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.

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)

The purpose of this practice note is to provide guidance to public bodies and trustees about responding to a privacy breach. Amendments to FIPPA and PHIA in January 2022 place requirements on public bodies and trustees to notify individuals affected by a privacy breach when a real risk of significant harm has been determined to have been created for those individuals.

This practice note also provides guidance to public bodies and trustees about fulfilling the requirement to notify Manitoba Ombudsman of a privacy breach including guidance on completing our office's Privacy Breach Reporting Form.

What is a privacy breach?

Both FIPPA and PHIA define a privacy breach, in relation to personal or personal health information, as:

- theft or loss, or
- access, use, disclosure, destruction or alteration in contravention of the acts

A privacy breach 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).

Table of contents

What is a privacy breach?	1
What do you do when a privacy breach happens?	2
Step 1: Contain the breach	2
Step 2: Evaluate the risks	3
Sensitivity	3
Probability of harm	4
Step 3: Notify and report	5
Notifying affected individuals	5
Reporting privacy breaches to Manitoba Ombudsman	9
Step 4: Prevent future breaches	10

Privacy breaches can also be intentional:

- such as when personal or personal health information has been accessed, used, disclosed, destroyed or altered without authority to do so under FIPPA and PHIA. Examples include snooping, hacking, phishing, and ransomware.

What do you do when a privacy breach happens?

The most important step you can take is to respond immediately to the breach. The four steps below can help guide your response.

Four key steps in responding to a privacy breach:

1. **Contain the breach**
2. **Evaluate the risks associated with the breach**
3. **Notify and report**
4. **Prevent future breaches**

You should undertake steps 1, 2 and 3 – contain, evaluate and notify – as soon as possible following identification that a privacy breach has occurred. Step 4 – prevent future breaches – provides suggestions for longer-term solutions and prevention strategies.

Step 1: Contain the breach

Take immediate common-sense steps to contain or limit the breach. These steps may include:

- Stopping an unauthorized practice, such as ceasing transmission of email or correspondence to an incorrect recipient.
- Removing, moving or isolating exposed information or files, to prevent further unauthorized access or disclosure.
- Retrieving any documents or copies of documents that were wrongfully disclosed or taken by an unauthorized person.
- Conducting physical searches for records that were lost or stolen.
- Returning physical records to their original location or providing them to the intended recipient.
- Requesting and verifying that an unintended recipient double deleted all affected email, correspondence and records.
- Shutting down the system that was breached or correcting weaknesses in security.
- Revoking access to the system.
- Changing passwords.
- Contacting the person responsible for security in your organization so that further security measures can be put in place.

Step 2: Evaluate the risks associated with the breach

As of January 1, 2022, under both FIPPA and PHIA, when a public body or trustee determines that a privacy breach creates a *real risk of significant harm* to affected individuals, the public body or trustee *must* provide notification of the breach to the affected individuals and to the ombudsman.

A thorough evaluation of the *real risk of significant harm* is critical for public bodies and trustees. The evaluation will determine your next steps in your response to the breach, and will also dictate if notification to affected individuals and the ombudsman is required under the acts.

To consider what steps are necessary take in response to a breach, public bodies and trustees need to determine if the privacy breach created a *real risk of significant harm* for affected individuals. The acts define the term *significant harm* and provide examples of harm which can impact an individual:[1]

- bodily harm
- humiliation
- damage to the individual's reputation or relationships
- loss of employment, business or professional opportunities
- financial loss
- identity theft
- negative effects on the individual's credit rating or report
- damage to or loss of the individual's property

The regulations also list the factors that must be considered in your determination of whether the breach created a real risk of significant harm.[2] Please review the applicable FIPPA or PHIA Regulation for certainty. The summary below lists these factors and important questions to take into account.

Sensitivity

The personal and personal health information involved

- What personal and or personal health information has been breached? Generally, the more sensitive the information, the higher the risk of significant harm to individuals affected. Health information, Social Insurance Numbers (SIN) and financial information that could be used for identity theft are examples of very sensitive information.

[1] See FIPPA 41.1(1) and PHIA 19.0.1(1)

[2] See FIPPA regulation 3.1 and PHIA regulation 8.7

Probability of harm

Cause and extent of the breach

- What are the circumstances that caused the privacy breach and is there evidence of any malicious intent, such as the breach being the result of theft or gaining unauthorized access to a computer system? Was the information deliberately accessed by an employee for a non-work-related purpose? Or, was the breach accidental?
- How many people actually or potentially accessed the information? Are their identities known?
- Is there any known relationship between any of the people who actually or potentially accessed the information and the individual(s) to whom the information relates? What is the nature of that relationship?

Individuals affected by the breach

- How many individuals are affected?
- Who was affected: clients, patients, students, employees, contractors, service providers?
- Were potentially vulnerable individuals affected: children or youth, individuals with disabilities, the elderly?

Security of the personal or personal health information

- Is the public body or trustee reasonably satisfied that any person who actually or potentially accessed the information has destroyed any unauthorized copies of it and has committed to not use or disclose it?
- When did the breach first occur and for what length of time was the information available to be accessed, used or disclosed, destroyed or altered?
- Is there a risk of ongoing or further exposure of the information? Is there a risk of further unauthorized access, use or disclosure of the information?
- What is the amount of information involved?
- Has the information been recovered?
- Was the information adequately encrypted, anonymized or otherwise not easily accessible?

Evidence of harm from the breach

- Has harm already materialized (such as what is described under the definition of significant harm)?

An assessment of all the risk factors described under the applicable regulations, as summarized above, will inform your decision regarding whether there is a real risk of significant harm to an individual created as a result of a privacy breach.

When making a determination that a breach creates a real risk of significant harm, it is important to note that:

- The determination is based on the sensitivity of the personal or personal health information involved, along with the probability that the personal or personal health information could be used to cause significant harm to the individual(s).
- The term "significant" is used because there must be some risk of damage, detriment, or injury to the individual that is significant in nature.
- The description of "real" in relation to risk means that there must be a strong evidence to indicate that the information in question has been or will be misused. The "real risk of significant harm" should not be interpreted as a vague possibility or mere speculation or conjecture.

Manitoba Ombudsman has updated our privacy breach resources for public bodies and trustees. Our *Privacy Breach Risk Rating Tools* now include the risk factors noted in the regulations and may suggest a ***possible*** risk rating for each risk factor. The FIPPA and PHIA tools each provide examples of the risk factors, within a range and how they may be assessed. It is important to emphasize that each public body and trustee must make their own assessment of the risks given the unique circumstances of each breach situation. The tools are intended to provide general guidance to ratings, but are not exhaustive.

Again, a thorough assessment of the real risk of significant harm is critical for public bodies and trustees. The assessment will determine your next steps in your response to the breach, and will also dictate if notification to affected individuals and the ombudsman is required under the acts.

Step 3: Notify and Report

Notifying affected individuals[3]

As of January 1, 2022, under both FIPPA and PHIA, when a public body or trustee determines that a privacy breach creates a real risk of significant harm to affected individuals, the public body or trustee *must* provide notification of the breach to the affected individuals and to the ombudsman.

Notification to the affected individuals is mandatory under FIPPA and PHIA if a privacy breach creates a real risk of significant harm to affected individuals. Notification can also be an important risk mitigation strategy in the appropriate circumstances, whether it is deemed mandatory or not. A key consideration in deciding whether to notify affected individuals should be whether notification is necessary to avoid or mitigate harm to an individual whose personal or personal health information has been affected by the privacy breach.

[3] See FIPPA 41.1(2) and PHIA 19.0.1(2)

Notification to an affected individual may also help you to more accurately assess the risk of harm, as the individual may share information about possible harms that you would not otherwise be aware of. Review your risk assessment in step 2 to determine whether or not to proceed with notification.

There may be other factors that influence a public body or trustee's decision to notify individuals about a privacy breach, such as a policy, contractual obligation or a commitment to be transparent.

Note that the amendments to Manitoba's privacy legislation in 2022 make it **mandatory** for public bodies and trustees to notify affected individuals of a privacy breach if the breach could reasonably be expected to create a real risk of significant harm to the affected individuals.

A third-party entity, contracted to maintain or process personal or personal health information, should work together with the public body or trustee to determine the real risk of significant harm and to notify affected individuals and Manitoba Ombudsman when a privacy breach occurs.

When and how to notify affected individuals

When?

When **mandatory** notification is being provided to individuals affected by the breach, because the public body or trustee has determined that a real risk of significant harm has been created, FIPPA and PHIA require that the notification be given **as soon as is practicable.**[4]

If a public body is not mandated to provide notification, but chooses to notify individuals affected by a privacy breach – to be transparent, out of caution for any level of risk to individuals, or because it is their practice or policy to do so – this should also occur as soon as is practicable or reasonable.

If a public body or trustee has contacted law enforcement authorities about the breach, the public body should discuss the timing of notification with those authorities to ensure that notification does not inadvertently impede a criminal investigation.

How?

When **mandatory** notification is being provided to individuals affected by the breach, the acts require that the notification contain both specific information and be given in a specific form and manner as set out in the regulations. The regulations indicate that notification must be in **writing and include:**[5]

[4] See FIPPA 41.1(3) and PHIA 19.0.1(3)

[5] See FIPPA regulation 3.2(1) and PHIA regulation 8.8(1)

- A description of the circumstances of the privacy breach.
- The date or period of time that the privacy breach occurred, or is believed to have occurred.
- The name of the public body or trustee who had custody or control of the personal or personal health information at the time of the privacy breach.
- A description of the personal or personal health information that was the subject of the privacy breach.
- A description of the steps that the public body or trustee has taken or is intending to take, as of the date of the notice,
    - to reduce the risk of harm to be individual as a result of the privacy breach and
    - to reduce the risk of a similar privacy breach in future.
- A description of the steps that the individual can take to reduce the risk of harm that could result from the privacy breach or to mitigate that harm.
- A statement that Manitoba Ombudsman has or will be given notice about the privacy breach, as required under subsection 19.0.1(4) of PHIA or subsection 41.1(4) of FIPPA.
- The name or contact information of an officer or employee of the public body or trustee who is able to answer questions about the privacy breach.
- Any other information that the public body or trustee considers relevant.

Our revised *Privacy Breach Notification Checklist* summarizes these notification requirements.

A mandatory notification under the acts also requires that the notice to the individual be given **directly,** except in specific circumstances as described in the regulations (see "exceptions to the rule" below for the required form and manner of indirect notification required by the regulations).

Direct notification of individuals in writing is the best practice when the following apply:

- 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.)

Exceptions to the rule

While direct notification to individuals in writing may be required and/or best practice, there are exceptions under FIPPA and PHIA under specific circumstances:

1. If a public body or trustee reasonably believes that the **delay** necessary to provide written notice is likely to significantly increase a real risk of significant harm to the individual, the public body or trustee ***may*** give the notice orally, provided:[6]

[6] See FIPPA regulation 3.2(2) and PHIA regulation 8.8(2)

(a) at the time the oral notice is given, the public body or trustee records the information that was given and the date on which it was provided, or
(b) the public body or trustee gives notice in writing in accordance with subsection (1) within a reasonable time after the oral notice is provided

2. A notice can be given **indirectly** to one or more individuals in the following circumstances:
   - if the public body or trustee reasonably believes that the privacy breach may result in a risk to public health or safety
   - if the identify or current contact information of the affected individual is not known
   - if the public body or trustee reasonably believes that giving notice directly and in writing:
     - is impractical or unduly expensive because of the large number of individuals that may have been affected by the privacy breach, or
     - could threaten or harm the affected individual's mental or physical health[7]

3. In circumstances where indirect notice is permitted, it must be given:
   - by public communication or similar measure that:
     - can be reasonably expected to reach the affected individual or individuals, and
     - does not include any information that could reasonably identify the affected individual or individuals, or
   - if the notice of the privacy breach can be reasonably expected to threaten or harm the recipient's mental or physical health, notification must be provided in writing to an individual who provides care to the recipient or an individual with whom the recipient is known to have a close personal relationship[8] (for example, notification could be given to an affected individual's physician, service provider, parent or guardian, or caregiver)

Examples of public communication include posting a notice on a public body or trustee's website, on social media, in a common or public area of a building or community, or by distributing a news release. Note that the public communication avenues should be selected based on the likelihood of reaching the affected individuals. Multiple methods of public notification may be the most effective way to notify all affected individuals.

[7] See FIPPA regulation 3.3(1) and PHIA regulation 8.8.1(1)
[8] See FIPPA regulation 3.3(2) and PHIA regulation 8.8.1(2)

Reporting privacy breaches to Manitoba Ombudsman

If your assessment determines that the privacy breach does not create a *real risk of significant harm* to the affected individuals, then the privacy breach does not have to be reported to Manitoba Ombudsman. However, we encourage reports to our office where there may be a risk of harm to the affected individual(s) and you are unsure about whether a real risk of significant harm has resulted and/or consultation would be helpful.

When making a report of a privacy breach to Manitoba Ombudsman, the legislation requires that it be in the form and manner determined by our office. Therefore, our office has created a Privacy Breach Reporting Form. Please ensure that you use this form available on our website to report a privacy breach as it will help ensure that you provide our office with the information we need.

Why notify Manitoba Ombudsman of a privacy breach?

In addition to fulfilling mandatory reporting obligations, reporting a privacy breach to Manitoba Ombudsman can be viewed as a positive action:

- The act of notifying affected individuals, as well as the ombudsman, of a privacy breach is a fundamental indicator of a privacy-respectful organizational culture.
- It demonstrates that the public body or trustee considers the protection of personal and personal health information to be an important and serious matter.
- We 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 intervention required by our office 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 later.

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.

Step 4: Prevent Future Breaches

After steps are taken to mitigate the risks associated with the breach, a public body or trustee should undertake a thorough investigation into the cause of the breach. This could require a security audit of physical safeguards, technical safeguards, and administrative safeguards, such as:

Physical safeguards – locked cabinets or doors, alarms, visitor access
Technical safeguards – encryption, passwords, user access
Administrative safeguards – review of policies, privacy training

Once an investigation into the cause and extent of the breach is completed, adequate long-term safeguards against further breaches should be developed. A list of commonly used safeguards can be found on the Manitoba Health and Seniors Care website.[9]

Additionally, policies should be reviewed and updated on a regular basis to reflect the lessons learned from the breach. Your resulting plan should include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

Finally, staff should be trained to know about their responsibilities under FIPPA and PHIA and training should be refreshed periodically.

Revised January 2022

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, and *Breach Notification Assessment Tool*, jointly produced by the OIPC 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, 2018; *Keys Steps to Responding to Privacy Breaches* developed by the OIPC of Nova Scotia, March 2015 and *Privacy Breach Guidelines for Government Institutions and Local Authorities*, developed by the Information and Privacy Commissioner (OIPC) of Saskatchewan, September 2021. We are particularly indebted to the Office of the Privacy Commissioner of Canada (OPC) and the OIPC Alberta for their support and assistance in our preparation for the amendments to Manitoba public sector laws relating to privacy breach reporting.

[9] https://www.gov.mb.ca/health/phia/docs/security_safeguards.pdf