GUIDE TO CREATING AN INTERNAL

# PRIVACY BREACH INVESTIGATION REPORT

This document assists public bodies and/or trustees in creating an internal privacy breach investigation report. It presents a series of questions that public bodies and/or trustees can use to assist them in investigating privacy breaches and preparing a privacy breach report.

Office of the
Saskatchewan Information
and Privacy Commissioner

SEPTEMBER 2020

# PURPOSE

The Office of the Information and Privacy Commissioner (IPC) recommends the following four steps when a public body or trustee is responding to a privacy breach:

- contain the privacy breach;
- notify affected individuals;
- investigate the privacy breach; and
- prevent future privacy breaches.

This document focuses on documenting the four steps when writing a privacy breach report. This document is to assist public bodies and trustees in creating its internal privacy breach investigation report. It presents a series of questions that public bodies and/or trustees can use to assist in investigating privacy breaches and preparing a privacy breach report. Please note that it is not an exhaustive list of questions.

The IPC encourages public bodies and trustees to use this document as a guide.

For additional guidance on how to manage privacy breaches, please refer to the following two resources: *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Health Trustees*.

# CONTAIN THE PRIVACY BREACH

Soon after a public body/trustee learns of a privacy breach, it should contain and recover any personal information/personal health information that is involved. This will require determining how broad the privacy breach is and what type of records are involved.

If paper records are involved, then efforts should be made to physically recover the paper records.

If electronic records are involved, then efforts should be made to:

- physically recover any devices that contain information, such as a USB key, CDs, and DVDs;
- recall emails and/or requesting recipients to destroy the email containing personal information/personal health information; and/or
- immediately take down personal information/personal health information if it was posted online.

## NOTIFY AFFECTED INDIVIDUALS

Notice to affected individuals should happen as soon as possible when learning of a breach. Section 29.1 of FOIP and section 28.1 of LA FOIP require that government institutions and local authorities take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution or local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual. For more information on what "real risk of significant harm" means, please refer to IPC's blog entry entitled *Real Risk of Significant Harm*.

For more information about how to notify affected individuals, please refer to the following resources: *Privacy Guidelines for Government Institutions and Local Authorities* and *Privacy Guidelines for Trustees*.

1. Who are the affected individuals?
2. How many individuals are affected?
3. Has the public body identified the risks that the affected individuals will be exposed to because of the privacy breach?
4. Has the public body notified (or will the public body notify) the affected individuals? Why or why not?

## INVESTIGATE THE PRIVACY BREACH

Investigating the privacy breach to identify the root cause is key to understanding what happened. Identifying the root cause will help prevent similar breaches in the future. The IPC has developed the *Privacy Breach Investigation Questionnaire* (*Questionnaire*) which is a valuable tool to aid public bodies during an investigation. The *Questionnaire* will help public bodies answer important questions, including the following:

- What happened?
- When did the privacy breach occur?
- When and how did the public body/trustee learn of the breach (if different from above)?
- What efforts have the public body/trustee made to contain the privacy breach?
- Has the privacy breach been contained completely? Why or why not?

- What personal information/personal health information was involved in the privacy breach?
- Where did the privacy breach occur?
- Who was involved?
- Which employee(s) (if any) are involved or witnessed the privacy breach?
- What type of personal information/personal health information is involved?
- Who has been affected by this privacy breach?

## PREVENT FUTURE PRIVACY BREACHES

Public bodies/trustees should be safeguarding personal information/personal health information. Administrative, physical, and technical safeguards should be reviewed regularly to determine their adequacy in protecting information. They should also be reviewed after the discovery of a privacy breach.

Examples of **administrative safeguards** include policies, procedures, agreements, contracts, and training resources. Examples of **physical safeguards** include locked filing cabinets, restricted access to areas containing personal information/personal health information, computer monitor privacy screens, and alarm systems. Examples of **technical safeguards** include protecting information through strong passwords and encryption, automatic log off features for computers (after a short time of user inactivity), and firewalls.

1. What administrative safeguards has the public body identified as relevant to this privacy breach?
2. What physical safeguards has the public body identified as relevant to this privacy breach?
3. What technical safeguards has the public body identified as relevant to this privacy breach?
4. Has the public body made changes to any of the identified safeguards to prevent similar privacy breaches?
5. Has the public body created any new safeguards to prevent similar privacy breaches? If so, please describe.

## CONTACT INFORMATION

If you have any questions or concerns about creating an internal privacy breach investigation report, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

webmaster@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC