



**Personal Information Protection Act (PIPA)
Notifying Affected Individuals**

The *Personal Information Protection Act* (PIPA) requires organizations to make reasonable security arrangements to protect personal information in their custody or control from such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

PIPA was amended on May 1, 2010, adding a new requirement for organizations to notify the Information and Privacy Commissioner of certain breaches involving personal information. In addition, the amendments added new powers **authorizing the Commissioner to require organizations to notify individuals affected by a reportable breach.**

With respect to notifying individuals, the new section 37.1 of PIPA states:

Power to require notification

37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure

(a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) 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.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms or conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

The *Personal Information Protection Act Regulation* has also been 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.

Section 19.1 of the *Regulation* states:

Notification to individuals

19.1(1) Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must

(a) be given directly to the individual, and

(b) include

- (i) a description of the circumstances of the loss or unauthorized access or disclosure,
- (ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred,
- (iii) a description of the personal information involved in the loss or unauthorized access or disclosure,
- (iv) a description of any steps the organization has taken to reduce the risk of harm, and
- (v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure.

(2) Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.

Despite section 37.1 giving the Commissioner the power to require an organization to notify affected individuals, section 37.1(6) of the amended PIPA clearly states that **an organization is not prohibited nor restricted from notifying individuals on its own initiative.**

Organizations are encouraged to notify individuals, in the form prescribed by the *Regulation*, of breaches that they know present a real risk of significant harm to those individuals.

Other Resources

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

- *Breach Report Form*, which can be used to submit a report to the Commissioner,
- *Reporting a Breach to the Commissioner*, which sets out the minimum requirements for what must be included in a report to the Commissioner,
- *OIPC Process for Determining Whether to Require Notification*,
- *Key Steps in Responding to Privacy Breaches* 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*.