obligation to report privacy breach statistics, see ***Annual Reporting of Privacy Breach Statistics to the Commissioner***.

Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector details the circumstances in which it is mandatory to report a privacy breach to the IPC.

For information about how to detect and prevent unauthorized access to PHI, refer to ***Detecting and Deterring Unauthorized Access to Personal Health Information*** and ***Protecting Against Ransomware***. If you have further questions or concerns about responding to a health privacy breach or the duties and obligations of custodians, please contact us at **info@ipc.on.ca** or 1-800-387-0073.

Responding to a Health Privacy Breach: Guidelines for the Health Sector

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

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

Updated: March 2025