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 or 1-800-665-0531
Fax: 204-942-7803
Website: 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]

Public bodies and trustees that are developing a privacy breach policy or procedure may find it helpful to incorporate some of this information.

What is a privacy breach?

A privacy breach occurs when there is unauthorized collection, use, disclosure or disposal of personal or personal health information. Such activity is "unauthorized" if it is not permitted by FIPPA or PHIA. Privacy breaches can occur in various ways including when personal or personal health information about clients, patients, students or employees is stolen, lost or mistakenly disclosed. Examples include the loss or theft of mobile devices (ex: laptop, USB stick) or misdirected communication (ex: fax, email, mail).

Privacy breaches can also be intentional, such as when personal or personal health information has been accessed, used or disclosed by an employee without authority to do so under FIPPA and PHIA.

[1] This document was adapted with permission from *Privacy Breaches: Tools and Resources*, developed by the Office of the Information and Privacy Commissioner (OIPC) of British Columbia, March 2012, *Breach Notification Assessment Tool*, jointly produced by the OIPC of BC and the OIPC of Ontario, December 2006, *Key Steps in Responding to Privacy Breaches* and *Privacy Breach Report* form developed by the OIPC of Alberta, July 2012 and *Keys Steps to Responding to Privacy Breaches* developed by the OIPC of Nova Scotia, March 2015.

Four key steps in responding to a privacy breach

There are four key steps to consider when responding to a suspected or actual privacy breach. The steps are as follows:

1. Contain the breach
2. Evaluate the risks associated with the breach
3. Notify affected individuals and others
4. Prevent further breaches

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 suggestions for longer-term solutions and prevention strategies.

STEP 1: CONTAIN THE BREACH

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

- 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.
- Contact your privacy officer, access and privacy coordinator, access and privacy officer, senior management and/or the person responsible for security in your organization.
- Notify the police if the breach involves suspected theft or other criminal activity.
- Be careful not to destroy information related to the privacy breach that may be valuable in determining the cause or that will allow you to take appropriate corrective action.

STEP 2: EVALUATE THE RISKS ASSOCIATED WITH THE BREACH

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

Personal or personal health information involved

- What personal and/or personal health information 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.

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?

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 of the information?
- Is there a risk of further access, use or disclosure of information?

- Is there a risk of ongoing or further exposure of the information?
- Has the information been recovered?
- Is the information encrypted or otherwise not readily accessible?
- What steps have you already taken to minimize the harm?

Possible harm from the breach

- Is there any relationship between the affected individuals and the unauthorized recipients?
- Could the affected individuals be considered to be vulnerable? For example, youth or seniors.
- What possible use is there for the information? Can the information be used for fraudulent or otherwise harmful purposes?
- What harm to the affected individuals could result from the breach? Harm may include:
    - physical or mental harm
    - identity theft or fraud
    - loss of business or employment opportunities
    - hurt, embarrassment, damage to reputation or relationships
    - potential discriminatory action taken against individual

An assessment of all the risks described above will inform your decision about whether or not to notify an affected individual(s). The following tables are intended to assist in the assessment of risk to affected individuals.

The table on the next page summarizes the risk factors and suggests *possible* risk rating for each risk factor. The table provides examples of the risk factors and how they may be assessed; however, each public body and trustee must make their own assessment of the risks given the unique circumstances of the situation. The table is intended to provide some general guidance for ratings, but is not an exhaustive list.

Risk Rating Overview

Risk Factor	Low	Medium	High
Nature of personal and/or personal health information	▪ Publicly available personal information not associated with any other information	▪ Personal information unique to the organization that is not medical or financial information	▪ Medical, psychological, counselling, or financial information or unique government identification number ▪ Information relates to a vulnerable individual (ex. youth or seniors)
Scope of the breach	▪ Very few affected individuals	▪ Identified and limited group of affected individuals	▪ Large group or entire scope of group not identified
Relationships	▪ Accidental disclosure to another professional who reported the breach and confirmed destruction or return of the information	▪ Accidental disclosure to a stranger who reported the breach and confirmed the destruction or return of the information	▪ Used by or disclosed to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to ex-partners, family members, neighbours or co-workers ▪ Theft by a stranger
Cause of the breach	▪ Technical error that has been resolved	▪ Accidental loss or disclosure	▪ Intentional breach ▪ Cause unknown ▪ Technical error (if not resolved)
Containment efforts	▪ Data was adequately encrypted ▪ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping ▪ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread	▪ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping ▪ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed	▪ Data was not encrypted ▪ Data files, or device have not been recovered ▪ Data at risk of further disclosure particularly through media or online
Possible harm from the breach	▪ No foreseeable harm from the breach	▪ Loss of business or employment opportunities ▪ Hurt, embarrassment, damage to reputation or relationships ▪ Social/relational harm ▪ Loss of trust in the public body/trustee ▪ Loss of public body/trustee assets ▪ Loss of public body/trustee contracts or business ▪ Financial or legal exposure to public body/trustee	▪ Security risk (ex. physical safety) ▪ Identify theft or fraud risk ▪ Hurt, embarrassment, damage to reputation may also be high risk depending on the circumstances ▪ Risk to public health or safety

Risk Evaluation Summary

Potential harm from the privacy breach is often the key factor used in deciding whether or not to notify affected individuals. In general, a medium or high risk rating should result in notification to the affected individuals. A low risk rating may also result in notification depending on the unique circumstances of each case. For each of the factors reviewed above, determine the risk rating.

Risk Factor	Low	Medium	High
Nature of personal and/or personal health information			
Relationships			
Cause of the breach			
Scope of the breach			
Containment efforts			
Foreseeable harm from the breach			
Other factors			
Overall risk rating			

STEP 3: NOTIFY AFFECTED INDIVIDUALS AND OTHERS

Notification to affected individuals can be an important risk 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 to proceed with notification.

If the privacy breach occurs with 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.

Notifying Affected Individuals

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. There may be other factors that influence a decision to notify individuals, such as wanting to be transparent about the breach.

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 event of a privacy breach?
- **Risk of identity theft or fraud**: Identity theft or fraud is a concern if the breach includes information such as names in conjunction with SIN, credit card number, driver's licence number, Personal Health Identification Number (PHIN), or any other information that can be used for fraud by third parties (ex: financial).

- **Risk of physical or mental harm**: Does the privacy breach place any individual at risk of physical or mental harm, stalking or harassment?
- **Risk of hurt, embarrassment or damage to one's reputation**: Could the privacy breach lead to hurt, embarrassment or damage to an individual's reputation? This type of harm can occur with the loss of information such as mental health records, 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?
- **Intentional breach**: In the case of an intentional breach, the affected individual may be in the best position to assess risks and take steps to mitigate them. The perpetrator of the breach may not fully disclose their motivation or their relationship to the individual (ex: ex-partner, family member, neighbour).

When and How to Notify Affected Individuals

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.

On very rare occasions medical evidence may indicate that notification could reasonably be expected to result in immediate and grave harm to the individual's mental or physical health. In those circumstances, consider alternative approaches, such as having the physician give the notice in person or waiting until the immediate danger has passed.

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
- 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, website information or 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

- a very large number of individuals are affected by the breach such that direct notification could be impractical

Indirect notification may also be used in conjunction with direct notification.

Manitoba Ombudsman has created a practice note, *Privacy Breach Notification Letter Checklist*, that outlines what information to include in a notification letter to an affected individual.

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

Reporting Privacy Breaches to Manitoba Ombudsman

Reporting a privacy breach to Manitoba Ombudsman is not mandatory under FIPPA and PHIA. However, we encourage reports to our office where there may be a risk of harm to the affected individual(s). 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 information could be used to commit identity theft or fraud
- whether there is a reasonable risk of harm to affected individuals, including damage to their reputation or relationships, physical or mental harm, embarrassment, hurt or humiliation
- the number of people affected by the breach

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 above. 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.

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 ensuring 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, managing any complaints that are received as a result of the breach and assists us in determining the type of response required by Manitoba Ombudsman, such as an informal discussion or the initiation of an investigation.

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.

STEP 4: PREVENT FURTHER BREACHES

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 physical safeguards (ex: locked cabinets or doors, alarms, visitor access controls), technical safeguards (ex: encryption, passwords, user access) and administrative safeguards (ex: review of policies, privacy training). 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 breach. 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.

Revised November 2018