



Office of the Information and Privacy Commissioner (OIPC)  
**Breach Report Form**

---

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal or health information. The most common privacy breach happens when personal or health information about your employees, customers, or patients is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal or health information is stolen or information is mistakenly emailed to the wrong person.

**It is mandatory to report certain privacy breaches to the Commissioner under section 34.1(1) of the *Personal Information Protection Act (PIPA)***; specifically, organizations are required to notify the Commissioner of incidents “involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual.”

Reporting a privacy breach is not mandatory under the *Health Information Act (HIA)* or the *Freedom of Information and Protection of Privacy Act (FOIP)*. Even so, reporting a breach to the OIPC is a good practice for the following reasons:

- A decision to notify the OIPC is viewed as a positive action by the public. It tells your clients and the public that you view the protection of personal or health information as an important and serious matter. This may enhance public/client confidence.
- The OIPC can provide advice or guidance in responding to the incident.
- It will assist the OIPC in responding to inquiries made by the public and managing any complaints that may be received as a result of the breach.

When reporting a privacy breach to the OIPC, it is important to do so **without unreasonable delay** (PIPA section 34.1(1)), or **as soon as possible**, so that the OIPC can respond in a timely way. Although you may not have all the details relating to the incident, additional information may follow your initial report to the OIPC, or may be requested by the Commissioner.

**For organizations that are subject to PIPA, a report to the Commissioner must be written, and must include the specific information set out in section 19 of the *PIPA Regulation*.**

Custodians and public bodies that are regulated by the HIA and FOIP respectively may report a privacy breach to the OIPC in various ways: verbally, by letter, or by completing the attached Breach Report Form. Organizations subject to PIPA can also use the Breach Report Form to notify the Commissioner. Information elements that **MUST be included in a PIPA organization’s report** to the Commissioner appear in red on the Breach Report Form, and are also marked with an asterisk (\*).

When completing the Breach Report Form, please provide as much information as possible. If necessary, attach additional pages.

Once completed, submit the Breach Report Form to the OIPC at the address below. It is preferable to submit the form by fax to avoid unreasonable delay.

### **Office of the Information and Privacy Commissioner**

**Calgary (PIPA):** Suite 2460, 801 – 6 Avenue SW  
Calgary, Alberta T2P 3W2  
Fax: (403) 297-2711  
Phone: (403) 297-2728

**Edmonton (FOIP and HIA):** #410, 9925 - 109 Street  
Edmonton, Alberta T5K 2J8  
Fax: (780) 422-5682  
Phone: (780) 422-6860

Toll Free: 1-888-878-4044  
Email: [generalinfo@oipc.ab.ca](mailto:generalinfo@oipc.ab.ca)

Upon receipt of the Breach Report Form, someone from the OIPC will contact you.

It is important to know that reporting a breach does not preclude the OIPC from conducting an investigation of the incident. Additional information may be required and will be gathered after an investigation has been initiated.

Whether or not the breach is reported to the OIPC, the Breach Report Form can be used as an internal assessment and action tool, as it can assist you in understanding what questions to ask about the breach, and what steps need to be taken.

### **Other Resources**

For more information on the key steps to be taken in the event a breach occurs, see *Key Steps in Responding to Privacy Breaches*, available on the OIPC website at [www.oipc.ab.ca](http://www.oipc.ab.ca).

**Additional resources for organizations subject to PIPA** are also available on the OIPC website, and include:

- *OIPC Process for Determining Whether to Require Notification*,
- *Reporting a Breach to the Commissioner*, which sets out the minimum requirements for what must be included in a Report to the Commissioner,
- *Notifying Affected Individuals*, which sets out the minimum requirements for what must be included when notifying individuals of an incident,

Additional PIPA resources are also available on the Access and Privacy, Service Alberta website at [www.pipa.alberta.ca](http://www.pipa.alberta.ca), including *Information Sheet 11: Notification of a Security Breach*.

## Breach Report Form<sup>1</sup>

<b>Report Date:</b>
<b>Contact Information</b>
<b>Name of Organization, Public Body or Custodian:</b>
<b>NAME AND CONTACT INFORMATION for a person who can answer the Commissioner's questions about the breach*</b>
Name: _____
Title: _____
Phone: _____ Fax: _____
Email: _____
Mailing Address: _____
_____
<b>Risk Evaluation</b>
<b>INCIDENT DESCRIPTION*</b>
<b>Describe the circumstances of the breach and its cause*:</b> _____
_____
_____
<b>Date of incident or time period during which the incident occurred*:</b>
_____
Date incident discovered: _____
How was the incident discovered? _____
_____
_____
Location of incident: _____

<sup>1</sup> Adapted with permission from the *Privacy Breach Reporting Form* developed by the Office of the Information and Privacy Commissioner of British Columbia, December 2006.

\* Indicates information that MUST be included by PIPA organizations reporting an incident to the Commissioner when required by section 34.1(1) of PIPA.

**Estimated number of individuals to whom there is a real risk of significant harm as a result of the incident\*:** \_\_\_\_\_

Type of individuals affected

- Client/ customer / patient
- Employee
- Other: \_\_\_\_\_

**PERSONAL INFORMATION INVOLVED\***

**Describe the personal or health information involved in the breach\*** (e.g. name, address, Social Insurance Number (SIN), financial, medical information) and the form it was in (e.g. paper records, electronic database). Do **not** send the OIPC identifiable personal information.

---

---

---

---

---

---

---

---

---

---

**Safeguards**

Describe physical security at the time of the incident (locks, alarm systems, etc.): \_\_\_\_\_

---

---

---

Describe technical security (encryption, passwords, etc.) \_\_\_\_\_

---

---

---

**HARM\***

**Provide an assessment of the type of harm(s) that may result from the breach.\*** Indicate whether the level of harm is considered to be low, medium,

or high/significant.

Level of harm			Type of Harm
L	M	H	
			Identity theft (most likely when the breach includes loss of SIN, credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information and any other information that can be used to commit financial fraud)
			Risk of physical harm (if the loss of information places any individual at risk of physical harm, stalking or harassment)
			Hurt, humiliation, damage to reputation (associated with the loss of information such as mental health records, medical records, disciplinary records)
			Loss of business or employment opportunities (usually as a result of damage to reputation to an individual)
			Breach of contractual obligations (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
			Future breaches due to similar technical failures (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)
			Failure to meet professional standards or certification standards (notification may be required to professional regulatory body or certification authority)
			Other (specify):



**Notification**

Has your Privacy Officer/FOIP Coordinator/Responsible Affiliate been notified?

- Yes Who was notified and when? \_\_\_\_\_
- No When to be notified? \_\_\_\_\_

Have the police or other authorities been notified (e.g. professional bodies or person required under contract)?

- Yes Who was notified and when? \_\_\_\_\_
- No When to be notified? \_\_\_\_\_

**Have affected individuals been notified\*?**

- Yes Form of notification?\*** \_\_\_\_\_
- No When to be notified? \_\_\_\_\_

**Describe any steps taken to notify individuals\*** (e.g. who was notified, the form and content of notification. Please provide a copy of notification to the OIPC).

---

---

---

---

---

---

**Describe any steps that have been taken to reduce the risk of harm to individuals\*** (e.g. recovery of information, locks changed, computer systems shut down)

---

---

---

---

You may wish to provide the OIPC with any additional information you have collected regarding the breach, including:

- internal investigation reports or findings,
- long-term strategies you intend to implement to correct the situation (e.g. staff training, policy development).

As noted above, however, if you intend to seek advice from the OIPC regarding how to respond to the breach and what actions should be taken, you should report the incident **as soon as possible** even where the above information is not yet available. PIPA organizations are required to notify the Commissioner of reportable breaches **without unreasonable delay**.

Once completed, submit the Breach Report Form to the OIPC at the address below. It is preferable to submit the form by fax where timing is an issue.

### **Office of the Information and Privacy Commissioner**

**Calgary (PIPA):**

Suite 2460, 801 – 6 Avenue SW  
Calgary, Alberta T2P 3W2  
Fax: (403) 297-2711  
Phone: (403) 297-2728

**Edmonton (FOIP and HIA):**

#410, 9925 - 109 Street  
Edmonton, Alberta T5K 2J8  
Fax: (780) 422-5682  
Phone: (780) 422-6860

Toll Free: 1-888-878-4044

Email: [generalinfo@oipc.ab.ca](mailto:generalinfo@oipc.ab.ca)