



Personal Information Protection Act (PIPA)
OIPC Process for
Determining Whether to Require Notification

Amendments to the *Personal Information Protection Act* (PIPA) were proclaimed in force on May 1, 2010, and added a new requirement for organizations to notify the Information and Privacy 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 Act was also amended to give the Commissioner the power to require organizations to notify individuals to whom there is a real risk of significant harm as a result of such an incident.

In addition, pursuant to the new section 37.1(3) of PIPA, **the Information and Privacy Commissioner is required to establish an expedited process for determining whether to require an organization to notify individuals** in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate. This document sets out that process.

Reporting a Breach to the Commissioner

An organization must 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 include the information prescribed by section 19 of the *PIPA Regulation* (PIPA section 34.1).

**It is an offence to fail to provide notice to the
Commissioner under section 34.1 [PIPA section 59(1)(e.1)]**

A Report to the Commissioner must be made **in writing** (by mail or fax), and must be submitted **without unreasonable delay** to:

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

OIPC Process

Upon receiving a Report from an organization, the OIPC will open a Report File, and assign a tracking number. A letter will be sent to the organization's contact, acknowledging receipt of the Report.

OIPC will review the organization's Report to ensure it includes all of the information required by section 19 of the *PIPA Regulation*.

- If the Report is not complete, OIPC will contact the organization without unreasonable delay, requesting that the organization submit a complete Report.
- Upon being contacted by the OIPC, the organization must submit a complete Report without unreasonable delay.

Once a completed Report has been received, OIPC staff will forward the Report File to the Commissioner.

The Commissioner will review the organization's Report, and decide whether or not to require the organization to notify individuals to whom there is a **real risk of significant harm**.

If the Commissioner decides to require that the organization notify individuals, the Commissioner may require that:

- the organization notify the individual(s) of the incident in a form and manner prescribed by the *PIPA Regulation* [PIPA section 37.1(1)(a)]
- individuals be notified within a time period determined by the Commissioner [PIPA section 37.1(1)(b)]
- the organization satisfy any additional terms or conditions that the Commissioner considers appropriate [PIPA section 37.1(2)].

The Commissioner may require the organization to provide additional information in order to make a decision whether to require that the organization notify individuals [PIPA section 37.1(4)].

An organization is not restricted from notifying individuals on its own initiative [PIPA section 37.1(6)]. However, in the event an organization has notified individuals on its own initiative before reporting an incident to the Commissioner, the Commissioner may, upon reviewing the organization's notice and finding it deficient, require the organization to notify individuals in the form and manner prescribed by the *PIPA Regulation*, (if this has not been done), or to satisfy additional terms and conditions as determined by the Commissioner.

Direct vs. Indirect Notification

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 [*PIPA Regulation* section 19.1].

If an 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.

Commissioner's Decision

The Commissioner's written decision to require an organization to notify individuals will be issued to the organization within a reasonable time of the OIPC having received the organization's Report of an incident that includes, at a minimum, the information required by section 19.1 of the *PIPA Regulation*.

The Commissioner has exclusive jurisdiction to require an organization to notify individuals [PIPA section 37.1(6)].

Publishing Decisions

Pursuant to section 38(6) of PIPA, the Commissioner "may publish any finding or decision in a complete or an abridged form."

Where the Commissioner requires that an organization notify individuals to whom there is a real risk of significant harm, the Commissioner's decision will be published on the OIPC website at www.oipc.ab.ca.

In the event the Commissioner decides that notification of individuals is not required, an anonymized, abridged version of the Commissioner's decision may be published.

Complaint Received

If the Commissioner receives a complaint from a person with respect to an incident that has already been reported to the Commissioner under section 34.1, the Commissioner will advise the person that the incident was reported, and that the Commissioner will make a decision as to whether or not the organization is required to notify individuals to whom there is a real risk of significant harm. The Commissioner may also initiate a separate investigation as a result of having received the complaint.

Other Resources

Additional resources are available on the OIPC website at www.oipc.ab.ca, including:

- *Reporting a Breach to the Commissioner*, which sets out the minimum requirements for what must be included in a Report to the Commissioner,
- *Breach Report Form*, which can be used to submit a Report to the Commissioner,
- *Notifying Affected Individuals*, which sets out the minimum requirements for what must be included in a notice to individuals of a breach, and
- *Key Steps in Responding to Privacy Breaches*, which provides guidance to organizations for dealing with a security breach.

Additional resources are also available on the Access and Privacy Service Alberta website at www.pipa.alberta.ca, including *Information Sheet 11: Notification of a Security Breach*.