ATIPPA, 2015 Guidelines

How to Complete the Reporting a Privacy Breach Form

CONTENTS

Purpose

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

Notification to OIPC

Section 64(4) of the **Access to Information and Protection of Privacy Act, 2015** (ATIPPA, 2015) requires a public body to notify the Office of the Information and Privacy Commissioner (OIPC) of a privacy breach:

> Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.

To notify OIPC, a public body must complete and send the Reporting a Privacy Breach Form as soon as reasonably possible to breachreport@oipc.nl.ca. A public body 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.

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

Notification to ATIPP Office

The Access to Information and Protection of Privacy Office (ATIPP Office) requests public bodies notify its Office of a privacy breach.

To notify the ATIPP Office a public body can send a copy of the form to ATIPPOffice@gov.nl.ca. A public body may also send this form by mail to ATIPP Office, PO Box 8700, Station A, St. John's, NL A1B 4J6.

Removing or Anonymizing Personal Information

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

- the affected individuals (e.g. the persons whose personal 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 information of someone else sometimes referred to as the wrongful recipient); or
- the public body employees involved in the privacy breach beyond their title or role (e.g. the employee who sent personal information to the wrong person).

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

Example: Emma is a public body employee. She sent James' application form containing his personal information to Jacob by accident. James and Jacob had similar email addresses. When filling out the form, you could anonymize this information as follows:

> A public body employee sent Person A's application form 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 a public body informally relayed information to OIPC. OIPC encourages and appreciates when a public body 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 64(4) of ATIPPA, 2015.

The date you send OIPC the completed Reporting a Privacy Breach Form is the date the public body is notifying OIPC of a privacy breach in compliance with section 64(4) of ATIPPA, 2015.

Example: On **January 10, 2025**, Kelsey, the public body's privacy officer, calls OIPC to let it know they recently became aware of a privacy breach affecting at least 400 people and are taking steps to manage this breach. Kelsey says she will send in the form as soon as she can. On **January 24, 2025**, Kelsey completes the Reporting a Privacy Breach Form and emails it to OIPC. In the form, Kelsey fills out the reporting date as follows:

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

Section 1: Public Body Information

Public Body Name and Division or Program

Fill in the complete public body name and, if applicable, the division or program name.

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 public body.

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

Fill in the first and last name of the public body's contact person and the title of that contact person (e.g. Privacy Officer, Clerk, ATIPP Coordinator, 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 public body became aware of a privacy breach. A public body may discover a privacy breach through internal monitoring, reports from affected individuals, or notifications from other parties.

Fill in the specific date when the public body discovered the breach.

Number of Affected Individuals

The affected individuals are the individuals who had their personal 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: The public body is unsure of the exact number of people impacted by the privacy breach. Based upon the information in their records, at the time of filling in the form they estimate that approximately 400 people were affected. When filling out the form, you could specify this as follows:

Number of Affected Individuals	400 (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 public body discover and become aware of the privacy breach?
- What steps did the public body 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 public body do to contain the breach or reduce the harm of the breach?
- Were the containment measures successful or not?

If a public body'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 public body after its 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 information; and
- correcting weaknesses in physical, administrative, or technical safeguards.

Example: The public body describes discovery, investigation, and containment steps of a misdirected email as follows in the form:

> A public body employee sent an email that contained Person A's personal information to Person B by accident. Person A and B had similar email addresses and the employee relied on the "auto-fill" feature. The employee discovered this error later that day. The employee immediately tried to recall the email but this was not successful. They tried to call Person B but there was no answer. After discussing it with their supervisor, the employee emailed Person B to ask them not to open or forward the email; to delete it permanently from their inbox and deletion folders; and to confirm once this was done. The next day, Person B confirmed the email was deleted.

Section 3: Personal Information Involved

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

The form lists several common types of personal information. A privacy breach often involves more than one type of personal 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 information that is not on the form, check the ☑ Other box and insert the type of personal information. The insertion should be a general category or kind of personal information (not the personal information itself).

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

Section 4: Risk Evaluation and Potential Harm

In this section, you are identifying potential risks or harms to the affected individuals whose personal 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 information that could lead to the identified harm under the different categories include the following.

- **Identity theft**: Personal 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 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, etc.
- **Emotional harm, humiliation, or damage to reputation or relationships**: Personal 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 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 information susceptible to this risk or harm includes, but is not limited to, disciplinary investigations or proceedings, performance reviews, termination records, criminal history, controversial affiliations, etc.

Section 5: Notification to Affected Individuals

Date of Notification to Affected Individuals

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

If the public body 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 Public Body Required to Notify Affected Individuals?**

Example: The breach involved an email containing Person A's name, email address and a photograph of Person A. The public body fills out this information in the form as follows :

☑ Name

☑ Email

☑ Other (please specify): Digital Photograph of Person A and its meta data

Notification Method

The notification method is <u>how</u> a public body 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 the public body used.

Find more information about notification methods in **Common Questions** under subheading titled **How Should a Public Body 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 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 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;
- public body'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 public body may also wish to provide an apology to affected individuals within its notification.

Example 1: A public body may **describe** the notification content (BCC Related Error):

We sent letters to affected individuals advising them of the **date of the breach** (March 25, 2023), the **general description of the privacy breach** (an email sent to them and several recipients was mistakenly sent via CC versus BCC), the **personal information description** (confirmed that email addresses and names within email addresses were visible to other recipients of the email), the **steps taken so far to address breach** (explained that we attempted a recall, and then sent a request for deletion of the email and for individuals not to use any of the exposed email addresses), our **future steps planned to prevent further privacy breaches** (confirmed we were going to have staff engage in retraining for our email program and will develop an email review checklist), the **steps the individual can take** (warned individuals how emails can be used for phishing to obtain more information for fraudulent purposes and directed them to CRAs website which includes an explanation of email phishing and tips on preventing identity fraud) and provided our **privacy officer's contact information** (name and contact information to speak with our privacy officer about the privacy breach). ☑ **Yes**. We notified individuals of their right to file a privacy complaint with OIPC.

Example 2: A public body may **copy** the notification content (BCC Related Error):

Dear [**AFFECTED INDIVIDUAL**] We are writing to inform you that on March 25, 2023, our Office sent an email sharing a service opportunity. Instead of inserting email addresses into the BCC (blind carbon copy) field of the email as is normally done, email addresses were mistakenly put in the carbon copy (CC) field. As a result of this error, your email address and your name (that was contained within that email address) were visible to the other recipient individuals. Upon discovering the error, the email was immediately recalled, and we requested each individual delete the email.

We would like to extend sincere apologies for this error. We are taking steps to improve organizational safeguards to prevent such errors from occurring again, including retraining for employees on our email program, and development of a review checklist for sending out emails that are to be distributed by the BCC method.

Email addresses paired with other information such as an individual's name can be used to try to obtain more information for fraudulent purposes through a method known as phishing. Be careful before you respond to suspicious emails or before clicking on links in emails you receive. For more information about phishing, getting cyber safe, and protecting yourself from identity theft online, visit the Canadian Centre for Cyber Security website.

Should you have any questions please contact our privacy officer [**Privacy Officer's Name and Contact Information**]

If you are not satisfied with our response to this privacy breach, you have the right to file a privacy complaint with the Office of the Information and Privacy Commissioner. The address and contact information is as follows: [**OIPC's Contact Info here**]

Reasons Why Notification Did Not Occur

If notification to affected individuals is required under ATIPPA, 2015 and it did not happen, use this section to detail the public body's attempted notification efforts or reasons that prevented notification.

If the public body is relying upon section 64(7) of ATIPPA, 2015 and has made the decision not to notify affected individuals, explain why the public body believes the privacy breach does not create a risk of significant harm to affected individuals.

Section 6: Other Notifications

A public body may wish to notify other organizations or persons within the public body of the privacy breach.

Identify other organizations or persons within the public body that were notified of the privacy breach. If unlisted, please check the ☑ Other box and specify the type of notification.

The ATIPP Office has requested that all public bodies notify its Office of a privacy breach. For more information on this please see **Notification to ATIPP Office** on page two.

Section 7: Safeguards, Mitigation, and Prevention

Safeguards

Safeguards are the strategies or controls put in place by a public body to protect personal 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 information that was involved in this particular breach (the public body may not have all safeguards).

If there were other or additional safeguards in place to protect the personal 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 public body 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 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 public body expects mitigation or prevention measures to be complete.

Example: A public body employee sent an email to 100 different individuals and forgot to use the BCC field resulting in email addresses and names within addresses being visible to the entire group. The public body 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 are sending out periodic "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 information from the attachments.

Common Questions

What is a Privacy Breach?

A privacy breach occurs when there is an unauthorized collection, use, or disclosure of personal information and this includes when personal information is lost or stolen. This unauthorized activity is in contravention of ATIPPA, 2015.

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

What is Personal Information?

Section 2(u) of ATIPPA, 2015 defines "personal information" as being recorded information about an identifiable individual. A record can contain "personal information" even if it does not have the individual's name associated with it.

An identifiable individual is a natural person and not a corporation. OIPC does not accept forms about privacy breaches related to a corporation or a corporation's information.

Section 2(u) also provides a list of "personal information" examples:

- the individual's name, address, or telephone number;
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
- the individual's age, sex, sexual orientation, marital status, or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- information about the individual's health care status or history, including a physical or mental disability;
- information about the individual's educational, financial, criminal or employment status or history;
- the opinions of a person about the individual; or
- the individual's personal views or opinions, except where they are about someone else.

This list of "personal information" examples is non-exhaustive and therefore it is not a complete list. This means that other types of recorded information may be considered personal information, even if it is not on the list within the section 2(u) definition.

How Should a Public Body Respond to a Privacy Breach?

A public body 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 public body 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 public body's response to a privacy breach in order to maintain our independent role.

However, the ATIPP Office can provide more direct guidance and assistance to public bodies responding to specific privacy breaches.

Therefore, a public body seeking more information on what steps to take in managing a privacy breach may wish to:

- review the ATIPP Office's guidance documents found on its website, including Privacy Breach Protocol or What to do if a Privacy Breach Occurs; and
- contact the ATIPP Office for assistance at 709-729-7072 or toll free at 1-877-895-8891, or ATIPPOffice@gov.nl.ca.

Is a Public Body Required to Notify Affected Individuals?

Pursuant to section 64(3) of ATIPPA, 2015, public bodies must notify individuals impacted by the privacy breach at the first reasonable opportunity where the information is stolen, lost, disposed of (except as permitted by law), disclosed to an unauthorized person, or accessed by an unauthorized person.

However, as set out in section 64(7), if the head of the public body reasonably believes that the privacy breach does not create a risk of significant harm to the impacted individual, the public body is not required to notify the impacted individual. This requires the public body to conduct a risk assessment for significant harm. While a public body may take into consideration a number of factors, section 64(9) specifies two key factors relevant to this assessment: the sensitivity of the personal information and the likelihood of its misuse.

Public bodies may still wish to notify affected individuals despite believing there is no risk of significant harm. Reasons why a public body may still decide to notify affected individuals include:

- wanting to **prevent any possible harm** by promptly informing individuals and allowing them to take precautions to protect themselves;
- wanting to **build or foster trust** through openness and transparency as it relates to affected individuals or sometimes the public in general; or
- using this as an **opportunity to learn** as engaging with impacted individuals may provide an opportunity to gather feedback, address concerns, and learn from the incident.

Even if a public body head believes a privacy breach does not create a risk of significant harm, the Commissioner may still recommend notifying affected individuals under section 64(5) of ATIPPA, 2015.

How Should a Public Body Notify Affected Individuals?

Under section 64(3) of ATIPPA, 2015, a public body must notify affected individuals at the first reasonable opportunity.

ATIPPA, 2015 does not specify how a public body should notify affected individuals. This means a public body must determine what notification method or methods to use.

In most cases, a public body 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 the public body 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 public body uses indirect notification, it must use a method or methods it reasonably expects will reach affected individuals.

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

Common examples of when a public body 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 the public body undue hardship, such as when the breach impacted a very large number of individuals and the public body 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 the public body 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 public body'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 public body after reviewing the form. In this case, after filing the form, the public body will not receive any requests or communications from OIPC about the privacy breach.

If the public body did not notify affected individuals, the Commissioner may recommend it do so under section 64(5) of ATIPPA, 2015. If recommended, the APA will notify the public body's Contact Person and request confirmation of notification.

A privacy breach may result in affected individuals filing a privacy complaint with OIPC or an own motion privacy complaint investigation pursuant to section 73 of ATIPPA, 2015, although most breach reports (particularly minor ones) do not result in either. The **Reporting a Privacy Breach Form** a public body submits to OIPC may be used in OIPC's investigation of a privacy

complaint. An APA will notify the public body's Contact Person in writing in the event of a privacy investigation. For further details on the investigation process, refer to our guidelines Public Body 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
Toll Free: 1-877-729-6309
commissioner@oipc.nl.ca
https://www.oipc.nl.ca