Privacy Breach Checklist

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 or part 3 of the Freedom of Information and Protection of Privacy Act.

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.

If you are reporting the breach to the OIPC, you must answer every question on this form. If a question does not apply to your situation, write "N/A." If you do not know the answer, write "unknown." Fax a completed copy, including any other necessary information, to (250) 387-1696. The OIPC will contact you after we receive this form.

Use this form to evaluate your public body or organization's response to a privacy breach, and to decide whether to report the breach to the Office of the Information and Privacy Commissioner ("OIPC").

Privacy Breach Checklist

Date of report: _____

Contact information

Public Body / Organization: _____

Contact Person: _____

Name: _____

Title: _____

Phone: _____ Fax: _____

E-Mail: _____

Mailing address: _____

_____

_____

Risk evaluation

Incident Description

1. Describe the nature of the breach and its cause:

_____

_____

_____

2. Date of incident:

_____

_____

_____

3. Date incident discovered:

_____

_____

_____

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)

☐ 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

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?

☐ Date of the breach

☐ Description of the breach

☐ Description of the information inappropriately accessed, collected, used or disclosed

☐ Risk(s) to the individual caused by the breach

☐ Steps taken so far to control or reduce the harm

☐ Future steps planned to prevent further privacy breaches

☐ Steps the individual can take to reduce the harm

☐ Privacy Commissioner contact information

☐ Organization contact information for further assistance

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 or public body requires assistance in responding to the privacy breach
- ☐ You want to ensure that the steps taken comply with the organization's or public body'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.

Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner for British Columbia

PO Box 9038, Stn. Prov. Govt. Victoria, BC V8W 9A4 | Telephone: 250.387.5629 | Toll free in B.C. 1.800.663.7867
E-mail: info@oipc.bc.ca | www.oipc.bc.ca