Privacy Breaches: Tools and Resources

Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Contents

1	**Key Steps in Responding to Privacy Breaches**	3
	Step 1: Contain the Breach	4
	Step 2: Evaluate the risks	5
	Step 3: Notification	7
	Step 4: Prevention	10
2	**Privacy Breach Checklist**	11
3	**Privacy Breach Management: Policy Template**	17
4	**Breach Notification Assessment Tool**	20

1 Key Steps in Responding to Privacy Breaches

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 the *Personal Information Protection Act* or part 3 of the *Freedom of Information and Protection of Privacy Act*.

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

Use this document to take action when a privacy breach has occurred. These key steps are applicable to both public bodies and private organizations.

» This document is for general information only. It is not intended to be, and cannot be relied upon as, legal advice or other advice. Its contents do not fetter, bind or constitute a decision or finding by, the Office of the Information and Privacy Commissioner ("OIPC") with respect to any matter, including any complaint, investigation or other matter, respecting which the OIPC will keep an open mind. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization and public body.

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 public body or 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.[1]
    - 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.

1 Steps that Ministries must follow when responding to a privacy breach are described in the BC Government's "Process for Responding to Privacy Breaches" document, which can be accessed at www.cio.gov.bc.ca/cio/information_incident/.

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 personal information is 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 or not?
- 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 affected by the breach

- How many individuals are affected by the breach?
- Who was affected by the breach: employees, 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 the individuals will 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 could result to the public body or organization as a result of the breach? For example:
    - loss of trust in the public body or organization
    - loss of assets
    - financial exposure
    - loss of contracts/business
- What harm could result to the public as a result of 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 is necessary in order to 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 public bodies and organizations make this determination.

Notifying affected individuals

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. 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 public body or 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.

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:

- Date of the breach;
- Description of the breach;
- Description of the information inappropriately accessed, collected, used or disclosed;
- Risk(s) to the individual caused by the breach;
- The steps taken so far to control or reduce the harm;
- Future steps planned to prevent further privacy breaches;
- 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, information explaining how to change a personal health number or driver's licence number);
- Contact information of an individual within the public body or organization who can answer questions or provide further information;
- Privacy Commissioner contact information and the fact that individuals have a right to complain to the Office of the Information and Privacy Commissioner. If the public body or 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 public body or 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 the further 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 or public body requires assistance in developing a procedure for responding to the privacy breach, including notification and/or,
    - to ensure steps taken comply with the organization's or public body's obligations under privacy legislation.

To notify the Office of the Information and Privacy Commission, you must complete the "Privacy Breach Checklist."

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 the *Personal Information Protection Act*. Staff of public bodies should be trained to know the public body's privacy obligations under the *Freedom of Information and Protection of Privacy Act*.

Additional resources

For more ideas on how to prevent privacy breaches, consult the OIPC personal information security guidelines at:

http://www.oipc.bc.ca/pdfs/private/PhysicianSecurityofpersonalinformation.pdf

2 Privacy Breach Checklist

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 the *Personal Information Protection Act* or part 3 of the *Freedom of Information and Protection of Privacy Act.*

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

Step 15 of the Checklist will help you decide whether to report the breach to the OIPC.

If you are reporting the breach to the OIPC, you must answer every question on this form. If a question does not apply to your situation, write "N/A." If you do not know the answer, write "unknown." Fax a completed copy, including any other necessary information, to (250) 387-1696. The OIPC will contact you after we receive this form.

Use this form to evaluate your public body or 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").

Privacy Breach Checklist

Date of report: _____

Contact information

Public Body / Organization: _____

Contact Person: _____

Name: _____

Title: _____

Phone: _____ Fax: _____

E-Mail: _____

Mailing address: _____

_____

_____

Risk evaluation

Incident Description

1. Describe the nature of the breach and its cause:

_____

_____

_____

2. Date of incident:

_____

_____

_____

3. Date incident discovered:

_____

_____

_____

4. Location of incident:

_____

_____

_____

5. Estimated number of individuals affected:

_____

_____

_____

6. Type of individuals affected:

_____

_____

_____

- ☐ Client / Customer / Patient
- ☐ Employee
- ☐ Student
- ☐ Other: _____

Personal Information Involved

7. Describe the personal information involved (e.g. name, address, SIN, financial, medical) (Do **not** include or send us identifiable personal information):

_____

_____

_____

Safeguards

8. Describe physical security measures (locks, alarm systems etc.):

_____

_____

9. Describe technical security measures:

☐ Encryption

☐ Password

☐ Other (Describe) _____

Describe organizational security measures (security clearances, policies, role-based access, training programs, contractual provisions):

_____

_____

Harm from the Breach

10. Identify the type of harm(s) that may result from the breach:

☐ **Identity theft**
(most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information and any other information that can be used to commit financial fraud)

☐ **Risk of physical harm**
(when the loss of information places any individual at risk of physical harm, stalking or harassment)

☐ **Hurt, humiliation, damage to reputation**
(associated with the loss of information such as mental health records, medical records, disciplinary records)

☐ **Loss of business or employment opportunities**
(usually as a result of damage to reputation to an individual)

☐ **Breach of contractual obligations**
(contractual provisions may require notification of third parties in the case of a data loss or privacy breach)

☐ **Future breaches due to similar technical failures**
(notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)

☐ **Failure to meet professional standards or certification standards**
(notification may be required to professional regulatory body or certification authority)

☐ **Other (specify):** _____

_____

Notification

11. Has your Privacy Officer been notified?

☐ Yes Who was notified and when? _____

☐ No When to be notified? _____

12. Have the police or other authorities been notified (e.g. professional bodies or persons required under contract)?

☐ Yes Who was notified and when? _____

☐ No When to be notified? _____

13. Have affected individuals been notified?

☐ Yes Manner of notification: _____

Number of individuals notified: _____

Date of notification: _____

☐ No Why not? _____

14. What information was included in the notification?

☐ Date of the breach

☐ Description of the breach

☐ Description of the information inappropriately accessed, collected, used or disclosed

☐ Risk(s) to the individual caused by the breach

☐ Steps taken so far to control or reduce the harm

☐ Future steps planned to prevent further privacy breaches

☐ Steps the individual can take to reduce the harm

☐ Privacy Commissioner contact information

☐ Organization contact information for further assistance

15. Should the Office of the Information and Privacy Commissioner be notified of the breach? Consider the following factors:

- ☐ The personal information involved is sensitive
- ☐ There is a risk of identity theft or other harm including pain and suffering or loss of reputation
- ☐ A large number of people are affected by the breach
- ☐ The information has not been fully recovered
- ☐ The breach is the result of a systemic problem or a similar breach has occurred before
- ☐ Your organization or public body requires assistance in responding to the privacy breach
- ☐ You want to ensure that the steps taken comply with the organization's or public body's obligations under privacy legislation

If you are reporting this breach to the OIPC, please include a copy of the notification letter.

Prevention

16. Describe the immediate steps taken to contain and reduce the harm of the breach (e.g. locks changed, computer access codes changed or revoked, computer systems shut down):

_____

_____

_____

17. Describe the long-term strategies you will take to correct the situation (e.g. staff training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security):

_____

_____

_____

If you have completed a security audit and are reporting this breach to the OIPC please forward a copy of the audit with your report.

3 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 or public body	• Program area staff (report to management) • Management (report to Privacy Officer) • PO report to executive as required	Same day as breach discovered
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 independent auditor or investigator	Within 2 to 3 weeks of the breach
15. Review investigative findings and develop prevention strategies	Privacy Officer or program area manager	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:

- Date of the breach
- Description of the breach
- Description of the information inappropriately accessed, collected, used or disclosed
- Risk(s) to the individual caused by the breach
- Steps taken so far to control or reduce the harm
- Future steps planned to prevent further privacy breaches
- Steps the individual can take to reduce the harm
- Privacy Commissioner contact information
- Organization contact information for further assistance

Related Policies

The public body or 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

4 Breach Notification Assessment Tool

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Information and Privacy Commissioner, Ontario, Canada

The Information and Privacy Commissioners for British Columbia and Ontario have jointly produced this *Notification Assessment Tool* to assist you in making key decisions after a privacy breach occurs. It should be read along with:

B.C.: Key Steps in Responding to Privacy Breaches

Ontario: *What to do if a privacy breach occurs: Guidelines for government organizations*, http://www.ipc.on.ca/images/Resources/up-prbreach.pdf
What to do When Faced With a Privacy Breach: Guidelines for the Health Sector, http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf

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

Step 2: When and How to Notify

Step 3: What to Include in the Notification

Step 4: Others to Contact

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.

	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 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 physical 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 chart below sets 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 an indirect notification (due to mental capacity, age, language, etc.)	

CONSIDERATIONS FAVOURING INDIRECT NOTIFICATION OF AFFECTED 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	CONFIRM INFORMATION INCLUDED
Date of the breach.	
Description of the breach. A general description of what happened.	
Description of the information. Describe the information inappropriately accessed, collected, used or disclosed.	
Steps taken so far to control or reduce the harm.	
Future steps planned to prevent further privacy breaches.	
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), information explaining how to change a personal health number or driver's licence number.	
Privacy Commissioner contact information. Include information about how to complain to the Privacy Commissioner.	
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

Contact Information

For public and private sector bodies in British Columbia:

Office of the Information and Privacy Commissioner for British Columbia

250.387.5629

info@oipc.bc.ca
www.oipc.bc.ca

For public and health care sectors in Ontario:

Information and Privacy Commissioner, Ontario

416.326.3333 or
1.800.387.0073

info@ipc.on.ca
www.ipc.on.ca

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.)	
Privacy Commissioner's Office	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.	

Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner for British Columbia

PO Box 9038, Stn. Prov. Govt. Victoria, BC V8W 9A4 | Telephone: 250.387.5629 | Toll free in B.C. 1.800.663.7867
E-mail: info@oipc.bc.ca | www.oipc.bc.ca