



PRIVACY BREACH REPORTING FORM

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 *Personal Information Protection Act* or part 3 of the *Freedom of Information and Protection of Privacy Act*. The most common privacy breach happens when personal information of your patients, customers or employees is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong person. Upon receipt of this form, you will be contacted by the OIPC.

Note: *All fields must be completed before you submit this form to the Office of the Information and Privacy Commissioner. Submit the form by fax to (250) 387-1696. If a question does not apply to your situation, or you do not know the answer now, please indicate this. Append added pages if necessary. Upon receipt of this form, you will be contacted by the OIPC.*

Report Date: _____

Contact Information

1. Public Body / Organization: _____

2. 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 (locks, alarm systems etc.)

9. Describe the technical security

- Encryption
 - Password
 - Other (Describe)
-

Harm from the Breach

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

- Identify theft
(most likely when the breach includes loss of S.I.N., 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 / Director/Manager of Information and Privacy (DMIP) 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 Form of notification: _____

No Why not? _____

14. Describe the notification process (e.g. who was notified, the form and content of notification): _____

Please forward a copy of the notification to our office.

Note: A Notification Assessment Tool is available on the OIPC website at: http://www.oipc.bc.ca/pdfs/policy/ipc_bc_ont_breach.pdf

Mitigation and Prevention

15. Describe the immediate steps taken to reduce the harm of the breach (e.g. locks changed, computer systems shut down):

16. Describe the long-term strategies you will take to correct the situation (e.g. staff training, policy development):

If you have completed a security audit please forward to our office.