PHIA Guidelines

How to Complete the Reporting a Privacy Breach Form

CONTENTS

Purpose

These are guidelines to assist custodians in completing our Reporting a Privacy Breach Form.

Notification to OIPC

Section 15(4) of the **Personal Health Information Act** (PHIA) requires a custodian to notify the Office of the Information and Privacy Commissioner (OIPC) of a privacy breach:

> Where a custodian reasonably believes that there has been a material breach as defined in the regulations involving the unauthorized collection, use, or disclosure of personal health information, that custodian shall inform the commissioner of the breach.

To notify OIPC, a custodian must complete and send the Reporting a Privacy Breach Form as soon as reasonably possible to breachreport@oipc.nl.ca. A custodian may also send this form by mail to the Office of the Information and Privacy Commissioner, PO Box 13004, Station A, St. John's, NL A1B 3V8, or by fax to 709-729-6500.

Find more information about what constitutes a material breach in **Common Questions** under subheading titled **What is a Material Privacy Breach?** Although custodians are not required to inform OIPC of breaches which do not meet the definition of material, they are welcome to do so.

Notification to OIPC of a material privacy breach is one of many steps a custodian must take in managing a privacy breach. Find more information about managing a privacy breach in **Common Questions** under subheading titled **How Should a Custodian Respond to a Privacy Breach?**

OIPC is a public body and therefore subject to the **Access to Information and Protection of Privacy Act, 2015**. Pursuant to this Act, OIPC receives access to information requests for records in its custody or control. The Reporting a Privacy Breach Form qualifies as a record under OIPC's custody or control and therefore it may be subject to an access to information request.

Removing or Anonymizing Personal Health Information or Personal Information

When filling out the different sections of the form you should remove or anonymize personal health information or personal information. Do not include information that would identify:

- the affected individuals (e.g. the persons whose personal health information was improperly collected, used, disclosed, lost, stolen, etc.);
- the other individuals involved in the breach (e.g. the person who was sent the personal health information of someone else sometimes referred to as the wrongful recipient); or
- the custodian's employees involved in the privacy breach beyond their title or role (e.g. the employee who sent personal health information to the wrong person).

If you are attaching additional documents to the form, it is also necessary to remove or anonymize the personal health information or personal information contained within those attachments.

Example: Alexis is an employee of the custodian. She sent Jacob's medical assessment containing his personal health information to Jackson by accident. Jacob and Jackson had similar email addresses. When filling out the form, you could anonymize this information as follows:

> An employee of the custodian sent Person A's assessment to Person B by accident. Person A and Person B had similar email addresses.

Date of Reporting this Privacy Breach

For the "Date of Reporting this Privacy Breach", fill in the date you are sending the Reporting a Privacy Breach Form to OIPC. Do not use the date on which the custodian informally relayed information to OIPC. OIPC encourages and appreciates when a custodian informally advises that a privacy breach has occurred and formal notification is pending, however this informal step is not notification within the meaning of section 15(4) of PHIA.

The date you send OIPC the completed Reporting a Privacy Breach Form is the date the custodian is notifying OIPC of a privacy breach in compliance with section 15(4) of PHIA.

Example: On **January 10, 2025**, Joan, the custodian's privacy officer, calls OIPC to let them know they recently became aware of a privacy breach affecting at least 75 patients and are taking steps to manage this breach. Joan says she will send in the form as soon as she can. On **January 24, 2025**, Joan completes the Reporting a Privacy Breach Form and emails it to OIPC. In the form, Joan fills out the reporting date as follows:

> **Date of Reporting this Privacy Breach:** January 24, 2025

Section 1: Custodian Information

Custodian Name, Mailing Address, and Physical Work Address

Fill in the custodian's full name.

Fill in the custodian's complete mailing address, and if different, the custodian's complete physical work address as well.

Do not use initials, acronyms, or abbreviations when filling in this section.

Name and Title of Contact Person, Contact Phone Number, and Contact Email

At times, OIPC may have follow-up questions about the privacy breach, may seek clarification on information or statements in the form, or may wish to offer general guidance to a custodian.

The contact person in this section should be the person who OIPC can communicate with about the privacy breach.

Fill in the first and last name of the custodian's contact person and the title of that contact person (e.g. Privacy Officer, Custodian, etc.).

Fill in the contact person's current phone number and email address. OIPC may use this to communicate with the contact person about the privacy breach.

Section 2: Discovery, Investigation, and Containment

Date Breach Occurred

This is the date when the privacy breach took place.

If known, fill in the specific date that the privacy breach occurred.

If you do not know the specific date, you may provide an estimated date or date range and an explanation of this estimate in the Discovery, Investigation, and Containment Details text box.

Date Breach Discovered

This is the date when the custodian became aware of a privacy breach. A custodian may discover a privacy breach through internal monitoring, reports from affected individuals, or notifications from other parties.

Fill in the specific date when the custodian discovered the breach.

Number of Affected Individuals

The affected individuals are the individuals who had their personal health information improperly collected, used, disclosed, lost, stolen, etc.

When filling in the number of affected individuals try to be as precise as possible. If you do not know or if you cannot readily calculate the number, you may provide an estimate. If providing an estimate, specify this on the form.

Example: A custodian is unsure of the exact number of patients impacted by the privacy breach. Based upon the information in their records, at the time of filling in the form they estimate that approximately 75 patients were affected. When filling out the form, you could specify this as follows:

Number of Affected Individuals	75 (estimate)

Breach Type

Identify what type of privacy breach occurred.

The form lists several common breach types. Check the appropriate box.

If the type of privacy breach does not fit well within the offered options, check the ☑ Other box and specify the type of breach.

Discovery, Investigation, and Containment Details

Provide details presently known about the discovery, investigation, and containment of the privacy breach.

Use this section to explain or answer questions such as the following.

- How did the custodian discover and become aware of the privacy breach?
- What steps did the custodian take to investigate the privacy breach?
- How did the privacy breach occur?
- What was the root cause of the privacy breach?
- What factors or circumstances, if any, contributed to the privacy breach?
- What did the custodian do to contain the breach or reduce the harm of the breach?
- Were the containment measures successful or not?

If a custodian's investigation or containment steps are ongoing and have not concluded, explain this in the form. OIPC may request additional information after reviewing the form or may request an update from the custodian after their investigation has concluded.

Examples of containment steps include:

- stopping the unauthorized practice;
- recovering the records;
- shutting down the system that was breached;
- revoking access to personal health information; and
- correcting weaknesses in physical, administrative, or technical safeguards.

Example: The custodian describes discovery, investigation, and containment steps of a misdirected fax as follows in the form:

> On Feb. 25, 2025, I discovered that a fax containing a patient's personal health information (PHI) was mistakenly sent to the wrong doctor's office. The error was identified on the same day when I received a call from the incorrect recipient. I reviewed the fax transmission log and confirmed that the fax number had been entered incorrectly. I confirmed with the incorrect recipient that the misdirected fax was shredded and not shared or retained.

Section 3: Personal Health Information Involved

Identify what type of personal health information was involved in the privacy breach. In other words, what kind of personal health information was stolen, lost, improperly collected, used, or disclosed?

The form lists several common types of personal health information. A privacy breach often involves more than one type of personal health information. Check all of the boxes that apply to the privacy breach you are reporting on.

If the privacy breach involved a type of personal health information that is not on the form, check the ☑ Other box and insert the type of personal health information. The insertion should be a general category or kind of personal health information (not the personal health information itself).

Find out more about personal health information in **Common Questions** under the subheading titled **What is Personal Health Information?**

Section 4: Risk Evaluation and Potential Harm

In this section, you are identifying potential risks or harms to the affected individuals whose personal health information was impacted by the breach.

A privacy breach often involves more than one risk or potential harm. Check all of the boxes that apply to this privacy breach.

The form lists several common risks or harms. If the privacy breach involved a type of risk or harm that is not on the form, check the ☑ Other box and specify the risk or harm.

Common examples of personal health information that could lead to the identified harm under the different categories include the following.

- **Identity theft**: Personal health information vulnerable to this risk or harm includes, but is not limited to, social insurance numbers, credit card numbers, bank account details, driver's license numbers, passport numbers, MCP numbers, etc.
- **Bodily harm or harassment**: Personal health information can be linked to personal safety but must be assessed on a case-by-case basis. Such information may include, but is not limited to, personal addresses, emails, phone numbers, locations, daily routines, medications on hand, etc.

> Many types of information that might initially seem unrelated to health care are considered personal health information under PHIA. It is important to recognize that personal health information can include a broader range of details than one might typically assume. Find out more in **Common Questions** under the subheading titled **What is Personal Health Information?**

- **Emotional harm, humiliation, or damage to reputation or relationships**: Personal health information susceptible to this risk or harm includes, but is not limited to, medical information, sexual orientation, religious beliefs, political views, records exposing financial troubles or missteps, etc.
- **Financial loss:** Personal health information vulnerable to financial exploitation includes, but is not limited to, credit card details, bank account numbers, social insurance numbers, compromised login credentials for online accounts, etc.
- **Loss of employment, business, or professional opportunities:** Personal health information susceptible to this risk or harm includes, but is not limited to, disciplinary investigations or proceedings, termination records, communicable disease status, chronic illness diagnosis, mental health issues, criminal history, controversial affiliations, etc.

Section 5: Notification to Affected Individuals

Date of Notification to Affected Individuals

If a custodian has notified affected individuals, check the ☑ Yes box and fill in the date of notification. If notifications took place on more than one date, fill in a date range (when notifications started and when they were completed) and explain the notification date range within the Notification Details text box.

If a custodian has not yet notified affected individuals, check the ☑ Not Yet box and fill in the anticipated completion date for notification.

If a custodian is not going to notify individuals, check the ☑ No box, and skip to the Reasons Why Notification Did Not Occur text box to explain why.

If there is a combination of two or more of these options (☑ Yes, ☑ No, or ☑ Not Yet) check all boxes that apply, fill in all applicable dates or date ranges, and provide explanations as appropriate.

Find more information about notification requirements in **Common Questions** under subheading titled **Is a Custodian Required to Notify Affected Individuals**?

Example: A breach involved the person's name, birth date, medical history, MCP and a photograph of the impacted person. The custodian fills out this information in the form as follows:

☑ Name ☑ Birth Date ☑ Medical History ☑ Medicare Plan (MCP) Number

☑ Other (please specify): Digital Photograph of the impacted person and its meta data

Notification Method

The notification method is how a custodian informs affected individuals about the privacy breach.

The form lists several common notification methods. Identify the notification method that you used or will be using to notify affected individuals. If multiple methods are used, ensure you check all applicable boxes.

If a method used is not listed, check the ☑ Other box and specify what other methods of notification were used.

Find more information about notification methods in **Common Questions** under subheading titled **How Should a Custodian Notify Affected Individuals?**

Notification Details

Use this section to provide details of notifications to affected individuals, including a summary of the content, any extended notification periods (date ranges), or reasons for lack of direct notification.

You may copy notification content into this section or attach it ensuring identifying personal health information or personal information is removed.

In general, the content of a notification of a privacy breach should include:

- the date of the privacy breach or approximate period if exact date is unknown;
- general description of the circumstances of the privacy breach;
- general description of the impacted personal health information;
- steps taken so far to control or reduce the harm;
- future steps planned to prevent further privacy breaches;
- steps affected individuals can take to reduce or mitigate the harm from the privacy breach;
- custodian's contact information that the affected individual can use to obtain further information about the privacy breach; and
- OIPC's contact information and notification of an individual's right to make a complaint.

A custodian may also wish to provide an apology to affected individuals within its notification.

Example: A medical report being faxed to the wrong insurance company (misdirected fax). The custodian copies the notification content into the form as follows:

Dear [Patient's Name],

Subject: Notification of Privacy Breach – Incorrect Fax Transmission

We are writing to inform you of an incident involving your personal health information that occurred on March 3, 2025. We want to be transparent and let you know what happened, the steps we have taken to address the issue, and the actions you can take if you are concerned.

What Happened

On March 3, 2025, a medical report containing your personal health information was faxed to the wrong insurance company adjuster. The report was intended for [Correct Insurance Company and Adjuster Name], but it was mistakenly sent to [Incorrect Insurance Company]. The error occurred because an outdated fax number was used in the fax transmission. Although the correct adjuster name and company were on the fax sheet, the old template had an incorrect fax number.

What Information Was Affected

The medical report included the following personal health information: your name, MCP number, date of birth, medical history, and medical diagnosis.

Steps Taken So Far

As soon as we were informed of the mistake, we took immediate action. The insurance company that received the fax contacted us, and we reviewed the fax log. We confirmed that an outdated fax number was the cause of the error. We requested and received written confirmation that the information sent in error was securely destroyed and no copies retained.

Steps We Are Taking to Prevent Future Breaches

To prevent a similar incident from occurring in the future, we are taking the following steps:

- updating all fax templates with the correct contact information;
- conducting additional staff training on the importance of verifying fax numbers before sending sensitive information; and
- implementing a new procedure to double-check recipient details before faxing reports.

How You Can Protect Yourself

Although we have taken action to address this breach, you may want to review your insurance statements for any discrepancies or concerns. If you notice anything unusual, please contact us or your insurance company right away.

Further Information and Assistance

If you have any questions or concerns, please don't hesitate to contact us directly at [Phone Number] or [Email Address]. We are committed to ensuring your privacy is protected.

Additionally, you have the right to make a formal complaint. Should you decide to make a complaint, contact the Office of the Information and Privacy Commissioner at [OIPC Contact Information].

We sincerely apologize for this error and any inconvenience it may have caused. Please rest assured that we are doing everything we can to prevent future breaches and protect your personal health information.

Thank you for your understanding.

Sincerely, [Custodian's Name and Contact Information]

Reasons Why Notification Did Not Occur

If notification to affected individuals is required under PHIA and it did not happen, use this section to detail the custodian's attempted notification efforts or reasons that prevented notification.

If the custodian is relying upon section 15(7) of PHIA and has made the decision not to notify affected individuals, explain why the custodian believes the privacy breach will not have an adverse impact upon the provision of health care or other benefits to the affected individual, or the mental, physical, economic, or social well-being of the affected individual. Find more information in **Common Questions** under subheading titled **Is a Custodian Required to Notify Affected Individuals**?

Section 6: Other Notifications

A custodian may wish to notify other organizations of the privacy breach.

Identify other organizations that were notified of the privacy breach. If unlisted, please check the ☑ Other box and specify the name of the organization notified.

Section 7: Safeguards, Mitigation, and Prevention

Safeguards

Safeguards are the strategies or controls put in place by a custodian to protect personal health information. In general, there are technical safeguards, administrative safeguards, and physical safeguards.

The form lists several common safeguards. Identify all applicable safeguards that existed to protect the personal health information that was involved in this particular breach (the custodian may not have all safeguards).

If there were other or additional safeguards in place to protect the personal health information, check the ☑ Other box and provide an explanation specifying the type of safeguards used.

Mitigation and Prevention Details

Provide details of what steps the custodian has taken in an effort to prevent or mitigate the risk of this type of privacy breach from occurring again in the future.

Examples of mitigation and prevention steps include:

- cautioning an employee;
- employee training or retraining;

- reviewing and signing or resigning of confidentiality oaths, affirmations, or agreements;
- educational awareness campaign;
- conducting or reviewing and updating a privacy impact assessment;
- stopping a practice that caused or contributed to the privacy breach;
- changing or creating policies or procedures;
- changing and strengthening passwords;
- strengthening physical security safeguards (e.g. alarms, locks, barriers, etc.); or
- strengthening technical security safeguards (e.g. restricting user access, data encryption, firewalls, multi-factor authentication, auditing, etc.).

If steps are ongoing or not yet complete, explain this in the form and, if possible, provide an estimate as to when the custodian expects mitigation or prevention measures to be complete.

Example: A custodian employee sent an email to five different patients and forgot to use the BCC field resulting in email addresses and names within addresses being visible to the entire group. The custodian describes its mitigation and prevention steps as follows in the form:

> A supervisor cautioned the employee on the importance of reviewing all email input fields prior to sending emails. We are developing a new policy and procedure for emails, which will include a section addressing the BCC field and hope to complete this within three months. In the meantime, we have added this issue as a standing item to our regular meetings with staff "BCC reminders" (awareness campaign).

Attaching Additional Documents

You may attach additional documents if you believe it necessary to supplement the information provided in the form.

Check the appropriate box to indicate if you are or are not attaching documents to the form.

If you do attach additional documents, you must remove or anonymize all identifying personal health information or personal information from the attachments.

Common Questions

What is Personal Health Information?

Section 5(1) of PHIA defines "personal health information" as identifying information in oral or recorded form about an individual that relates to:

(a) the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family;

(b) the provision of health care to the individual, including information respecting the person providing the health care;

(c) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;

(d) registration information;

(e) payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;

(f) an individual's entitlement to benefits under or participation in a health care program or service;

(g) information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;

(h) a drug as defined in the Pharmacy Act, 2024, a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or

(i) the identity of a person referred to in section 7.

More details about **section 5(1)(b)** are found in section 5(2)(a)-(c). The "information respecting the person providing health care" means, in relation to that person, the following information as applicable: the name, business title, address and telephone number; licence number; and profession, job classification and employment status.

What person is **section 5(1)(i)** talking about? Section 7 is under the subheading **Representative** and lists out different types of representatives a person may have. Be sure to review section 7 of PHIA to get all the details.

Section 5(3) notes that personal health information also includes identifying details about an individual found in a record that contains personal health information; for example, identifying details relating to next of kin, children, or other family members.

Section 5(5) defines what is meant by “identifying information” stating it is information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or together with other information, to identify an individual.

A record can contain “personal health information” even if it does not have the individual’s name associated with it.

What is a Privacy Breach?

A privacy breach occurs when there is an unauthorized collection, use, or disclosure of personal health information and this includes when personal health information is lost or stolen. This unauthorized activity is in contravention of PHIA.

Privacy breaches may arise due to accidental human error, insufficient safeguards, faulty procedures or practices, as well as intentional or malicious actions.

The following are privacy breach examples:

- personal health information mailed, emailed, or faxed to the wrong person;
- records containing personal health information left unsecured in an area accessible by the public (insufficient safeguards);
- equipment or records containing personal health information are lost or stolen;
- disclosing personal health information to an unauthorized person; or
- a malicious actor infiltrating, accessing, copying, or removing personal health information within the custodian's email account, computer systems, servers, etc.

What is a Material Privacy Breach?

Section 15(4) of PHIA requires a custodian to notify OIPC when they reasonably believe a material privacy breach has occurred. Section 5 of the **Personal Health Information Regulations** provides a list of factors to consider when assessing whether a privacy breach is material, stating:

> The factors that are relevant to determining what constitutes a material breach for the purpose of subsection 15(4) of the Act include the following:
>
> (a) the sensitivity of the personal health information involved;
>
> (b) the number of people whose personal health information was involved;
>
> (c) whether the custodian reasonably believes that the personal health information involved has been or will be misused; and
>
> (d) whether the cause of the breach or the pattern of breaches indicates a systemic problem.

This list of factors is non-exhaustive and therefore it is not a complete list. This means custodians may want to consider other important factors, even if not on the list within section 5. For example, such other factors may include:

- Duration of Exposure: how long the personal health information was exposed or at risk;
- Intentional Breaches: whether this was an intentional privacy breach; and
- Vulnerable Individuals: whether the privacy breach involved vulnerable individuals, such as youth or seniors.

Custodians should err on the side of caution and report privacy breaches to the Commissioner if there is any doubt as to whether a breach is material.

Although custodians are not required to inform OIPC of breaches which do not meet the definition of "material," they are welcome to do so.

How Should a Custodian Respond to a Privacy Breach?

A custodian must take reasonable steps to manage a privacy breach.

While OIPC can provide high level, general guidance about steps to take in responding to privacy breaches, we cannot provide a custodian with advice or direction on responding to a specific privacy breach. Because of our role in overseeing compliance with privacy law, OIPC may subsequently receive a complaint and need to investigate a particular privacy breach. Accordingly, we must avoid taking an active role in a custodian's response to a privacy breach in order to maintain our independent role.

The Department of Health and Community Services has created resources to assist custodians meet their obligations under PHIA. Custodians seeking more information on what steps to take in managing a privacy breach may wish to review the Department's **Privacy Breach Guidelines** located within its **PHIA Risk Management Toolkit** resources by visiting the Department's PHIA Webpage and downloading its Toolkit.

Custodians may also find the ATIPP Office's guidance documents Privacy Breach Protocol or What to do if a Privacy Breach Occurs useful. While these documents are directed at public bodies and are based upon the **Access to Information and Protection of Privacy Act, 2015**, many of the steps and principles remain applicable.

Is a Custodian Required to Notify Affected Individuals?

Pursuant to section 15(3) of PHIA, a custodian must notify individuals impacted by the privacy breach at the first reasonable opportunity when personal health information is stolen, lost, disposed of (except as permitted by law), disclosed to an unauthorized person, or accessed by an unauthorized person.

However, under section 15(7), a custodian is not obligated to notify the impacted individual if the custodian reasonably believes the privacy breach will not have an adverse impact on the individual's:

- provision of health or other benefits; or
- mental, physical, economic, or social well-being.

If a custodian is uncertain about the potential impact of a privacy breach, they should notify the impacted individual. If the custodian reasonably believes the privacy breach will not have an adverse impact, the custodian may choose to err on the side of caution and notify the impacted individual.

Even if a custodian believes the privacy breach will not have an adverse impact and is not required, the Commissioner may still recommend notifying affected individuals under section 15(5) of PHIA.

Custodian researchers are custodians who received personal health information from another custodian under section 44, which is the Disclosure for Research provision.

There are additional steps required of custodian researchers for privacy breaches that occur to the personal health information disclosed to them for research purposes. Section 15(6) confirms a custodian researcher cannot notify the impacted individual of the privacy breach unless the custodian who provided the personal health information to the researcher:

- first obtains the impacted individual's consent to be contacted by the researcher; and
- then informs the researcher that the impacted individual has given their consent.

The impact of section 15(6) means that the custodian researcher must contact the custodian who provided them with the personal health information impacted by the privacy breach and work with that custodian so that the necessary notifications to impacted individuals can occur.

How Should a Custodian Notify Affected Individuals?

Under section 15(3) of PHIA, a custodian must notify affected individuals at the first reasonable opportunity.

PHIA does not specify how a custodian should notify affected individuals. This means a custodian must determine what notification method or methods to use.

In most cases, a custodian should directly notify affected individuals via meetings (in-person or virtual), letters, phone calls, emails, or similar direct notification means.

In some cases, direct notification may not be possible or feasible, leading a custodian to resort to indirect notification methods like public advisories, newspaper advertisements, media releases, website alerts, or social media posts to inform affected individuals. If a custodian uses indirect notification, they must use a method or methods they reasonably expect will reach affected individuals.

If direct notification does not occur and only indirect notification methods are used, a custodian should explain the reasons why in the Notification Details text box in the form.

Common examples of when a custodian may decide to use indirect notification methods include:

- if contact information is unknown or unreliable, such as when this information is significantly dated; or
- if using direct notification could reasonably cause a custodian undue hardship, such as when the breach impacted a very large number of individuals and the custodian has limited resources.

At times, using multiple methods of notification may be the most effective approach, for example using indirect public notification to reach as many people as quickly as possible, and

then following this up with direct notification letters. It is important that the content of notification remains consistent throughout all methods to avoid unnecessary confusion.

What Happens After OIPC Receives the Reporting a Privacy Breach Form?

OIPC records information contained in the form for breach management purposes including, but not limited to, statistical, educational, and investigative purposes.

After a custodian sends a completed **Reporting a Privacy Breach Form** to breachreport@oipc.nl.ca, OIPC will assign an Access and Privacy Analyst (APA) to review the contents of the form.

If OIPC has questions, the APA will communicate with the custodian's designated Contact Person using the provided phone or email from the form.

The APA will inform the Commissioner of the privacy breach.

OIPC may not need to follow up with the custodian after reviewing the form. In this case, after filing the form, the custodian will not receive any requests or communications from OIPC about the privacy breach.

If the custodian did not notify affected individuals, the Commissioner may recommend it do so under section 15(5) of PHIA. If recommended, the APA will notify the custodian's Contact Person and request confirmation of notification.

A privacy breach may result in affected individuals, or someone on their behalf, filing a privacy complaint with OIPC. The **Reporting a Privacy Breach Form** a custodian submits to OIPC may be used in OIPC's investigation of a privacy complaint. An APA will notify the custodian in writing in the event of a privacy investigation. For further details on the investigation process, refer to our guidelines Custodian Responding to a Privacy Complaint.

How do I Contact OIPC with Questions or Concerns?

If you have any questions or concerns about these guidelines or the **Reporting a Privacy Breach Form**, please do not hesitate to contact our Office at:

Office of the Information and Privacy Commissioner
PO Box 13004, Station A
St. John's, NL A1B 3V8
Phone: (709) 729-6309 Fax: (709) 729-6500
Toll Free: 1-877-729-6309
commissioner@oipc.nl.ca
https://www.oipc.nl.ca