Office of the Information and Privacy Commissioner of Alberta

Guidance for Notifying the Commissioner about a Privacy Breach under PIPA

April 1, 2024

This guidance, along with the PIPA Privacy Breach Notification Form, may be used by an organization that is notifying the Information and Privacy Commissioner (the Commissioner) about a privacy breach under section 34.1 of the *Personal Information Protection Act* (PIPA). The form is found on the Forms page here, under the heading "Mandatory and Self-Reported Breach Forms".

Organizations may have other obligations in law or otherwise regarding privacy breaches, including the duty to notify individuals affected by the privacy breach. Organizations are responsible for making themselves aware of these obligations.

Individuals (members of the public) should not use this guidance. Individuals who believe their personal information has been lost or improperly collected, used, disclosed or accessed by an organization may file a complaint with the Office of the Information and Privacy Commissioner (OIPC) by visiting the Request a Review / File a Complaint webpage.

What is a Privacy Breach?

For purposes of the PIPA Privacy Breach Notification Form and this guidance, a "privacy breach" or "breach" means 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 loss or unauthorized access or disclosure.

Privacy breaches can occur in a number of ways. Some of the more common incidents about which organizations notify the Commissioner include:

- Loss or theft of mobile devices (e.g. laptops, USB sticks or hard drives);
- Misdirected communications (via email, fax or mail);
- Employee "snooping" of patient or customer records (also known as unauthorized access to or misuse of customer or patient information by an authorized user);
- Hacking of computers, servers and websites, including deployment of malicious software ("malware") such as ransomware;
- Phishing or social engineering attacks;
- Insecure or improper disposal of records, computer systems, storage media;
- Stolen paper records from an employee's vehicle, home or office;

Requirement to Notify the Commissioner about a Privacy Breach

Under PIPA, it is **mandatory** for an **organization** with personal information under its control to notify the Commissioner without unreasonable delay about a privacy breach where a reasonable person (section 2) would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure (section 34.1).

Who is Responsible for Notifying the Commissioner?

The organization having **control** of the personal information has the legal obligation to notify the Commissioner of a breach that meets the requirements of section 34.1 of PIPA. The organization with control may authorize, in writing, a third party to notify the Commissioner about a breach on its behalf. See, for example, Breach Notification Decisions P2022-ND-060 and P2022-ND-061.

Custody vs. Control

Generally, information is considered to be in the **custody** of an entity when the entity has physical possession of the information or the information systems that store the information. Information is under the **control** of an entity when the entity has the authority to manage the information, including restricting, regulating and administering its use, retention and disposition, and demanding the return of the information.

An entity may not have custody of the information but still be considered to have the information under its control. For example, a contractor of an organization may have custody of personal information because it has collected or created the information in relation to services performed by the contractor on behalf of the organization. **However, the organization retains control** over the information because it establishes the purposes for which the contractor may collect, use or disclose the information, directs how the information is to be secured and when it is to be disposed of, and can obtain access to the information.

Additional discussion of the criteria for establishing custody or control can be found in OIPC orders. See, for example, Orders F2010-022, F2010-023, F2015-21 and P2015-08.

How Quickly Does an Organization Need to Notify the Commissioner about a Privacy Breach?

Organizations are required to notify the Commissioner about privacy breaches **without unreasonable delay** where there is a real risk of signification harm to the affected individuals (section 34.1).

Where there exists a real risk of significant harm to affected individuals, the OIPC recommends that the Commissioner be informed of a breach as soon as possible regardless of whether all the information requested in the PIPA Privacy Breach Notification Form is available (e.g. in cases where the organization has not completed an internal investigation or established long-term strategies to correct the situation).

Please note that *informing* the Commissioner of a privacy breach is *not* considered notice to the Commissioner without unreasonable delay under section 34.1.

What Information Should Be Included in the Notice to the Commissioner?

The PIPA Privacy Breach Notification Form is designed to ensure organizations provide the Commissioner with the information they are required to provide under PIPA and that the Commissioner would typically request in follow-up communications. Providing as much information upfront expedites the breach process.

A notice of a breach under section 34.1(1) of PIPA must include the information prescribed by section 19 of the *Personal Information Protection Act Regulation* (PIPA Regulation).

Section 19 of the PIPA Regulation states the notice must **be in writing and include the following information:**

- A description of the circumstances of the breach;
- The date on which or time period during which the breach occurred;
- A description of the personal information involved in the breach;
- An assessment of the risk of harm to individuals as a result of the breach;
- An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the breach;
- A description of any steps the organization has taken to reduce the risk of harm to individuals;
- A description of any steps the organization has taken to notify individuals of the breach;
- The name and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.

The Commissioner has the power to require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization to notify affected individuals or to satisfy the terms and conditions that the Commissioner may have placed on an organization that has been directed to notify affected individuals (section 37.1(4)).

Offences

Pursuant to section 59(1)(e.1) of PIPA, it is an offence for a person to fail to notify the Commissioner of an incident that meets the criteria under section 34.1 of the Act. If guilty of an offence, an individual is

subject to a fine up to $10,000, and a person other than an individual is subject to a fine up to $100,000 (section 59(2)).

The Commissioner may investigate whether an organization complied with its section 34.1 duty to notify the Commissioner of a privacy breach, as provided by sections 36(1)(a) and 36(2)(e.1).

Additional Resources

OIPC orders, investigation reports, past PIPA Breach Notification Decisions and additional information on how to respond to a privacy breach are available on the OIPC website.

Instructions for Completing the PIPA Privacy Breach Notification Form

The headings below correspond to the sections of the PIPA Privacy Breach Notification Form.

Section A: Information of Organization

Date of Notification

The date of the notification is the date an organization submits the completed PIPA Privacy Breach Notification Form to the Commissioner. The information in the form should be as accurate as possible as of the date of the notification and should meet the requirements of section 19 of the *PIPA Regulation*.

Name of Organization

Provide the legal name of the organization notifying the Commissioner about the breach under section 34.1 of PIPA.

Address of Organization

Provide the address of the organization.

Organization File Number

Include any file number that the organization has assigned to the breach.

Description of Organization

To establish context for the privacy breach, provide a description of the organization and its services.

Organization Classification

The *North American Industry Classification System* (NAICS) is an industry classification system developed by the statistical agencies of Canada, Mexico and the United States. For

categorization and statistical purposes, select the sector which best describes the activities of the organization.

Contact information for a person who can answer the OIPC's questions about the breach

Provide the name, title/position and contact information for the person who, on behalf of the organization, can answer the Commissioner's questions about the breach (*PIPA Regulation*, section 19(h). The OIPC will communicate with this person.

PIPA non-profit organizations

This section applies only to not-for-profit organizations that meet the definition of a "non-profit organization" in section 56(1)(b) of PIPA.

For purposes of PIPA, a non-profit organization is an organization that is:

- Incorporated under the *Societies Act* or the *Agricultural Societies Act*, or
- Registered under Part 9 of the *Companies Act.*

These non-profit organizations must notify the Commissioner of a privacy breach when the personal information involved in the breach was collected, used or disclosed by the organization **in connection with a commercial activity** carried out by the organization.

Section 56(1)(a) of the Act defines what is a commercial activity.

A privacy breach involving the personal information of employees of a non-profit organization (as defined in section 56) can be subject to the mandatory breach notification requirements in PIPA. The OIPC has determined that employees hired to perform functions necessary to carry out a commercial activity are hired "in connection with" that commercial activity (Order P2017-07). The Commissioner has required non-profit organizations to notify employees whose personal information was the subject of a breach. For example, in Breach Notification Decision P2018-ND-003, the individuals affected by the breach worked as a housekeeper, cook and kitchen staff, banquet server, or maintenance worker. These are functions that are necessary to carry out the non-profit organization's commercial activity of operating a recreational facility.

When a not-for-profit organization does not meet the definition of a non-profit organization under section 56 of PIPA (e.g. the organization is established by private Act, federal or other provincial legislation or is an unincorporated association), PIPA applies fully to the organization and the organization must notify the Commissioner about a breach in accordance with section 34.1 of PIPA.

Third party notifying the Commissioner about the breach

Occasionally, the entity notifying the Commissioner about the breach is not the organization that is required to notify the Commissioner.

Complete this section of the form if the entity notifying the Commissioner about the breach is **not** the organization responsible for notifying (i.e. the organization named at the beginning of the form). Indicate the relationship with the organization, whether the breach has been reported to the organization, and whether the entity is authorized to notify the Commissioner on behalf of the organization.

Section B: Breach Description

Date breach occurred and date breach ended

Provide the date on which the breach started and ended. If the actual date(s) of the breach are not known at this time, provide the suspected date range during which the breach occurred (PIPA Regulation, section 19(b)).

Date breach was discovered

Provide the date on which the breach was discovered.

Total number of individuals affected

Provide the number (or an estimate if the actual number is not yet known) of individuals whose personal information is involved in the breach (PIPA Regulation, section 19(e)).

Was the information collected in Alberta?

Indicate if any of the personal information involved in the breach was collected in Alberta. If yes, provide the number of individuals (or an estimate if the actual number is not yet known) of the individuals whose information was collected in Alberta.

Personal information is considered "collected in Alberta" if the subject individual is in Alberta at the time of collection and/or if the organization operates in Alberta. For example:

An individual residing in Alberta submits a job application electronically to an organization in Ontario. The personal information is transmitted over the internet and stored on a server hosted in Ontario. The personal information was "collected in Alberta" because the individual was in Alberta at the time it was collected by the organization.

An individual residing in the United States submits a job application electronically to an organization operating in Alberta. The personal information is transmitted over the internet and stored on a server hosted in British Columbia. The personal information was "collected in Alberta" because the organization operates in Alberta.

An individual residing in Alberta drives to the United States. The individual checks into a hotel in Arizona, no pre-booking was done in advance. The personal information was not "collected in Alberta" because the information was collected in-person at the hotel, outside of Alberta.

An individual visits the United States to shop at an outlet shopping centre. A store the individual made a purchase from, in the United States, was subject to a cyberattack, resulting in the unauthorized access to that individual's personal information. The personal information was not "collected in Alberta" because the information was collected in-person at the store, outside of Alberta.

The breach involved

Indicate the type of breach:

- A **loss** of personal information (e.g. theft of information from an office, home or vehicle; organization does not know where the information is; information lost during office relocation);

- **Unauthorized access** to personal information (e.g. electronic system compromise; ransom demand; phishing or social engineering; payment card skimming; break-in; employee accessing information without authorization);

- **Unauthorized disclosure** of personal information (e.g. transmission errors by email, fax, mail or verbally; information improperly shared on internal network drives, social media, published on leak site, dark web, etc.).

Location of the breach

Provide the address of the physical location where the breach occurred, if known.

Describe the circumstances of the breach including cause, how it was discovered, and by whom.

Provide a description of the breach and the causes of the breach, if known (PIPA Regulation, section 19(a).

Do not include personal information about the individuals whose information is involved in the breach ("individually identifying information").

Provide a description of how the breach was discovered and the circumstances associated with the discovery. Indicate who discovered the breach by way of their title and position within the organization.

If the person who discovered the breach is a service provider to the organization, provide the name of the service provider and describe their relationship with the organization.

PIPA requires organizations to notify the Commissioner without unreasonable delay (section 34.1). If there has been a delay between the discovery of the breach and notifying the Commissioner, provide an explanation for the delay.

Personal Information Involved

Identify the types of personal information and list the data elements involved.

Specify the various elements of personal information involved in the breach (*PIPA Regulation*, section 19(c)).

Select categories from the drop-down boxes. Additional space is provided to enter a description if the involved personal information is not represented in the provided categories.

List each specific element involved. For example:

> *Identity information including age, date of birth, copy of passport, signature, birth certificate, and Social Insurance Number.*
>
> *Contact information including email address, home address, and telephone number.*

Do not include individually identifying information.

Examples of personal information include but are not limited to:

- Name;
- Address;
- Email address;
- Telephone number;
- Social Insurance Number (SIN);
- Driver's licence number;
- Education history;
- Employee number, pay, benefits, disciplinary records, performance evaluations;
- Credit card information;
- Banking and other financial information;
- Personal Health Number;
- Medical diagnostic, treatment or care information.

Section C: Significant Harm

- **Describe the significant harm (damage, detriment, or injury) that may occur to the affected individual(s) as a result of the breach.**

  The test for notifying the Commissioner about a breach under PIPA is whether "a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure" (section 34.1).

  Identifying the harm that could result from the breach is a component of the overall assessment of the real risk of significant harm to an **individual (not the organization)** as a result of the breach (PIPA Regulation, section 19(d)).

  Harm means some damage or detriment or injury that could be caused to an affected **individual (not the organization)** as a result of the loss of or unauthorized access to or disclosure of personal information.

  Some examples of harm that could flow from a breach of personal information are:

  - A breach of an individual's name and credit card number could result in identity theft and financial fraud.
  - A breach of an individual's name, driver's licence and SIN could result in identity theft and fraud.
  - A breach of an individual's diagnostic, treatment or care information could result in hurt, humiliation, mental distress, and embarrassment.
  - A breach of an individual's name and subscription to an adult magazine or website could result in reputational harm or embarrassment.
  - A breach of an individual's disciplinary letter could result in humiliation.

  The damage or detriment or injury that could be caused to an **individual (not the organization)** as a result of the breach must be **significant** – it must be important, meaningful, and with non-trivial consequences or effects.

  Examples of significant harm may include, but are not limited to:

  - Embarrassment, hurt or humiliation;
  - Damage to reputation or relationships;
  - Loss of employment, business or professional opportunities;
  - Financial loss;
  - Identity theft;
  - Fraud;
  - Negative effects on a credit record;
  - Damage to or loss of property;
  - Bodily harm;
  - Blackmail or extortion;

Real Risk of Significant Harm

Describe the Organization's assessment that a real risk of significant harm exists as a result of the privacy breach.

Submissions using the PIPA Privacy Breach Notification Form are made under section 34.1 of PIPA.
If there does **not** exist a real risk of significant harm to an individual as a result of the privacy breach, the organization is **not** required to provide notice under section 34.1.

The notice to the Commissioner must include an assessment of the risk of harm as a result of the privacy breach (*PIPA Regulation*, section 19(d)).

Whether a real risk of significant harm exists must be more than mere speculation or conjecture. There must be a cause and effect relationship between the breach and the harm.

In determining whether there exists a real risk of significant harm, the organization must consider all the circumstances surrounding the breach. Factors that influence whether a real risk of significant harm exists include, but are not limited to:

- What is the nature of the information involved?
- Who obtained or could have obtained access to the information?
- How many persons was the information exposed to?
- Is there any personal or professional relationship between the affected individual and the unauthorized recipient of the information?
- Were there security measures in place to prevent unauthorized access such as encryption? Are there known flaws in these security measures?
- How long was the information exposed?
- Is there evidence of malicious intent or purpose such as theft, hacking or malware?
- Could the information be used for criminal purposes such as for identity theft or fraud?
- Was the information recovered?
- How many individuals are affected by the breach?
- Are there vulnerable individuals involved such as youth or seniors?

Simply describing the risk of harm as being "low", "medium" or "high" does not meet the requirement for an assessment of the risk of harm.

Examples of what is considered a real risk of significant harm can be found in the Commissioner's past Breach Notification Decisions or published summaries.

Risk Mitigation

Describe the steps taken to reduce the risk of significant harm to affected individual(s)

List the actions taken by the organization to reduce the risk of harm to affected individuals as a result of the breach (e.g., information recovered; undertaking by unauthorized recipient that ensures the information was not viewed, used, or disclosed and was securely destroyed; device remotely disabled or wiped permanently; credit report monitoring). Include any actions that are planned, but not implemented (PIPA Regulation, section 19(f)).

Actions taken by the organization should mitigate the possible harm or risk of harm to the **affected individual(s)**. For example, review and enhancement of technical safeguards or implementation of new administrative procedures *after* a breach may not mitigate possible harm or reduce risk of harm to individuals affected in the incident at hand.

Describe the steps taken to reduce the risk of a similar event occurring in the future

List the actions taken by the organization to reduce the risk of a similar breach occurring in the future (e.g., mobile devices encrypted; physical locks changed; policies and procedures revised; new training implemented; known risks monitored; auditing processes implemented). Include any actions that are planned, but not implemented.

Section D: Notice to Affected Individuals

Have affected individuals been notified directly pursuant to *PIPA Regulation* section 19.1?

> The Commissioner has the power to require an organization to notify affected individuals when a privacy breach presents a real risk of significant harm as a result of the breach (section 37.1). This does not prohibit or restrict an organization from notifying individuals on their own initiative (section 37.1(7)). The Commissioner encourages organizations to not wait for direction from the Commissioner but to immediately notify affected individuals on their own initiative when the organization believes that there exists a real risk of significant harm to the individuals as a result of the breach.

Organizations must provide the Commissioner with a description of any steps the organization has taken to notify affected individuals of the privacy breach (*PIPA Regulation*, section 19(g)).

Notice must be given to the individual **directly** unless the Commissioner determines that direct notification would be unreasonable in the circumstances; the Commissioner may authorize the organization to notify individuals indirectly (*PIPA Regulation*, section 19.1(2)).

Indicate if the individuals affected by the breach have been notified **directly**.

Attach a copy of the notice. If notice was given verbally, attach a copy of the script.

The required contents of notice to an affected individual are set out in section 19.1 of the *PIPA Regulation.*

Attach a copy of the actual notice being given to the individuals. If notice was or is to be given verbally, attach a copy of the script. ***Do not include individually identifying information.***

Describe the form in which the notice was given (e.g. by letter, email, telephone) and the date on which, or date range during which, notification was given.

If an organization is unable to notify affected individuals directly, or if it believes direct notification would be unreasonable in the circumstances, it may consider making a submission explaining why direct notification is unreasonable and propose a plan for notifying affected individuals indirectly. See, for example, Breach Notification Decisions P2021-ND-284, P2020-ND-172, and P2019-ND-127.

Section E: Provide any Additional Relevant Information Regarding the Privacy Breach

Have the police or any other authorities or organizations been notified of the breach?

Indicate if other entities have been notified of the breach and provide their contact information. An organization may notify other entities of the breach for different reasons. For example:

- Police: if theft or other crime is suspected;
- Insurers or others: if required by contractual obligations;
- Professional or other regulatory 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;
- Other privacy commissioners: the breach may involve personal information in several jurisdictions.

Add any other information that the organization considers relevant in the space provided.

Submitting to the Commissioner

Organizations are required to notify the Commissioner about a privacy breach under the *Personal Information Protection Act* **without unreasonable delay**.

Email submissions are preferred. Please submit the completed PIPA Privacy Breach Notification Form to breachnotice@oipc.ab.ca. Please note that the previous email address (breachreport@oipc.ab.ca) has been disabled.

If you are unable to submit the form by email, you can submit it to:

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

For general information about responding to a privacy breach, please contact the OIPC by telephone at (780) 422-6860, toll free at 1-888-878-4044, or by email at breachnotice@oipc.ab.ca. Contacting the OIPC does not mean that an organization has fulfilled its legal obligation to notify the Commissioner about a privacy breach. Notification to the Commissioner about a privacy breach must meet the requirements of section 19 of the PIPA Regulation. Information provided by the OIPC does not constitute legal advice and is not binding on the Commissioner.