Privacy breach quick reference guide for small and medium-sized businesses

April 2026

Organizations in British Columbia are subject to the *Personal Information Protection Act* (PIPA). PIPA has rules for how and when organizations can collect, use and/or disclose personal information (i.e. information about identifiable individuals, such as their name, account numbers, photographs, etc.). This can include information about customers, employees, patients, etc. Organizations also need to make reasonable security arrangements to protect personal information.

The Office of the Information and Privacy Commissioner (OIPC) of British Columbia oversees and enforces the administration of PIPA. This means that the OIPC investigates privacy complaints, including whether organizations have reasonable safeguards to protect personal information as required by PIPA.

When personal information is collected, used, disclosed or destroyed in contravention of PIPA it is called a "privacy breach." Even with reasonable safeguards, privacy breaches can still happen.

The most common privacy breaches happen when personal information is stolen, lost or mistakenly disclosed. When this occurs, organizations need to take steps to contain the breach, mitigate harms, and prevent any reoccurrence.

This reference guide explains how to respond to privacy breaches, and how the OIPC can help.

What to do in the event of a privacy breach?

There are four steps to responding to a privacy breach.

1. Containment

Take immediate, common-sense steps to limit the breach, such as stopping the unauthorized practice, recovering the records, shutting down the system that was breached, revoking or changing computer access codes or correcting weaknesses or gaps in physical or online security.

Designate an individual to lead the initial investigation and make recommendations. This could include individuals such as your privacy officer and/or the person responsible for security.

Do not compromise the ability to investigate the breach and be careful not to destroy evidence that may be valuable in determining the cause or that will allow you to take corrective action.

Notify the police if the breach involves theft or other criminal activity.

2. Risk assessment

To determine what other steps are immediately necessary, you must assess the risk.

Factors to consider include the personal information compromised (type and volume) and the potential for that information to be used for fraudulent or other harmful purposes. For example,

inappropriately accessed financial data or other sensitive information could be used for identity theft, financial loss or to damage reputations or relationships.

The context of the breach can also matter. For example, a simple list of customers in one context may not be as potentially harmful as in another, such as in the case of a mental health clinic.

You should also assess the cause and extent of the breach. For example, whether it was caused by malicious activity that indicates the possibility of further harm, and to what extent the breach has been contained (e.g. have the records been recovered or securely destroyed by a party who received them in error; were the records password protected or encrypted, etc.).

Be sure to document your risk assessment.

3. Notification to affected individuals and reporting to the OIPC
Notification to affected individuals can be an important mitigation strategy.

A key consideration is whether notification can help to mitigate harm(s) to an individual whose personal information has been inappropriately collected, used or disclosed.

Other considerations in determining whether to notify individuals include legal or contractual obligations; a risk of significant harm (financial loss, hurt or humiliation, etc.); and to maintain confidence in the organization and/or for good customer-client relations.

Organizations can report breaches to the OIPC. When this happens, the OIPC will monitor the organization's breach response and can provide information about best practices. The OIPC may also investigate what occurred and decide whether the breach response was compliant with PIPA and make recommendations. Reporting to the OIPC where there is a significant risk of harm shows due diligence by the organization, allows them to leverage OIPC expertise, and helps the OIPC better understand and respond to the threats facing organizations across BC.

Information on reporting to the OIPC and what to include in a notice is on the OIPC website.

4. Prevention
Conduct a review of what occurred and how the breach happened. This should help to identify what administrative, technical and/or physical measures need to be improved or put in place to prevent this kind of breach from re-occurring, and guides steps for prevention.

Additional resources available on the OIPC website

- OIPC Privacy Right education program for businesses
- Privacy Breach Checklist for private organizations
- Securing Personal Information: A Self-Assessment Tool for Public Bodies and Organizations
- Getting Accountability Right with a Privacy Management Program