MANITOBA OMBUDSMAN

Privacy Breach Notification Letter Checklist

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.

In the event of a privacy breach, notification is 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. 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.

As of January 1, 2022, under both the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Act (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.

When making a mandatory notification under the legislation, your letter must include the required elements under subsection 3.2(1) of the Access and Privacy Regulation or subsection 8.8(1) of the Personal Health Information Regulation summarized in the checklist that follows.

If you have not determined that a real risk of significant harm was caused by the privacy breach, but still want to notify affected individuals, the following list can also be used to guide the content of your letter. In all cases, it is recommended that you review our practice note Keys Steps in Responding to Privacy Breaches Under FIPPA and PHIA along with this document.

List

- **Describe the circumstances of the privacy breach**

  Describe the incident. Include the date of discovery and explain how the privacy breach was discovered, provide details of what occurred, and if known, include whether the privacy breach was accidental or intentional, etc.

- **Provide the date of the privacy breach**

  Include the exact date if known or the date when the incident was believed to have occurred

- **Provide the name of the public body or trustee**

  Identify who had custody or control of the personal or personal health information at the time of the privacy breach.

- **Describe the information involved in the privacy breach**

  Be specific when describing the type of personal and/or personal health information involved. For example, a patient or client file that included the individual's diagnosis, list of medications, emergency contact information, personal health identification number (PHIN), etc. Each type of personal and personal health information may have varying degrees of impact on the individual.

- **Describe the steps that the individual can take to reduce the risk of harm that can result from the privacy breach or to mitigate that harm**

  Describe what the individual can do to protect themselves or their family. For example, provide contact information for credit monitoring agencies where there is a risk of identity theft, or suggest contacting financial institutions, changing account or email passwords.

  When a privacy breach impacts an individual's physical safety or security in their residence, examples include alerting building security in the case of disclosure of access codes (for multi-family dwellings) and ensuring entrance doors remained locked so that unknown individuals are not permitted to enter.

- **Describe the steps that the public body or trustee has taken or intends to take to reduce the risk of harm**

  Describe the corrective measures taken or planned to reduce the risk of harm to the individual as a result of the breach. Examples include stopping the

method of transmission if an accidental disclosure until the problem is addressed, contacting law enforcement or offering credit monitoring. You must also describe what your public body/trustee is doing to prevent any future privacy breaches (if known at the time of notification). For example, enhancing security measures (ex: encryption software), implementing new policies or procedures, changing locks on doors and filing cabinets and/or implementing new auditing practices.

- **Inform the individual that Manitoba Ombudsman has been notified about the privacy breach as required under subsection 41.1(4) of FIPPA or subsection 19.0.1(4) of PHIA**

  Under FIPPA and PHIA, an individual has the right to make a privacy complaint to Manitoba Ombudsman about their personal and/or personal health information. Should the individual contact the public body or trustee about making a complaint to Manitoba Ombudsman or to obtain further information about their privacy rights, the following contact information can be provided:

  Manitoba Ombudsman
  Address: 300 – 5 Donald St. Winnipeg, MB R3L 2T4
  Phone: (204) 982-9130
  Toll Free: 1-800-665-0531
  Email: ombudsman@ombudsman.mb.ca
  Website: www.ombudsman.mb.ca

- **Contact information for the public body or trustee**

  Provide contact information of someone within the public body/trustee who can answer the individual's questions and/or provide further information regarding the privacy breach. This letter should be signed by someone with authority in the organization, such as the access/privacy officer or senior manager.

- **Any other information that the public body or trustee considers relevant**

  This could include, for example, an acknowledgement that the privacy breach may have caused the individual distress and apologize on behalf of the public body/trustee.

Revised January 2022