Privacy Breach Checklist for private organizations

Use this form to evaluate your organization's response to a privacy breach.

The form can also be submitted to the OIPC for the purpose of notification. If a question does not apply to your situation, write "N/A." If you do not know the answer, write "unknown." Completed forms can be sent to info@oipc.bc.ca

The preferred method for notifying the OIPC is through the online form:
https://www.oipc.bc.ca/forms/public-bodies/online-privacy-breach-report-form/

Information entered into the online form is secured through encryption in transit and storage.

For more information on reporting a privacy breach, visit:
https://www.oipc.bc.ca/resources/report-a-privacy-breach/

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the *Personal Information Protection Act* (PIPA).

The most common privacy breaches happen when personal information of your patients, customers or employees is stolen, lost or mistakenly disclosed – for example, when a computer is stolen or personal information is mistakenly emailed to the wrong person.

Step 15 of the Checklist will help you decide whether to report the breach to the OIPC.

Contact information

Organization:

Contact Person:

Name:

Preferred pronoun:

Title:

Phone:

Email:

Mailing address:

Risk evaluation

Incident Description

1. Describe the breach and its cause:

2. Date of breach:

3. Date breach came to the attention of the organization:

4. Location of incident:

5. Estimated number of individuals affected:

6. Type of individuals affected:

- ☐ Client/ Customer/ Patient
- ☐ Employee
- ☐ Student
- ☐ Other:

Personal Information Involved

7. Describe the personal information involved (e.g. name, address, SIN, financial, medical): (Do not include or send us identifiable personal information.)

Safeguards

8. Describe physical security measures (locks, alarm systems etc.):

9. Describe technical security measures:

- ☐ Encryption
- ☐ Password
- ☐ Other (Describe):

Describe organizational security measures (security clearances, policies, role-based access, training programs, contractual provisions):

Harm from the breach

10. 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 licence numbers, personal health numbers, debit card numbers with password information and any other information that can be used to commit financial fraud)
- ☐ Bodily harm (when the loss of information places any individual at risk of physical harm, stalking or harassment)
- ☐ Humiliation (associated with the loss of information such as medical records or disciplinary records)
- ☐ Damage to reputation and relationships
- ☐ Loss of employment, business or professional opportunities (usually as a result of damage to reputation to an individual)
- ☐ Financial loss
- ☐ Negative impact of credit record
- ☐ Damage to, or loss of, property
- ☐ 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

11. Has your Privacy Officer been notified?

☐ Yes Who was notified and when? _____

☐ No When to be notified? _____

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

☐ Yes Who was notified and when? _____

☐ No When to be notified? _____

13. Have affected individuals been notified?

☐ Yes Manner of notification: _____
Number of individuals notified: _____
Date of notification: _____

☐ No Why not? _____

14. What information was included in the notification?

☐ Name of organization;

☐ Date the breach came to the attention of the organization;

☐ Date of the breach;

☐ Description of the breach, including identified harms;

☐ Date on which or the period during which the privacy breach occurred;

☐ Description of the personal information involved;

☐ Privacy Commissioner contact information. If the organization has already contacted the Privacy Commissioner, include this detail in the notification letter;

☐ Contact information of an individual within the public body or organization who can answer questions or provide further information;

☐ Description of steps that have been or will be taken to reduce the risk of harm to the affected individual;

- ☐ Description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

15. Should the Office of the Information and Privacy Commissioner be notified of the breach? Consider the following factors:

- ☐ The personal information involved is sensitive;
- ☐ There is a risk of identity theft or other harm including pain and suffering or loss of reputation;
- ☐ A large number of people are affected by the breach;
- ☐ The information has not been fully recovered;
- ☐ The breach is the result of a systemic problem or a similar breach has occurred before;
- ☐ Your organization requires assistance in responding to the privacy breach;
- ☐ You want to ensure that the steps taken comply with the organization's obligations under privacy legislation;
- ☐ If you are reporting this breach to the OIPC, please include a copy of the notification letter.

Prevention

16. Describe the immediate steps taken to contain and reduce the harm of the breach (e.g. locks changed, computer access codes changed or revoked, computer systems shut down):

17. Describe the long-term strategies you will take to correct the situation (e.g. staff training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security):

If you have completed a security audit and are reporting this breach to the OIPC, please forward a copy of the audit with your report.