Privacy breaches: tools and resources for the private sector

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Purpose of this guidance document

Use this document to take action when a privacy breach has occurred. These key steps are applicable to private organizations under the *Personal Information Protection Act* (PIPA). For public bodies, see Privacy breaches: tools and resources for public bodies.

This guidance also includes an assessment tool to evaluate your organization's response to a privacy breach, and to decide whether to report the breach to the Office of the Information and Privacy Commissioner (OIPC). To report a privacy breach to the Office of the Information and Privacy Commissioner for BC, use the online form or send a privacy breach checklist to info@oipc.bc.ca.

What is a privacy breach?

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure, or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of PIPA.

The most common privacy breach happens when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed – for example, when a computer is stolen or when personal information is mistakenly emailed to the wrong person.

There are four key steps in responding to a privacy breach. The first three steps must be undertaken as soon as possible following the breach. The fourth step provides recommendations for longer-term solutions and prevention strategies:

- Step 1: Contain the breach
- Step 2: Evaluate the risks
- Step 3: Notification
- Step 4: Prevention

Step 1: Contain the breach

Take immediate, common-sense steps to limit the breach, including:

- Immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, revoking or changing computer access codes or correcting weaknesses in physical security.
- Activate your breach management policy. If you do not have a breach management policy take the following steps:
    - Designate an appropriate individual to lead the initial investigation. This individual should have the authority within the organization to conduct the initial investigation and make initial recommendations. If necessary a more detailed investigation may subsequently be required.

  - Immediately contact your Privacy Officer and/or the person responsible for security in your organization. Determine others who need to be made aware of the incident internally at this preliminary stage.
  - Determine whether a breach response team must be assembled, which could include representatives from appropriate business areas and should include the Privacy Officer and/or person responsible for security.
  - Notify the police if the breach involves theft or other criminal activity.
- Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or that will allow you to take appropriate corrective action.

Step 2: Evaluate the risks

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

Consider the following factors:

Personal information involved

- What data elements have been breached? Generally, the more sensitive the data, the higher the risk. Some types of personal information are more sensitive than others (e.g. health information, government-issued pieces of identification, such as social insurance numbers, driver's licence and health care numbers and financial account numbers, such as credit or debit card numbers that could be used for identity theft.) A combination of personal information is typically more sensitive than a single piece of personal information.
- What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?
- What is the context of the personal information involved? For example, name and address in a phone book would be less sensitive than name and address on a list of clients receiving counselling or a list of clients away on holiday.

Cause and extent of the breach

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- Was the information lost or stolen? If it was stolen, can it be determined whether the information was the target of the theft?
- Is the information encrypted or otherwise not readily accessible?

- Has the information been recovered? What steps have you already taken to minimize the harm?
- Is this a systemic problem or an isolated incident?

Individuals or others affected by the breach

- How many individuals are affected by the breach?
- Who was affected by the breach: employees, members of the public, contractors, clients, service providers, other organizations?

Foreseeable harm from the breach

- Who is in receipt of the information? For example, a stranger who accidentally receives personal information and voluntarily reports the mistake is less likely to misuse the information than an individual suspected of criminal activity.
- Is there any relationship between the unauthorized recipients and the data subject? A close relationship between the victim and the recipient may increase the likelihood of harm – an estranged spouse is more likely to misuse information than a neighbour.
- What harm to individuals could result from the breach? Harm that may occur includes:
  - security risk (e.g. physical safety)
  - identity theft or fraud
  - loss of business or employment opportunities
  - hurt, humiliation, damage to reputation or relationships
- What harm to the organization could result from the breach?
  For example:
  - loss of trust in organization
  - loss of assets
  - financial exposure
  - loss of contracts/business
- What harm to the public could result from the breach? For example:
  - risk to public health
  - risk to public safety

Step 3: Notification

Notification of affected individuals can be an important mitigation strategy in the right circumstances. A key consideration is whether notification avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed.

Review your risk assessment to determine whether notification is appropriate. The OIPC has created a Breach Notification Assessment Tool to assist organizations to make this determination.

Notifying affected individuals

Some considerations in determining whether to notify individuals affected by the breach include:

- Legislation requires notification;
- Contractual obligations require notification;
- There is a risk of identity theft or fraud (usually because of the type of information lost/stolen/accessed/disclosed, such as SIN, banking information, identification numbers);
- There is a risk of physical harm (if the loss puts an individual at risk of stalking or harassment);
- There is a risk of hurt, humiliation or damage to reputation (for example, when the information lost includes medical or disciplinary records);
- There is a risk of loss of business or employment opportunities (if the loss of information could result in damage to the reputation of an individual, affecting business or employment opportunities).
- There is a risk of loss of confidence in the organization and/or good customer/client relations dictates that notification is appropriate.

When and how to notify

Notification should occur as soon as possible following the breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation. Direct notification is preferred – by phone, by letter or in person. Indirect notification – via websites, posted notices, or media reports – should generally only occur where direct notification could cause further harm, is cost prohibitive or contact information is lacking. Indirect notification should generally contain the same information as in a direct notification. Using multiple methods of notification in certain cases may be the most effective approach.

What should be included in the notification?
Notifications should include the following pieces of information:

- Name of organization;
- Date the breach came to the attention of the organization;
- Description of the breach, including any potential harms;
- Description of the personal information involved;
- The steps taken so far to control or reduce the harm;
- Steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch);
- Contact information of an individual within the organization who can answer questions or provide further information;
- If the organization has already contacted the Privacy Commissioner, include this detail in the notification letter.

Other sources of information
As noted above, the breach notification letter should include a contact number within the organization in case affected individuals have further questions. In anticipation of further calls, you should prepare a list of frequently asked questions and answers to assist staff responsible for responding to these inquiries.

Others to contact
Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

- Police: if theft or other crime is suspected;
- Insurers or others: if required by contractual obligations;
- Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies;
- Other internal or external parties not already notified: Your investigation and risk analysis may have identified other parties impacted by the breach such as third-party contractors, internal business units or unions;
- Office of the Information and Privacy Commissioner: The following factors are relevant in deciding when to report a breach to the OIPC:
    - the sensitivity of the personal information;
    - whether the disclosed information could be used to commit identity theft;
    - whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses;

- the number of people affected by the breach;
- whether the information was fully recovered without further disclosure;
- your organization requires assistance in developing a procedure for responding to the privacy breach, including notification and/or, to ensure steps taken comply with the obligations under privacy legislation.

To notify the Office of the Information and Privacy Commissioner, you must complete the online breach reporting form or a Privacy Breach Checklist. The OIPC will collect and use this submitted information to examine the reported breach. This can include formally investigating the circumstances around any privacy breach reported to the OIPC.

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long-term safeguards against further breaches.

Policies should be reviewed and updated to reflect the lessons learned from the investigation and regularly after that. Your resulting plan should also include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

Staff of organizations should be trained to know the organization's privacy obligations under PIPA.

Additional resources

For more information on securing your personal information, see our self-assessment tool for public bodies and organizations: https://www.oipc.bc.ca/guidance-documents/1439

We also have a webinar for privacy sector on breaches.
https://www.oipc.bc.ca/privacyright/webinars/webinar-8/

Appendix 1: Privacy breach management: policy template

Policy Date: (Most current policy review date)

Contact: Contact information for individuals with questions about the policy and to identify the program area responsible for the policy.

Purpose: State the purpose of the policy which will likely include:

- Obligation of all staff to report privacy breaches
- To describe process for managing privacy breaches
- To assign responsibilities and timelines

Document Owner: Program area and position responsible

Policy Applies to: Identify staff and/or contractors subject to policy

Process Responsibility: Likely the Privacy Officer

Final Accountability: Identify the management position responsible

Policy Scope: When does the policy apply?

Definitions: Include definitions of key words such as “personal information" and “privacy breach”

Action Plan/Steps in Managing a Privacy Breach

Set out the steps in managing a privacy breach. For each step, set out the action required, the individual responsible and the recommended time lines. The next page lists some recommended actions and suggested responsible positions and timelines.

Action required	Position responsible	Recommended timelines
1. Contain the breach	Program area where breach occurred	Immediate
2. Report the breach within the organization	• Program area staff (report to management • Management (report to Privacy Officer) • PO report to executive as required	Same day as breach occurred
3. Designate lead investigator and select breach response team as appropriate	Privacy Officer	Same day as breach discovered
4. Preserve the evidence	Lead Investigator, Privacy Officer	Same day as breach discovered
5. Contact police if necessary	Privacy Officer	Same day as breach discovered
6. Conduct preliminary analysis of risks and cause of breach	Lead Investigator	Within 2 days of breach discovery
7. Determine if the breach should be reported to the Privacy Commissioner	Privacy Officer in consultation with executive	Generally within 2 days of breach
8. Take further containment steps if required based on preliminary assessment	Lead Investigator or Privacy Officer	Within 2 days of breach
9. Evaluate risks associated with breach	Lead Investigator or Privacy Officer	Within 1 week of breach
10. Determine if notification of affected individuals is required	Privacy Officer	Within 1 week of breach
11. Conduct notification of affected Individuals	Privacy Officer or program area manager	Within 1 week of breach
12. Contact others as appropriate	Privacy Officer or program area manager	As needed
13. Determine if further in-depth investigation is required	Privacy Officer or program area manager	Within 2 to 3 weeks of the breach
14. Conduct further investigation into cause and extent of the breach if necessary	Privacy Officer, security officer or outside	Within 2 to 3 weeks of the breach
15. Review investigative findings and develop prevention strategies	independent auditor or investigator	Within 2 months of breach
16. Implement prevention strategies	Privacy Officer or program area manager	Depends on the strategy
17. Monitor prevention strategies.	Privacy Officer or program area manager	Annual privacy/security audits

Roles and Responsibilities
List the roles and responsibilities by position type

Tools
Develop and attach a breach reporting form for program areas.

Develop and attach checklists as appropriate for investigators.

Develop and attach a template breach notification letter that includes the following elements:

- Name of organization;
- Date the breach came to the attention of the organization; Date of the breach;
- Description of the breach, including any potential harms;
- Date on which or the period during which the privacy breach occurred
- Description of the personal information involved
- If the public body or organization has already contacted the Privacy Commissioner, include this detail in the notification letter.
- Contact information of an individual within the public body or organization who can answer questions or provide further information;
- Description of steps that have been or will be taken to reduce the risk of harm to the affected individual;
- Description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

Related Policies
The organization should have in place policies related to security of personal information, including:

- General operational security standards
- Network access and security
- Data protection
- Security on portable storage devices
- Travelling with personal information
- Secure destruction of personal information

Appendix 2: Breach Notification to Affected Individuals Assessment Tool[1]

Organizations that collect and hold personal information are responsible for notifying affected individuals when a privacy breach occurs. If the breach occurs at a third party entity that has been contracted to maintain or process personal information, the breach should be reported to the originating entity, which has primary responsibility for notification. This Notification Assessment Tool takes organizations through four decision-making steps regarding notification:

Step 1: Notifying Affected Individuals

Use this chart to help you decide whether you should notify affected individuals. If either of the first two factors listed below applies, notification of the individuals affected must occur. The risk factors that follow are intended to serve as a guide. If none of these applies, no notification may be required. You must use your judgment to evaluate the need for notification of individuals.

[1] This tool was originally developed in collaboration with the Information and Privacy Commissioner of Ontario.

Consideration	Check if applicable
1. Legislation requires notification Are you or your organization covered by legislation that requires notification of the affected individual? If you are uncertain, contact the Information and Privacy Commissioner (see contact information at the end of this publication).	
2. Contractual obligations Do you or your organization have a contractual obligation to notify affected individuals in the case of a data loss or privacy breach?	
3. Risk of identity theft Is there a risk of identity theft? How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information and any other information that can be used for fraud by third parties (e.g. financial).	
4. Risk of bodily harm Does the loss of information place any individual at risk of physical harm, stalking or harassment?	
5. Risk of hurt, humiliation, damage to reputation Could the loss of information lead to hurt, humiliation or damage to an individual's reputation? This type of harm can occur with the loss of information such as mental health records, medical records or disciplinary records.	
6. Loss of business or employment opportunities Could the loss of information result in damage to the reputation to an individual, affecting business or employment opportunities?	

Step 2: When and How to Notify Affected Individuals

When
Notification should occur as soon as possible following a breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How
The preferred method of notification is direct – by phone, letter or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

The charts below set out factors to consider in deciding how to notify the affected individuals.

Considerations favouring direct notification of affected individuals	Check if applicable
The identities of the individuals are known.	
Current contact information for the affected individuals is available.	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach.	
Individuals affected by the breach may have difficulty understanding and are better served through direct notice.	

Considerations favouring indirect notification of individuals	Check if applicable
A very large number of individuals are affected by the breach such that direct notification could be impractical.	
Direct notification could compound the harm to the individual resulting from the breach.	

Step 3: What to Include in the Notification of Affected Individuals

The information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include the information set out below:

Information required	Check information included
Name of organization	
Date the breach came to the attention of the organization	
Date on which or the period during which the privacy breach occurred	
Description of the breach. A general description of what happened, including any potential harms.	
Description of the personal information involved. Describe the information inappropriately accessed, collected, used or disclosed.	
Description of steps that have been or will be taken to reduce the risk of harm to the affected individual;	
Steps the individual can take. Provide information about how individuals can protect themselves, e.g. how to contact credit reporting agencies (to set up credit watch).	
Privacy Commissioner contact information. If the organization has already contacted the Privacy Commissioner, include this detail in the notification letter.	
Organization contact information for further assistance. Contact information for someone within your organization who can provide additional information and assistance and answer questions.	

Step 4: Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach. Do not share personal information with these other entities unless required.

Authority or organization	Purpose of contacting	Check if applicable
Law Enforcement	If theft or other crime is suspected. (Note: The police may request a temporary delay in notifying individuals, for investigative purposes.)	
Office of the Information and Privacy Commissioner **250-387-5629** **info@oipc.bc.ca** oipc.bc.ca	For assistance with developing a procedure for responding to the privacy breach, including notification. To ensure steps taken comply with the organization's obligations under privacy legislation.	
Professional or regulatory Bodies	If professional or regulatory standards require notification of the regulatory or professional body.	
Technology suppliers	If the breach was due to a technical failure and a recall or technical fix is required.	