Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

PRIVACYRIGHT fundamentals for business

Managing privacy breaches

Today's webinar you'll learn how to manage a privacy breach.

What is a privacy breach? Well, a privacy breach is the unauthorized access to or collection, use, disclosure or disposal of personal information.

A privacy breach can put your customers' or clients' at risk, is generally bad for business, and may be a contravention of PIPA (which requires organizations to protect the personal information in its custody or control).

Most privacy breaches happen when the PI of customers, clients, patients, or employees is mistakenly disclosed, lost or stolen. Some of the main causes include:

- Human error, such as:
  - inappropriate disposal;
  - emails sent to the wrong individuals or too many people;
  - faxes or mail sent to the wrong person; and
  - loss of paper files, laptops, portable memory sticks.

- Theft from an office or car where laptops, hard drives, or even paper files are stolen; and

- Inadequate electronic system security, such as:
  - Publicly accessible files
  - snooping by staff, and
  - targeted network attacks (external hackers).

Your organization should have a written privacy policy and protocols so that staff know what to do in the event of a breach. Be sure to state who should be involved (such as the privacy officer), and who should receive a report of the breach.

There are four steps your organization should take when responding to a suspected privacy breach: containment, risk assessment, notification, and prevention.

1. **Containment** (This step stops the breach)
   - Recover the records, stop the unauthorized access, shut down the system that was breached, revoke or change computer access codes, search for the lost USB…
   - Contact your Privacy Officer and initiate your Breach Management Policy, which may include conducting an investigation.

- Investigate the cause of the breach and the extent of the breach to ensure containment. This may require an audit of physical and technical security.
- Notify the police if the breach involves theft or other criminal activity.

2. **Risk assessment** (Now it's time to evaluate the risk of harm to affected individuals)
   - How sensitive is the personal information? Here, context is important. Medical or financial information is much more sensitive, for example, than a name and address in a phone book. However, the same name and address on a list of clients receiving counselling or treatment is considerably more sensitive.
   - If the personal information was on a stolen laptop or memory stick, was the device encrypted?
   - Is this a systemic problem, like snooping by an employee, or an isolated incident, such as a wrong email address?
   - Who has the information now?
   - Has the information been recovered?
   - How many individuals are affected?
   - What harm to the individuals could result from the breach? Think about the potential for identity theft or fraud, hurt or humiliation, damage to reputation, loss of business or employment opportunity.

3. **Notification** (This step is based on risk assessment)

If your risk assessment suggests the breach could reasonably be expected to cause harm to the individuals whose personal information was involved, your organization should notify those individuals as soon as possible following the discovery of the breach.

- Direct notification is preferred – by phone, letter, or in person. Indirect notification (such as posting a notice on your website or at your business, or through a media report) should only occur if direct notice could cause further harm to the affected individuals, is cost prohibitive for your organization, or you don't have contact information for the affected individuals.
- Notification should include:
  - the date of the breach.
  - a description of the breach and the PI affected.
  - the potential risk of harm to affected individuals. Be specific about types of potential harms and the likelihood they will occur.
  - steps you've taken to control or reduce the risk of harm,
  - steps you plan to take to prevent further breaches; and
  - contact information for someone in your organization who can answer questions, as well as contact info for the OIPC.
  - You should also let individuals know that they have a right to complain to the OIPC. If your organization reported the breach to the OIPC, include this detail in the notification, too.

4. **And finally, prevention**. Prevention will help you avoid further breaches.
    - Use the results from your investigation of the cause and extent of the breach to develop (or improve) adequate long-term safeguards against further breaches.
    - Review and update policies to reflect the lessons learned from the investigation.
    - Train your staff so they know and understand the individual and organizational privacy obligations under PIPA.

Now that we've gone over the basic steps to take when a breach occurs, let's talk about when your organization should report a breach to the OIPC. Remember the questions we asked in step 2 on risk assessment? The considerations for reporting to the OIPC are very similar. Here are some questions to help you decide whether to report to us:

- First of all, how sensitive is the PI?
- Could it be used to commit identity theft or fraud?
- Is there a reasonable chance of other harms to individuals whose PI was involved in the disclosure (what about hurt or humiliation, damage to reputation, loss of business or employment opportunity)?
- How many people are affected by the breach?
- Was the PI fully recovered without further disclosure?
- Does your organization require assistance through any of the steps for responding to the breach? And
- Do you have any questions about whether the steps you have implemented comply with your obligations under PIPA?

If you have any questions about responding to a potential breach, give us a call. If you know you want to report the breach, you can also fill out and submit the Privacy Breach Checklist found in the Privacy Breaches: Tools and Resources guidance document on our website. We're here to help.