



Reporting a Privacy Breach to the Office of the Information and Privacy Commissioner of Alberta

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 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 mistakenly emailed to the wrong person.

Reporting a privacy breach to the Office of the Information and Privacy Commissioner (OIPC) is not mandatory. However, reporting a breach to the OIPC is a good practice for the following reasons:

- An organization's decision to notify the OIPC on its own initiative is viewed as a positive action by the public. It tells your clients and the public that your organization views the protection of personal or health information as an important and serious matter. This may enhance public/client confidence in your organization.
- 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.

If you are going to report a privacy breach to the OIPC, it is important to do so as soon as possible so that the OIPC can provide timely advice. Although you may not have all the details relating to the incident, additional information may follow your initial report to OIPC.

You may report a privacy breach to the OIPC in various ways: verbally, by letter, or by completing the attached Privacy Breach Report form.

Even if you are not intending to report the breach to the OIPC, the Privacy 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.

When completing the form, please provide as much information as possible. If necessary, attach additional pages. If a question does not apply to your situation, or you do not know the answer to something, please indicate this on the form. Fax the form to either the Calgary or Edmonton OIPC office. Upon receipt of the form, you will be contacted by someone from the OIPC.

It is important to know that reporting a breach does not preclude the OIPC from conducting an investigation of the incident. However, the investigation process is intended to be educational and corrective with a goal of future compliance. Additional information may be required and will be gathered after an investigation has been initiated.

For more information on the key steps to be taken in the event a breach occurs, see *Key Steps in Responding to Privacy Breaches*, produced by the OIPC and available online at www.oipc.ab.ca.

Privacy Breach Report¹

Report Date:
Contact Information
Name of Organization, Public Body or Custodian:
Contact Person
Name: _____
Title: _____
Phone: _____ Fax: _____
Email: _____
Mailing Address: _____

Risk Evaluation
Incident Description
Describe the nature of the breach and its cause: _____

Date of incident: _____
Date incident discovered: _____
How was the incident discovered? _____

Location of incident: _____

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

Estimated number of individuals affected: _____

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 from the breach

Identify the type of harm(s) that may result from the breach:

- 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 (when 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 the notification process (e.g. who was notified, the form and content of notification. Please provide a copy of notification to the OIPC).

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

- steps that have been taken to reduce the risk of harm (e.g. recovery of information, locks changed, computer systems shut down),
- internal investigation reports or findings,
- long-term strategies you intend to implement to correct the situation (e.g. staff training, policy development).

However, as noted above, 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.

Once completed, submit the Privacy 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):

#500, 640 - 5 Avenue SW
Calgary, Alberta T2P 3G4
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