PRIVACY BREACH REPORTING FORM

Report Date:

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:

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, health care number, financial, medical information), 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.

- Identify theft (most likely when the breach includes loss of health insurance number, credit card 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 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 / 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 and when?
- 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)

Education

What additional education has been developed / provided to review / update policies, procedures, or training to:

- Individuals directly involved in the privacy breach?
- Organization

What sanctions (if any) have been applied to individuals directly involved in the privacy breach?

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

Organizations regulated by PIPA are REQUIRED to notify the Commissioner of any incident 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 as a result of the incident (PIPA section 34.1)

To notify the OIPC about a privacy breach under PIPA, use the reporting form from:

http://www.oipc.ab.ca/Content_Files/Files/Publications/Breach_Report_Form_2010.pdf

References

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

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

This publication provides general guidance for a Medical Office. Consultation with your Information Systems, Health Records, and Privacy Office is recommended. For additional assistance, contact Information Managers.