SECURITY

February 2023

Privacy breaches: tools and resources for public bodies

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 apply to public bodies under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and have been updated to include information about the legislation's mandatory breach notification requirements.

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.

For private organizations' obligations under the *Personal Information Protection Act*, please see *Privacy breaches: tools and resources for private sector organizations.*

What is a privacy breach?

A privacy breach means the theft or loss, or the collection, use, or disclosure of personal information in the custody or under the control of a public body in contravention of Part 3 of FIPPA.[1]

The most common privacy breach happens when personal information 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. Notification to the affected individuals and/or the OIPC can be mandatory or voluntary, depending on the circumstances. 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 process for responding to breaches. Having a documented process for responding to breaches is a required component of a public body's privacy management

[1] Based on the definition in s. 36.3(1) of FIPPA.

program.[2] If you do not yet have a breach management process take the following steps: [3]

- Designate an appropriate individual to lead the initial investigation. This individual should have the authority within the public body 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. 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, including the potential need to notify affected individuals and/or the OIPC, you must assess the risks and harms involved in the breach.

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.

[2] See BC Government's privacy management program direction: https://alpha.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/pmp_ministerial_direction_2023.pdf

[3] Steps that Ministries must follow when responding to a privacy breach are described in the BC Government's "Privacy Breaches" webpage: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-breaches

- 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 public directory would be less sensitive than name and address on a list of individuals receiving income or disability assistance.

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 or public bodies?

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 where there is reason to believe an individual is involved in 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:
    - identity theft, or significant:
        - bodily harm;
        - humiliation;
        - damage to reputation or relationships;

    - loss of employment, business or professional opportunities;
    - financial loss;
    - negative impact on a credit record; or
    - damage to, or loss of, property.[4]
- What harm to the public body could result from the breach?
  For example:
    - Loss of trust in the public body;
    - Loss of assets;
    - Financial exposure;
- What harm to the public could result from the breach? For example:
    - risk to public health
    - risk to public safety

Below are some examples of breaches that could result in significant harm and notification would likely be required:

- Social assistance or financial documents were sent to the wrong client.
- Records released as part of an access requests where the sensitive personal information of a third party was left unredacted.
- A camera with unencrypted images of client registrations was lost.
- A file containing notes that include personal information of those involved in an investigation went missing.
- Student grades or job evaluation materials were disclosed to the wrong parties or exposed online.
- A phone containing unencrypted personal contact information of law enforcement officials was stolen.

Step 3: Notification

Notification of affected individuals can be an important mitigation strategy in the right circumstances. In certain circumstances, notification to individuals and/or the OIPC is mandatory.

Public bodies must notify an affected individual and the Commissioner if a breach could reasonably be expected to result in significant harm to the individual. The types of harms that could fall into this category are listed in section 36.3(2) of the Act.

[4] These are the harms listed in s. 36(3)(2)(a) of FIPPA. And while they are indicative of the kinds of harm that could trigger mandatory breach notifications, there may be other harms as well that are not included in the list but may be relevant in a public body's decision making.

Notice given under this section must occur without unreasonable delay.

If public bodies are unsure if notification is required based on the criteria in the Act, they may still choose to notify based on an abundance of caution. This may be especially relevant if the breach involves a large number of individuals.

The exception to the requirement to notify is limited to cases where giving notice could reasonably be expected to result in immediate and grave harm to the individual's safety or physical or mental health, or threaten another individual's safety or physical or mental health.

Notice must be given to individuals in the prescribed manner, as set out in s. 11.1 of the FIPPA Regulation. This means that it needs to be given directly to the affected individual in writing, and include the following:

> (i) the name of the public body;
>
> (ii) the date on which the privacy breach came to the attention of the public body;
>
> (iii) a description of the privacy breach including, if known,
>
> > (a) the date on which or the period during which the privacy breach occurred, and
> >
> > (b) a description of the nature of the personal information involved in the privacy breach;
>
> (iv) confirmation that the Commissioner has been or will be notified of the privacy breach;
>
> (v) contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
>
> (vi) a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;
>
> (vii) a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

The Regulation also sets out the limited circumstances in which a notice can be given indirectly. This manner of notice can be given by public communication that can reasonably be expected to reach the affected individual, and must include the same information that is required to be provided when giving direct notification (e.g. name of the public body, description of the breach, etc.).

In all cases, including when notice is not required to be given due to concerns about an individual's safety or physical or mental health, notification must be given to the OIPC.

That notice must include the prescribed information listed in s. 11. 2 of the FIPPA Regulation, which includes the following:

> (a) the name of the public body;
>
> (b) the date on which the privacy breach came to the attention of the public body;
>
> (c) a description of the privacy breach including, if known,
>
> > (i) the date on which or the period during which the privacy breach occurred;
> >
> > (ii) a description of the nature of the personal information involved in the privacy breach; and
> >
> > (iii) an estimate of the number of affected individuals;
>
> (d) contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
>
> (e) a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individuals.

Breach notification requirements do not preclude public bodies from notifying individuals in other situations or other parties who could be impacted by a breach. For example, it may be the case that notification should occur due to other rules or requirements, such as a contractual agreement.

Other parties who could be notified of a breach include:

- 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.

To notify the Office of the Information and Privacy Commissioner, please complete the online reporting form or 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.

As part of its privacy management program, a public body must train its employees on its privacy obligations under FIPPA.

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

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 public body	• 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	Without unreasonable delay (e.g. 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	Without unreasonable delay (e.g. 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:

- The name of the public body;
- The date on which the privacy breach came to the attention of the public body;
- A description of the privacy breach including, if known,
    - the date on which or the period during which the privacy breach occurred; and
    - a description of the nature of the personal information involved in the privacy breach;
- Confirmation that the Commissioner has been or will be notified of the privacy breach;
- Contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- A description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;
- A 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 public body 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[5]

Public bodies 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 public bodies 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 a privacy breach could reasonably be expected to result in any of the harms listed below notification to the affected individual and to the OIPC must occur. Limited exceptions to the requirement to notify individuals are also listed below.

Consideration	Check if applicable
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)	
Bodily harm (when the loss of information places any individual at risk of physical harm, stalking or harassment)	
Humiliation (associated with the loss of information such as medical records, disciplinary records)	
Damage to reputation or relationships	
Loss of employment, business or professional opportunities. (usually as a result of damage to reputation to an individual)	
Financial loss	
Negative impact on a credit record	
Damage to, or loss of, property	

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

Notification to individuals is *not required* if it could reasonably be expected to result in one of the following:

- Immediate and grave harm to the individual's safety or physical or mental health
- Threaten another individual's safety or physical or mental health

Step 2: When and How to Notify Affected Individuals

When

Notification must occur without unreasonable delay. 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

Notification must be direct and in writing. It must include each of the required elements listed in Step 3 below (as set out in s. 11.1(1)(b) of the FIPPA Regulation).

Indirect notification – website information, posted notices, media releases, etc. – can only occur if one or more of the following circumstances apply:

Requirements for indirect notification of individuals	Check if applicable
The public body does not have accurate contact information for the affected individual.	
The head of the public body reasonably believes that providing the notice directly to the affected individual would unreasonably interfere with the operations of the public body.	
The head of the public body reasonably believes that the information in the notification will come to the attention of the affected individual more quickly if it is given in an indirect manner.	

Indirect notification must be given by public communication that can reasonably be expected to reach the affected individual, and include the same information required for direct notice (see the list below).

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
The name of the public body	
The date on which the privacy breach came to the attention of the public body	
A description of the privacy breach including, if known, **the date on which or the period during which the privacy breach occurred,** **and a description of the nature of the personal information involved in the privacy breach**	
Confirmation that the Commissioner has been or will be notified of the privacy breach	
Contact information for a person who can answer, on behalf of the public body, questions about the privacy breach	
A description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual	
A description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.	

Step 4: Notifying the OIPC

Public bodies must notify the OIPC in the same circumstances in which they must notify individuals (i.e. a breach could be expected to result in one of the significant harms listed above).

Public bodies must also notify the OIPC when there is a risk of such harm but the individual is not required because it could result in immediate and grave harm to the individual's safety or physical or mental health, or threaten another individual's safety or physical or mental health.

Notice given to the OIPC must occur without reasonable delay. It needs to be in writing and include the following:

Information required	Check information included
The name of the public body	
The date on which the privacy breach came to the attention of the public body	
A description of the privacy breach including, if known, • the date on which or the period during which the privacy breach occurred; • a description of the nature of the personal information involved in the privacy breach; and • an estimate of the number of affected individuals	
Contact information for a person who can answer, on behalf of the public body, questions about the privacy breach	
A description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individuals.	

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.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867 info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy