

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

KEY STEPS IN RESPONDING TO PRIVACY BREACHES UNDER *THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA)* AND *THE PERSONAL HEALTH INFORMATION ACT (PHIA)*

Purpose

The purpose of this document is to provide guidance to public bodies and trustees when a privacy breach occurs.¹

What is a privacy breach?

A privacy breach occurs when there is unauthorized collection, use, disclosure or destruction of personal or personal health information. Such activity is “unauthorized” if it occurs in contravention of FIPPA or 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 information is mistakenly faxed or emailed to the wrong person.

Reporting privacy breaches

Manitoba Ombudsman has created a Privacy Breach Reporting Form that allows public bodies and trustees to complete an analysis of the privacy breach using the four key steps described below. This form is contained in our Practice Note *Reporting a Privacy Breach to Manitoba Ombudsman* and is available on our web site.

Four key steps in responding to a privacy breach

The most important step you can take is to respond immediately to the breach. You should undertake steps 1, 2 and 3 outlined below immediately following the breach and do so simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies.

¹This document was adapted with permission from *Key Steps in Responding to Privacy Breaches* and *Privacy Breach Reporting Form*, developed by the Office of the Information and Privacy Commissioner of British Columbia (OIPC BC), December 2006, and *Breach Notification Assessment Tool*, jointly produced by the OIPC BC and the Information and Privacy Commissioner of Ontario, December 2006, as well as *Key Steps in Responding to Privacy Breaches* and *Privacy Breach Report* form developed by the Office of the Information and Privacy Commissioner of Alberta.

STEP 1: CONTAIN THE BREACH

Take immediate common sense steps to limit the breach. These steps include:

- Immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, revoking access or correcting weaknesses in physical security
- Immediately contact your Privacy Officer, Access and Privacy Coordinator, Access and Privacy Officer and/or the person responsible for security in your organization.
- Notify the police if the breach involves suspected theft or other criminal activity.

STEP 2: EVALUATE THE RISKS ASSOCIATED WITH THE BREACH

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following:

(i) PERSONAL OR PERSONAL HEALTH INFORMATION INVOLVED

- What data elements have been breached? Generally, the more sensitive the information, the higher the risk. Health information, Social Insurance Numbers (SIN) and financial information that could be used for identity theft are examples of sensitive information.
- What possible use is there for the information? Can the information be used for fraudulent or otherwise harmful purposes?

(ii) CAUSE AND EXTENT OF THE BREACH

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- Is the information encrypted or otherwise not readily accessible?
- What steps have you already taken to minimize the harm?

(iii) INDIVIDUALS AFFECTED BY THE BREACH

- How many individuals are affected by the breach?
- Who was affected by the breach: clients, patients, students, employees, contractors, service providers, other organizations?

(iv) FORESEEABLE HARM FROM THE BREACH

- Is there any relationship between the affected individuals and the unauthorized recipients?
- What harm to the affected individuals could result from the breach? Harm may include:
 - security risk (e.g. physical safety)
 - identity theft or fraud
 - loss of business or employment opportunities

- hurt, humiliation, damage to reputation or relationships
- What harm could result to the public body or trustee as a result of the breach? For example:
 - loss of trust in the public body or trustee
 - loss of assets
 - financial exposure
- What harm could result to the public as a result of the breach? For example:
 - risk to public health
 - risk to public safety

STEP 3: NOTIFICATION

Notification can be an important mitigation strategy in the appropriate circumstances. A key consideration in deciding whether to notify should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal or personal health information has been inappropriately collected, used or disclosed. Review your risk assessment in step 2 to determine whether or not notification is required.

If the breach occurs at a third party entity that has been contracted to maintain or process personal or personal health information, the breach should be reported to the originating public body or trustee. When notification is being provided, it is the responsibility of public bodies or trustees to notify the affected individuals when a privacy breach occurs.

(i) NOTIFYING AFFECTED INDIVIDUALS

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- **Legislation requires notification:** Is the public body or trustee covered by legislation that requires notification of the affected individual? Note that FIPPA and PHIA do not require notification.
- **Contractual obligations require notification:** Does the public body or trustee have a contractual obligation to notify affected individuals in the case of a privacy breach?
- **Risk of identity theft or fraud:** How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with Social Insurance Numbers (SIN), credit card numbers, driver's license numbers, Personal Health Information Numbers (PHIN), debit card numbers with password information or any other information that can be used for fraud by third parties (e.g. financial).
- **Risk of physical harm:** Does the privacy breach place any individual at risk of physical harm, stalking or harassment?
- **Risk of hurt, humiliation or damage to reputation:** Could the privacy breach lead to hurt, humiliation or damage to an individual's reputation? This type of harm can occur with the loss of information such as medical records or disciplinary records.
- **Risk of loss of business or employment opportunities:** Could the privacy breach result in damage to the reputation of an individual, affecting business or employment opportunities?

(ii) WHEN AND HOW TO NOTIFY

When?

When notification is being provided to individuals affected by the breach, this should occur as soon as possible following the breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How?

The method of notification will depend on the circumstances. Using multiple methods of notification in certain cases may be the most effective approach. The following sets out factors to consider in deciding how to notify the affected individuals.

Direct Notification

The preferred method of notification is direct – by telephone, letter or in person – to affected individuals. This method is preferred where:

- the identities of individuals are known,
- current contact information for the affected individuals is available,
- individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach, and/or
- individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.).

Indirect Notification

Providing indirect notification – posted notices, web site information, media – may be appropriate in some circumstances. This should generally occur only where:

- direct notification could cause further harm, is prohibitive in cost or contact information is lacking, and/or
- a very large number of individuals are affected by the breach such that direct notification could be impractical.

What Should be Included in the Notification?

Notifications should include the following information:

- Date of the breach;
- General description of the breach;
- Description of the information inappropriately collected, used or disclosed (e.g. name, credit card numbers, SINS, medical records, financial information, etc.);
- The steps taken so far to mitigate the harm;
- Next steps planned and any long term plans to prevent future breaches;
- Steps the individual can take to further mitigate the risk of harm. Provide contact information for credit reporting agencies (to set up a credit watch) and for changing a Personal Health Information Number (PHIN) or driver's license number.
- Contact information of someone within the public body or trustee who can answer questions or provide further information;
- Information on how to contact or complain to Manitoba Ombudsman.

(iii) OTHERS TO CONTACT

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed:

- **Police:** If theft or other crime is suspected
- **Insurers or others:** If required by contractual obligations
- **Professional or other regulatory bodies:** If professional or regulatory standards require notification of these bodies
- **Technology suppliers:** If the breach was due to a technical failure and a recall or technical fix is required.
- **Manitoba Ombudsman:** 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 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.

Reporting a privacy breach to Manitoba Ombudsman can be viewed as a positive action. It demonstrates that the public body or trustee views the protection of personal and personal health information as an important and serious matter. Manitoba Ombudsman may be able to assist you in developing a procedure for responding to the privacy breach and ensuring steps are taken to prevent breaches from occurring in the future. It will also assist us in responding to inquiries made by the public and managing any complaints that are received as a result of the breach.

To notify the Ombudsman, you may wish to use the Privacy Breach Reporting Form contained in our Practice Note *Reporting a Privacy Breach to Manitoba Ombudsman* located on our web site.

STEP 4: PREVENTION

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long term safeguards against further breaches. Policies should be reviewed and updated to reflect the lessons learned from the investigation and regularly after that. Your resulting plan should also include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented. Staff should be trained to know about their responsibilities under FIPPA and PHIA.