FIPPA and PHIA Privacy Breach Reporting Form

This reporting form is to be used only by public bodies and trustees for the purposes of reporting a privacy breach to Manitoba Ombudsman. This form satisfies the legislative requirement to report the privacy breach to our office. If your organization has a similar internal breach reporting form, you may submit that to our office in lieu of, or in addition to, our reporting form.

"Privacy breach" means, in relation to personal or personal health information: theft or loss; or access, use, disclosure, destruction or alteration in contravention of these acts.

As of January 1, 2022, amendments to the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Act (PHIA) require that public bodies and trustees provide notification to individuals affected by a privacy breach and to Manitoba Ombudsman, when a public body or trustee determines that the breach has created a real risk of significant harm for the individuals affected.

When completing this Privacy Breach Reporting Form:

- Refer to our practice note for public bodies and trustees, *Key Steps in Responding to a Privacy Breach under FIPPA and PHIA*, which contains information that can help you understand the questions that are included in the form and how they are relevant to your obligations under FIPPA and PHIA.
- Provide as much information as possible.
- Do not include identifiable personal or personal health information.
- 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 204-982-9130, toll free 1-800-665-0531 or by email to ombudsman@ombudsman.mb.ca

Upon completion, please submit this form to Manitoba Ombudsman in one of the following ways:

- By email at ombudsman@ombudsman.mb.ca
- By fax at 204-942-7803

You will be contacted by our office to verify that we have received the form. We may contact you again after reviewing the form to seek clarification and we may conduct an investigation. This privacy breach report will help our office determine the type of response required.

This form should not be used by individuals who believe that their personal or personal health information has been collected, used or disclosed, or safeguarded in a way that does not comply with FIPPA or PHIA. Individuals may make a complaint to the ombudsman using the FIPPA or PHIA complaint forms. Contact our office for the forms, see our website at www.ombudsman.mb.ca, or click on the links below:

FIPPA access or privacy complaints: www.ombudsman.mb.ca/info/making-a-complaint.html
PHIA access or privacy complaints: www.ombudsman.mb.ca/info/making-a-complaint-1.html

Submission date

CONTACT INFORMATION

Name of public body or trustee

Program/department (if applicable)

Contact Person

Name

Job Title

Phone

Fax

Email

Mailing Address

REASON FOR REPORTING

1. Identify your reasons for reporting this breach (check all that apply)
   - ☐ The privacy breach created a real risk of significant harm for an individual or individuals.
   - ☐ To inform Manitoba Ombudsman of potential complaints from the breach.
   - ☐ It is the public body/trustee's policy to report privacy breaches to Manitoba Ombudsman.
   - ☐ To seek advice and guidance.
   - ☐ Other, please specify

BREACH DESCRIPTION

2. Date of breach

3. Date breach was discovered

4. How was the breach discovered and who discovered it?

5. Where did the breach occur?

6. Type of breach

- ☐ accidental disclosure (ex: misdirected communication or accidentally unsecured information)
- ☐ loss of physical devices or paper records containing personal or personal health information
- ☐ theft of physical devices or paper records containing personal or personal health information
- ☐ unauthorized access by malicious or potentially malicious actors
- ☐ other, please specify

7. Describe the circumstances of the breach and its causes. Please indicate whether there is evidence of any malicious intent such as the breach being a result of theft or gaining unauthorized access to a computer system.

8. What was the length of time since the privacy breach first occurred and the duration of the period in which the personal health information was available to be accessed, used, disclosed, destroyed, or altered in contravention of FIPPA or PHIA?

9. What kinds of security safeguards were in place at the time of the breach? (select all that apply)

- ☐ Physical security (locks, alarm systems, etc.)
- ☐ Technical security (encryption, passwords, etc.)
- ☐ Administrative security (policies/procedures relevant to the breach)

Please explain

10. If applicable, please describe how the personal or personal health information involved in the privacy breach was adequately encrypted, anonymized or otherwise not easily accessible.

CONTAINMENT OF THE BREACH

11. Describe the steps that have been taken to limit the breach to reduce the risk of harm (ex: locks changed, computer systems shut down)

12. Has the personal or personal health information been recovered?

☐ Yes

☐ No

If yes, please provide details of how the information was recovered and any additional measures to secure it. If no, please provide details about the actions taken to try to recover the information.

RISK EVALUATION

A public body/trustee must determine if the privacy breach created a real risk of significant harm for an affected individual(s) based on the sensitivity of the personal or personal health information involved and the probability that the personal or personal health information could be used to cause significant harm to the individual(s) (see FIPPA 41.1(2) and PHIA 19.0.1(2)). The required factors that must be considered in determining the real risk of significant harm can be found under FIPPA regulation 3.1 and PHIA regulation 8.7.

Personal or personal health information involved

13. Describe the types of personal or personal health information involved in the breach (ex: name, address, Social Insurance Number, financial, medical information) and the form it was in (ex: paper records, electronic database).

13.1 Please indicate the volume of the information (the number of different types of information and the approximate number of records, if applicable). Do not include or send us identifiable personal or personal health information.

Individuals affected by the breach

14. Number of individuals affected by the breach (please be as specific as possible)

15. Category of individuals affected (check all that apply)

- ☐ Client/patient/student
- ☐ Employee
- ☐ Other, please specify

Harm from the breach

16. Does the privacy breach involve individuals who know each other (ex: an employee used or disclosed information about an individual that they know?)

- ☐ Yes
- ☐ No
- ☐ Unknown

17. If yes, what is the nature of the relationship?

- ☐ Friend
- ☐ Neighbour
- ☐ Family member
- ☐ Ex-partner
- ☐ Coworker
- ☐ Other, please specify

18. Estimated number of individuals who potentially or actually accessed the personal or personal health information

18.1 Is the public body or trustee reasonably satisfied that any person who actually or potentially accessed the personal or personal health information has destroyed any unauthorized copies of it and has committed to not use or disclose it?

- ☐ Yes
- ☐ No

Please explain

19. Identify the types of harm(s) that may result from the breach:

- ☐ Identity theft (most likely when the breach includes the breach of Social Insurance Numbers (SIN), credit card information, driver's license numbers, Personal Health Identification Numbers (PHIN), debit card numbers with password information and any other information that can be used to commit financial fraud)
- ☐ Financial loss
- ☐ Negative effects on the individual's credit rating or report
- ☐ Damage to or loss of the individual's property
- ☐ Risk of physical, bodily harm (when the loss of information places any individual at risk of physical or mental harm, stalking or harassment)
- ☐ Hurt, humiliation, embarrassment, damage to reputation (associated with the breach of information such as medical records or employee disciplinary records) or damage to relationships (impact on standing in community, family, colleagues, friends)

☐ Loss of employment, business or professional opportunities (usually as a result of damage to reputation of an individual)

☐ Other, please specify:

Public body/trustee determination of real risk of significant harm

20. Based on consideration of all the applicable factors under the regulations (see FIPPA regulation 3.1 and PHIA regulation 8.7), have you determined that a real risk of significant harm was created as a result of the privacy breach?

☐ Yes

☐ No

Please explain

NOTIFICATION

FIPPA and PHIA require that notification be made to individuals affected by a privacy breach and to Manitoba Ombudsman when a public body or trustee determines that the breach has created a real risk of significant harm for individuals (see FIPPA 41.1(3) and PHIA 19.0.1(3)).

21. Have affected individual(s) been notified in writing?

☐ Yes

☐ No

Have affected individuals also been notified orally?

☐ Yes

☐ No

If yes, please indicate the reasons for first notifying orally.

If yes, please indicate the date of notifications (or the planned dates):

Date notification(s) completed:

22. Method of notification used for affected individuals (please select all that apply)

- ☐ Affected individuals notified directly (ex: by phone, in person, via email)
- ☐ Affected individuals notified indirectly (ex: by news release, media or ad)
- ☐ Some affected individuals notified directly, some notified only indirectly
- ☐ Some or all affected individuals not notified

23. Describe the form(s) of notification (ex: letter, email, telephone, newspaper, website, etc.). If possible please attach an anonymized copy of the notification (or script of notification) and confirm if the notification conforms to the regulations (see FIPPA regulation 3.2, 3.3 and PHIA regulation 8.8). Do not include or send us identifiable personal or personal health information.

24. If you have chosen to notify affected individuals indirectly, describe the rationale for doing so as well as the type of indirect notification used (and the likelihood of it reaching the target audience).

25. If notification of affected individuals in any manner has not occurred, please explain why:

Notification of others

26. Other than affected individuals and the ombudsman, indicate who else has been notified and when this occurred (ex: executive management, privacy officer, access and privacy coordinator, police or law enforcement, IT service provider or government branch/department responsible for IT, professional regulatory bodies, or entities that should be notified according to their governing legislation or policy)

PREVENTION

27. Describe the steps you have taken or intend to take to reduce the risk of a similar event occurring in the future including any additional technical, physical or administrative safeguards. (ex: electronic device encryption, increased password protections, increased firewall protection, keyless building entry, increased storage in locked cabinets, development of policies or added procedures, staff training).

ADDITIONAL INFORMATION

28. Provide any additional relevant information regarding the breach below. Also provide a copy of any internal investigation report or other relevant documentation (without identifying personal or personal health information), if available, along with this breach report.