



Office of the Information and Privacy Commissioner (OIPC)
Key Steps in Responding to Privacy Breaches

Purpose

The purpose of this document is to provide guidance to organizations, public bodies and custodians when a privacy breach occurs.¹ Organizations, public bodies and custodians can also take preventative steps prior to a breach occurring. For more information on how to help prevent security breaches, see *Implementing Reasonable Safeguards*, produced by the Office of the Information and Privacy Commissioner (“OIPC”) and available online at www.oipc.ab.ca.

What is a privacy breach?

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal or health information. Such activity is “unauthorized” if it occurs in contravention of the *Personal Information Protection Act* (“PIPA”), the *Freedom of Information and Protection of Privacy Act* (“FOIP”) or the *Health Information Act* (“HIA”). The most common privacy breach happens when personal information about customers, patients, clients or employees is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal or health information is stolen or personal information is mistakenly emailed to the wrong person.

Reporting privacy breaches

Reporting a privacy breach is not mandatory under the *Health Information Act* (HIA) or the *Freedom of Information and Protection of Privacy Act* (FOIP). However, **it is mandatory to report certain privacy breaches to the Commissioner under section 34.1(1) of PIPA**; specifically, PIPA organizations are required to notify the Commissioner of incidents “involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual.”

The OIPC has created a Breach Report Form that allows organizations, public bodies and custodians to complete an analysis of the privacy breach using the four key steps described below. The Breach Report Form is available online at www.oipc.ab.ca.

Four key steps in responding to a privacy breach

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 recommendations for longer-term solutions and prevention strategies.

¹ These guidelines have been adapted with permission from *Key Steps in Responding to Privacy Breaches*, developed by the Office of the Information and Privacy Commissioner of British Columbia (OIPC BC), December 2006, and the *Breach Notification Assessment Tool*, jointly produced by the OIPC BC and the Information and Privacy Commissioner/Ontario, December 2006. These key steps can assist Alberta organizations that are subject to the *Personal Information Protection Act*, public bodies that are subject to the *Freedom of Information and Protection of Privacy Act*, and custodians subject to the *Health Information Act*.

Step 1. Contain the Breach

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

- Immediately 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.
- Immediately contact your Privacy Officer, FOIP Coordinator, or Responsible Affiliate and/or the person responsible for security in your organization.
- Notify the police if the breach involves theft or other criminal activity.

Step 2: Evaluate the Risks Associated with the Breach

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

(i) Personal or Health Information Involved

- What data elements have been breached? Generally, the more sensitive the information, the higher the risk. Health information, Social Insurance Numbers (SINs) and financial information that could be used for identity theft are examples of sensitive information.
- What possible use is there for the information? Can the information be used for fraudulent or otherwise harmful purposes?

(ii) 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 and the risk of further access, use or disclosure, including in mass media or online?
- Is the information encrypted or otherwise not readily accessible?
- What steps have you already taken to minimize the harm?

(iii) Individuals Affected by the Breach

- How many individuals are affected by the breach?
- Who was affected by the breach: employees, public, contractors, clients, service providers, other organizations?

(iv) **Foreseeable Harm From the Breach**

- Is there any relationship between the unauthorized recipients and the data subject?
- What harm to the individuals will result from the breach? Harm may include:
 - Security risk (e.g. physical safety)
 - Identity theft or fraud
 - Loss of business or employment opportunities
 - Hurt, humiliation, damage to reputation or relationships
- What harm could result to the organization, public body or custodian as a result of the breach? For example:
 - Loss of trust in the organization, public body or custodian
 - Loss of assets
 - Financial exposure
- What harm could result to the public as a result of the breach? For example
 - Risk to public health
 - Risk to public safety

Organizations regulated by PIPA are **REQUIRED** to notify the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information, **where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the incident** (PIPA section 34.1).

A Report to the Commissioner must comply with section 19 of the *PIPA Regulation* and, among other things, must include “an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure.” Considering the factors set out above may assist PIPA organizations in assessing the real risk of harm to individuals that could result from a breach incident. Organizations should refer to the Act and Regulation for the exact wording of the breach reporting requirements.

Step 3: Notification

Notification can be an important mitigation strategy in the right circumstances. The 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 information has been inappropriately collected, used or

disclosed. Review your risk assessment to determine whether or not notification is required.

Organizations, public bodies or custodians that collect and hold personal information are responsible for notifying affected individuals when a privacy breach occurs. If the breach occurs at a third party entity that has been contracted to maintain or process personal or health information, the breach should be reported to the originating entity, which has primary responsibility for notification.

Amendments to PIPA in May 2010 added new powers authorizing the Commissioner to require organizations to notify individuals affected by a reportable breach. In addition, The *PIPA Regulation* was amended to specifically set out what must be included in a notice to individuals in the event an organization experiences a loss of or unauthorized access to or disclosure of personal information that must be reported under section 34.1(1) of the Act.

Organizations subject to PIPA should refer to the Act and Regulation for the exact wording of these notification requirements.

(i) Notifying Affected Individuals

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- **Legislation requires notification:** Is your organization, public body or custodian covered by legislation that requires notification of the affected individual? If you are uncertain, contact the OIPC.
- **Contractual obligations require notification:** Does your organization, public body or custodian have a contractual obligation to notify affected individuals in the case of a data loss or privacy breach?
- **Risk of identity theft or fraud:** How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with SINs, credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information or any other information that can be used for fraud by third parties (e.g. financial).
- **Risk of physical harm:** Does the loss of information place any individual at risk of physical harm, stalking or harassment?

- **Risk of hurt, humiliation or damage to 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 loss of information result in damage to the reputation of an individual, affecting business or employment opportunities?

(ii) When and How to Notify

When: Notification of individuals affected by the breach 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 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, and/or
- individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.).

Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, contact information is lacking, or where a very large number of individuals are affected by the breach such that direct notification could be impractical. Using multiple methods of notification in certain cases may be the most effective approach.

Section 19.1 of the *PIPA Regulation* states that where the Commissioner requires an organization to notify an individual(s), the notification to the individual(s) **must be given directly** unless the Commissioner determines that direct notification would be unreasonable in the circumstances.

If a PIPA organization believes that direct notification to individuals is likely to be unreasonable, the organization should give **reasons for this at the time the organization submits its Report of the incident to the Commissioner;** doing so will help to expedite the decision-making process.

What Should be Included in the Notification?

Section 19.1(1) of the *PIPA Regulation* sets out what MUST be included in a notice to individuals in the event a PIPA organization is required to notify individuals of a breach. These mandatory elements of the notification are indicated below with an “*”.

Notification should include the following information:

- Date on which or time period during which the breach occurred*;
- Description of the circumstances of the breach (a general description of what happened)*;
- Description of the information involved in the breach* (e.g. name, credit card numbers, SINS, medical records, financial information, etc.);
- Description of any steps taken to reduce the risk of harm*;
- Next steps planned and any long term plans to prevent future breaches;
- Steps the individual can take to further mitigate the risk of harm. Provide information about how individuals can protect themselves e.g. how to contact credit reporting agencies (to set up a credit watch), how to change a personal health number or driver’s license number.
- Contact information of a person who can answer questions about the breach*;
- That individuals have a right to complain to the Office of the Information and Privacy Commissioner. Provide contact information.

(iii) 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
- **Insurers or others:** if required by contractual obligations
- **Professional or other regulatory bodies:** if professional or regulatory standards require notification of these bodies
- **Credit card companies and/or credit reporting agencies:** it may be necessary to work with these companies to notify individuals and mitigate the effects of fraud.

- **Office of the Information and Privacy Commissioner:** the following factors are relevant in deciding when to report a breach to the OIPC:
 - The sensitivity of the personal or health information;
 - Whether the disclosed information could be used to commit identity theft;
 - Whether there is a reasonable chance of harm from the disclosure including non pecuniary losses;
 - The number of people affected by the breach, and
 - Whether the information was fully recovered without further disclosure.

REMINDER

Organizations regulated by PIPA are REQUIRED to notify the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information, where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the incident (PIPA section 34.1).

The OIPC may be able to assist you in developing a procedure for responding to the privacy breach and ensuring steps taken comply with obligations under privacy legislation. To notify the OIPC, you may wish to use the Breach Report Form located at www.oipc.ab.ca.

Step 4: Prevention

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 both physical and technical security. 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 investigation and regularly after that. 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 privacy legislation. For more information on how to help prevent security breaches, see *Implementing Reasonable Safeguards*, produced by the OIPC and available online at www.oipc.ab.ca.

Contact Information

Calgary: Office of the Information and Privacy Commissioner
Suite 2460, 801 – 6 Avenue SW
Calgary, Alberta T2P 3W2
Phone: (403) 297- 2728
Fax: (403) 297-2711

Edmonton: Office of the Information and Privacy Commissioner
#410, 9925 – 109 Street
Edmonton, Alberta T5K 2J8
Phone: (780) 422-6860
Fax: (780) 422-5682

Toll Free: 1-888-878-4044

Web: www.oipc.ab.ca

Email: generalinfo@oipc.ab.ca

This document is for general information only. It is not intended to be, and cannot be relied upon as legal advice or other advice. Its contents do not fetter, bind or otherwise constitute a decision or finding by the Office of the Information and Privacy Commissioner (OIPC) with respect to any matter, including any complaint, investigation or other matter, respecting which the OIPC will keep an open mind. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization, public body and custodian.