

MANITOBA OMBUDSMAN PRACTICE NOTE

Practice Notes are prepared by Manitoba Ombudsman to assist persons using the legislation. They are intended as advice only and are not a substitute for the legislation.

Manitoba Ombudsman
750 – 500 Portage Avenue
Winnipeg, Manitoba R3C 3X1
Phone: (204) 982-9130 Toll free 1-800-665-0531
Fax: (204) 942-7803
Web site: www.ombudsman.mb.ca

REPORTING A PRIVACY BREACH TO MANITOBA OMBUDSMAN

A privacy breach occurs when there is unauthorized collection, use, disclosure or destruction of personal or personal health information.¹ Such activity is “unauthorized” if it occurs in contravention of *The Freedom of Information and Protection of Privacy Act* (FIPPA) or *The Personal Health Information Act* (PHIA). The most common privacy breaches happen when personal information about clients, patients, students or employees is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal or personal health information is stolen or the information is mistakenly faxed or emailed to the wrong person.

Reporting a privacy breach to Manitoba Ombudsman can be viewed as a positive action. It demonstrates that the public body or trustee considers the protection of personal and personal health information to be an important and serious matter. Manitoba Ombudsman may be able to assist you in your development of a plan for responding to the privacy breach and ensure steps are taken to prevent breaches from occurring in the future. Your report of the breach also helps us in responding to inquiries made by the public and managing any complaints that are received as a result of the breach. Reporting a privacy breach to Manitoba Ombudsman is not mandatory under FIPPA and PHIA.

The following factors are relevant in deciding whether to report a breach to the Ombudsman:

- the sensitivity of the personal or health information;
- whether the disclosed information could be used to commit identity theft;
- whether there is a reasonable chance of harm to affected individuals from the disclosure including non-financial losses;
- the number of people affected by the breach, and
- whether the information was fully recovered without further disclosure.

¹ This document has been adapted with permission from *Privacy Breach Reporting Form* developed by the Office of the Information and Privacy Commissioner of British Columbia (OIPC BC), December 2006, *Breach Notification Assessment Tool*, jointly produced by the OIPC BC and the Information and Privacy Commissioner of Ontario, December 2006 and *Reporting a Privacy Breach to the Office of the Information and Privacy Commissioner of Alberta* developed by the Office of the Information and Privacy Commissioner of Alberta.

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

You may report a privacy breach to Manitoba Ombudsman in various ways: verbally, by letter or by completing the attached Privacy Breach Reporting Form. Even if you are not intending to report the breach, the Privacy Breach Reporting 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.

It is important to know that reporting a breach does not preclude Manitoba Ombudsman 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 would be gathered after an investigation has been initiated.

For more information on the steps to be taken in the event a breach occurs, see our Practice Note *Key Steps in Responding to Privacy Breaches*.

PRIVACY BREACH REPORTING FORM

If you intend to seek the advice of Manitoba Ombudsman regarding how to respond to the breach and determine what actions should be taken, you should report this incident as soon as possible even where all of the information is not yet known.

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. If you have any questions about completing the form, contact us at 982-9130 or toll free 1-800-665-0531.

This form may be submitted by mail to:

Manitoba Ombudsman
750 – 500 Portage Avenue
Winnipeg, MB R3C 3X1

If it is preferable to submit the form by fax where timing is an issue, the fax number for Manitoba Ombudsman is (204) 942-7803.

Upon receipt of the form, you will be contacted by our office.

REPORT DATE: _____

CONTACT INFORMATION

Name of public body or trustee: _____

Program/Department: _____

Contact person

Name: _____

Title: _____

Phone: _____ Fax: _____

Mailing Address: _____

INCIDENT DESCRIPTION

Date of incident: _____

Date incident was discovered: _____

How was the incident discovered? _____

Location of incident? _____

Describe the breach and its cause: _____

CONTAINMENT OF THE BREACH

Describe the steps that have been taken to reduce the risk of harm (e.g. recovery of information, locks changed, computer systems shut down). Provide a copy of any internal investigation reports or findings about the incident.

RISK EVALUATION

Individuals Affected by the Breach

Estimated number of individuals affected: _____

Type of individuals affected:

Client/patient/student

Employee

Other: _____

Personal or Personal Health Information Involved

Describe the personal or personal 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** include or send us identifiable personal or personal health information.

Safeguards

Describe the physical security at the time of the incident (locks, alarm systems, etc.)

Describe the technical security (encryption, passwords, etc.)

Identify any relevant security policies or procedures (attach excerpts)

Harm from the Breach

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

- Identity theft (most likely when the breach includes the loss of Social Insurance Numbers (SIN), credit card information, driver's license numbers, Personal Health Information Numbers (PHIN), 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 medical records or employee disciplinary records)
- Loss of business or employment opportunities (usually as a result of damage to reputation of 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/Access and Privacy Coordinator/Access and Privacy Officer been notified?

- Yes Who was notified and when? _____
- No When to be notified? _____

Have the police or other authorities been notified?

- Yes Who was notified and when? _____
- No Why not? _____

Have the affected individuals been notified?

- Yes Form of notification? _____
- No Why not? _____

Describe the notification process (e.g. who was notified, the form and content of notification). Please provide a copy of the notification with the affected individuals' identities removed.

PREVENTION

Describe long-term strategies you intend to implement to correct the situation (e.g. staff training, change in policy or procedure).

