



# Key Steps to Responding to Privacy Breaches

Nova Scotia Freedom of Information and Protection of Privacy Review Office

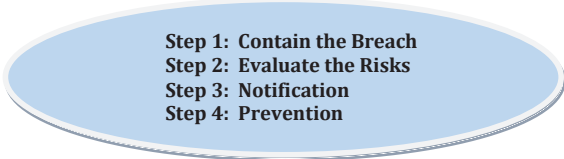


## Key Steps to Responding to Privacy Breaches<sup>1</sup>

### What is a privacy breach?

A privacy breach occurs whenever 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 *Freedom of Information and Protection of Privacy Act (FOI/POP)*, the *Municipal Government Act Part XX (MGA)* or the *Personal Health Information Act (PHIA)*.

### What are the four key steps?



**Step 1: Contain the Breach**  
**Step 2: Evaluate the Risks**  
**Step 3: Notification**  
**Step 4: Prevention**

The first three steps should be undertaken immediately upon discovery of the breach or in very quick succession. The fourth step is undertaken once the causes of the breach are known, in an effort to find longer term solutions to the identified problem.

### Purpose of the Key Steps Document

Privacy breaches take many different forms, from misdirected faxes containing tax data, to the loss of hard drives containing personal information, to medical files blowing out the back of a garbage truck. Public bodies, municipalities and health custodians in Nova Scotia should be prepared to manage their responses to privacy breaches. The four key steps to responding to privacy breaches are steps that have been adopted across most Canadian jurisdictions in both the public and private sector. They represent best privacy practices for mitigating the harm arising from a privacy breach.

Use this document in combination with the Privacy Breach checklist (p. 13 of this document) also available on our website at <http://foipop.ns.ca>.

---

<sup>1</sup> This brochure is adapted from material prepared by the Office of the Information Commissioner of British Columbia entitled: *Privacy Breaches: Tools and Resources* available at <https://www.oipc.bc.ca/tools-guidance/guidance-documents>.



## Other Resources for Health Custodians

Note that the *Personal Health Information Act* (PHIA) has particular breach notification requirements in sections 69 and 70. Included in those provisions is the expectation that notification will occur in prescribed circumstances, for events including when “information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification.” The Government of Nova Scotia has produced a *Privacy Breach Notification Decision Making Tool*, to assist custodians in determining what type of notification is required under PHIA. Breach notification is one of the four key steps discussed in this document. This document may be of assistance to health custodians in evaluating their overall response to a breach.

### Notice to Users

This document is intended to provide general information only. It is not intended, nor can it be relied upon, as legal advice. As an independent agency mandated to oversee compliance with FOIPOP, MGA and PHIA, the Freedom of Information and Protection of Privacy Review Office (Review Office) cannot approve in advance any proposal from a public body, municipality or health custodian. We must maintain our ability to investigate complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter, respecting which the Review Officer will keep an open mind. It remains the responsibility of each public body, municipality and health custodian, to ensure that they comply with their responsibilities under the relevant legislation. Contact information for the Review Officer is set out on page 22 of this document; further information about our role and mandate can be found at: <http://foipop.ns.ca>.



## Step 1: Contain the Breach

Before continuing, you should ensure that you record all steps taken to investigate and manage the breach. The privacy breach checklist tool can be used to complete all of the steps set out below and to record all relevant information. That tool is available at p. 13 of this document and at: <http://foipop.ns.ca>.

You should take immediate and common sense steps to limit the breach including:

- **Contain:** Immediately contain the breach by, for example, stopping the unauthorized practice, shutting down the system that was breached, revoking or changing computer access codes, sending a remote “kill” signal to a lost or stolen portable storage device, correcting weaknesses in physical security or searching the neighborhood or used item websites (such as Kijiji) for items stolen from a car or house.
- **Initial Investigation:** Designate an appropriate individual to lead the initial investigation. Begin this process the day the breach is discovered. 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.
- **Privacy Officer & Other Internal Notifications:** Immediately contact your Privacy Officer and the person responsible for security in your organization. Determine others who need to be made aware of the incident, internally at this stage. It is helpful to prepare in advance a list of all of the individuals who should be contacted along with current contact information.
- **Breach Response Team:** Determine whether a breach response team must be assembled which could include representatives from appropriate business areas (labour relations, legal, communications, senior management). Representatives from privacy and security should always be included and generally the privacy team is responsible for coordinating the response to the incident.
- **Police:** Notify the police if the breach involves theft or other criminal activity.
- **Preserve evidence:** 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:

- As soon as possible get a complete list of all of the personal information at risk. Generally this means developing a list of the data elements lost, stolen or inappropriately accessed. For example, the data could include, name, address, date of birth, medical diagnosis and health card number (MSI). At this stage it is important that the investigator confirm the data at risk as quickly as possible. Be aware that if the breach is caused by an error, or oversight by an employee they may be reluctant to fully disclose the scope of the lost data.
- Next, evaluate the sensitivity of the personal information. Some personal information is more sensitive than others. Generally information including: health information, government-issued pieces of information such as social insurance numbers, health care numbers and financial account numbers such as credit card numbers, is considered sensitive.
- Also consider the context of the information when evaluating sensitivity. For example, a list of customers on a newspaper carrier's route may not be sensitive. However, a list of customers who have requested service interruption while on vacation would be more sensitive.
- Finally, in your evaluation of sensitivity consider the possible use of the information. Sometimes it is the combination of the data elements that make the information sensitive or capable of being used for fraudulent or otherwise harmful purposes.
- The more sensitive the information, the higher the risk.

### Cause and Extent of the Breach:

The cause and extent of the breach must also be considered in your analysis of the risks associated with the breach. Answer all of the following questions:

- 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 personal 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

Knowing who was affected by the breach will shape your strategies in managing the breach and may also determine who will help manage the breach (e.g. union employees affected likely means labour relations should be on the breach management team), it will also determine who you decide to notify – if business partners are affected, then you will likely want to notify them.

- 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 a 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
  - Basis for potential discriminatory action that may be taken against the individual
  - Social/relational harm (damage to the individual's 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 including class action lawsuits
  - 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

Once you have assessed all of the risks described above you will be able to determine whether or not notification is an appropriate mitigation strategy. Further, the risk assessment will help you to identify appropriate prevention strategies.

The table below summarizes the risk factors and suggests a **possible** risk rating. Each public body, health custodian or municipality must make their own assessment of the risks given the unique circumstances of the situation. The table is intended to provide a rough guide to ratings.

<b>Risk Rating Overview</b>			
<b>Factor</b>	<b>Risk Rating</b>		
	Low	Medium	High
<b>Nature of personal information</b>	✓ Publicly available personal information not associated with any other information	✓ Personal information unique to the organization that is not medical or financial information	✓ Medical, psychological, counselling, or financial information or unique government identification number
<b>Relationships</b>	✓ Accidental disclosure to another professional who reported the breach and confirmed destruction or return of the information	✓ Accidental disclosure to a stranger who reported the breach and confirmed destruction or return of the information	✓ Disclosure to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to motivated ex-partners, family members, neighbors or co-workers ✓ Theft by stranger
<b>Cause of breach</b>	✓ Technical error that has been resolved	✓ Accidental loss or disclosure	✓ Intentional breach. ✓ Cause unknown ✓ Technical error – if not resolved
<b>Scope</b>	✓ Very few affected individuals	✓ Identified and limited group of affected individuals	✓ Large group or entire scope of group not identified





Risk Rating Overview			
Factor	Risk Rating		
	Low	Medium	High
<b>Containment efforts</b>	<ul style="list-style-type: none"> <li>✓ Data was adequately encrypted</li> <li>✓ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping</li> <li>✓ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread</li> </ul>	<ul style="list-style-type: none"> <li>✓ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping</li> <li>✓ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed</li> </ul>	<ul style="list-style-type: none"> <li>✓ Data was not encrypted</li> <li>✓ Data, files or device have not been recovered</li> <li>✓ Data at risk of further disclosure particularly through mass media or online</li> </ul>
<b>Foreseeable harm from the breach</b>	<ul style="list-style-type: none"> <li>✓ No foreseeable harm from the breach</li> </ul>	<ul style="list-style-type: none"> <li>✓ Loss of business or employment opportunities</li> <li>✓ Hurt, humiliation, damage to reputation or relationships</li> <li>✓ Social/relational harm</li> <li>✓ Loss of trust in the public body</li> <li>✓ Loss of public body assets</li> <li>✓ Loss of public body contracts or business</li> <li>✓ Financial exposure to public body including class action lawsuits</li> </ul>	<ul style="list-style-type: none"> <li>✓ Security risk (e.g. physical safety)</li> <li>✓ Identify theft or fraud risk</li> <li>✓ Hurt, humiliation, damage to reputation may also be a high risk depending on the circumstances</li> <li>✓ Risk to public health or safety</li> </ul>



### Step 3: Notification

Notification can be an important mitigation strategy that has the potential to benefit the public body, municipality, health custodian and the individuals affected by a breach. Prompt notification can help individuals mitigate the damage by taking steps to protect themselves. The challenge is to determine when notice should be required. Each incident needs to be considered on a case-by-case basis to determine whether the privacy breach notification is required. In addition, public bodies, municipalities and health custodians are encouraged to contact the Nova Scotia Freedom of Information and Protection of Privacy Review Office for assistance in managing a breach<sup>2</sup>.

Review your risk assessment to determine whether notification is appropriate. If sensitive information is at risk, if the information is likely to be misused, if there is foreseeable harm, then you will likely want to notify. The list below provides further information to assist in decision making.

**Note to health custodians:** There are additional considerations set out specifically in PHIA. In particular PHIA requires notification be given to either the affected individual or the Review Officer in accordance with sections 69 and 70 of PHIA.

Neither FOIPOP nor Part XX of the MGA requires notification. However, as noted above, notification in appropriate circumstances is best privacy practice and will help mitigate the losses suffered by individuals as a result of the breach. The steps taken in response to a breach have the potential to significantly reduce the harm caused by the breach, which will be relevant in any law suit for breach of privacy.

#### 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 – s. 69 and s. 70 of PHIA for example;
- Contractual obligations require notification;
- There is a risk of identity theft or fraud – usually because of the type of information lost, stolen, accessed or disclosed, such as a SIN, banking information, identification numbers;

---

<sup>2</sup> The Review Office has the responsibility for monitoring how privacy provisions are administered and the ability to provide advice and comments on the privacy provisions when requested by public bodies and custodians. Our contact information is included at page 22 of this document.



- 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; and
- There is a risk of loss of confidence in the public body or organization and/or good citizen relations dictates that notification is appropriate.

## **When and How to Notify**

Notification should occur as soon as possible following the breach – within days whenever possible. 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.

On very rare occasions medical evidence may indicate that notification could reasonably be expected to result in immediate and grave harm to the individual's mental or physical health. In those circumstances, consider alternative approaches, such as having the physician give the notice in person or waiting until the immediate danger has passed.

Direct notification is preferred – by phone, by letter or in person. Indirect notification – via websites, posted notices or media reports – should generally only occur in rare circumstances such as where direct notification could cause further harm 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 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;
- Where there is a risk of identity theft as a result of the breach, typically the notice should offer free credit watch protection as part of the mitigation strategy;
- Further steps planned to prevent future 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, municipality or health organization who can answer questions or provide further information;
- Review Officer contact information and the fact that individuals have a right to complain to the Review Officer under the *Privacy Review Officer Act* and PHIA. If the public body, municipality or health custodian has already contacted the Review Officer, 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, municipality or health custodian, 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 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;
- Review Office - The mandate of the Review Office includes a responsibility to monitor how the privacy provisions are administered and to provide advice and comments on the privacy provisions when requested by public bodies and health custodians.

The following factors are relevant in deciding whether or not to report a breach to the Review Office:

- For health custodians, s. 70 of PHIA sets out when the Review Office must be contacted. Health custodians may wish to contact the Review Office even when notification is not required, based on some of the factors listed below;



- The sensitivity of the information – generally the more sensitive the information at risk, the more likely the Review Office will be notified;
- 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 public body, municipality or health custodian wishes to seek advice or comment from the Review Officer to aid in managing the privacy breach;
- Your public body, municipality or health custodian requires assistance in developing a procedure for responding to the privacy breach, including notification;
- Your public body, municipality or health custodian is concerned that notification may cause further harm; and/or
- To ensure steps taken comply with the public body's obligations under privacy legislation.



## 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.

Typically prevention strategies will address privacy controls in all of the following areas:

- Physical
- Technical
- Administrative
- Personnel

So, for example, if any physical security weaknesses contributed to the breach, changes made to prevent a recurrence should be undertaken. Systems controls should also be reviewed to ensure that all necessary technical safeguards are in place. This could mean encrypting all portable storage devices or improving firewall protections on a database.

Administrative controls would include ensuring that policies are 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. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

Staff of public bodies, municipalities and health custodians should be trained to know the organization's privacy obligations under FOIPOP, MGA Part XX and/or PHIA.

In the longer term, public bodies, health custodians and municipalities should review and refresh their privacy management framework to ensure that they continue to comply with their privacy obligations. For more information on privacy management frameworks visit the Review Office website at: <http://foipop.ns.ca>.





# Privacy Breach Checklist

Nova Scotia Freedom of Information and Protection of Privacy Review Office





## Privacy Breach Checklist

Use this checklist to evaluate your response to a privacy breach and to decide whether or not to report the breach to the Nova Scotia Freedom of Information and Protection of Privacy Review Office<sup>3</sup>. For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: <http://foipop.ns.ca>.

---

Date of report: \_\_\_\_\_

Date breach initially discovered: \_\_\_\_\_

### Contact information:

Public Body/Health Custodian/Municipality: \_\_\_\_\_

Contact Person (Report Author): \_\_\_\_\_

Title: \_\_\_\_\_

Phone: \_\_\_\_\_ Fax: \_\_\_\_\_

E-Mail: \_\_\_\_\_

Mailing Address: \_\_\_\_\_

### Incident Description

Describe the nature of the breach and its cause. How was the breach discovered and when? Where did it occur?

---

---

---

---

---

<sup>3</sup> The Review Office's mandate includes an obligation to monitor how privacy provisions are administered and to provide advice and comments on privacy provisions on the request of health custodians and public bodies.





## Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary on page 17.

### (1) Containment

Check all of the factors that apply:

- The personal information has been recovered and all copies are now in our custody and control
- We have confirmation that no copies have been made
- We have confirmation that the personal information has been destroyed
- We believe (but do not have confirmation) that the personal information has been destroyed
- The personal information is encrypted
- The personal information was not encrypted
- Evidence gathered so far suggests that the incident was likely a result of a systemic problem
- Evidence gathered so far suggests that the incident was likely an isolated incident
- The personal information has not been recovered but the following containment steps have been taken (check all that apply):
  - The immediate neighbourhood around the theft has been thoroughly searched
  - Used item websites are being monitored but the item has not appeared so far
  - Pawn shops are being monitored
  - A remote wipe signal has been sent to the device but no confirmation that the signal was successful has been received
  - A remote wipe signal has been sent to the device and we have confirmation that the signal was successful
  - Our audit confirms that no one has accessed the content of the portable storage device
  - We do not have an audit that confirms that no one has accessed the content of the portable storage device
  - All passwords and system user names have been changed

Describe any other containment strategies used:

---

---

---

---



**(2) Nature of Personal Information Involved**

List all of the data elements involved (e.g. name, date of birth, SIN, address, medical diagnoses, connection with identified service provider such as welfare or counselling etc.)

- Name
- Address
- Date of birth
- Government ID number (specify) \_\_\_\_\_
- SIN
- Financial information
- Medical information
- Personal characteristics such as race, religion, sexual orientation
- Other (describe)

---

---

---

---

**(3) Relationship**

What is the relationship between the recipient of the information and the individuals affected by the breach?

- Stranger
- Friend
- Neighbour
- Ex-partner
- Co-worker
- Unknown
- Other (describe)

---

---

---

---



#### (4) Cause of the breach

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

- Accident or oversight
- Technical error
- Intentional theft or wrongdoing
- Unauthorized browsing
- Unknown
- Other (describe)

---

---

---

#### (5) Scope of the breach

How many people were affected by the breach?

- Very few (less than 10)
- Identified and limited group (>10 and <50)
- Large number of individuals affected (>50)
- Numbers are not known

#### (6) Foreseeable harm

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual; but harm may also be caused to the public body and other individuals if notifications do not occur:

- Identify theft** (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information etc.)
- Physical harm** (when the information places any individual at risk of physical harm from 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 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 a professional regulatory body or certification authority)
- Other** (specify)



**(7) Other factors**

The nature of the public body’s relationship with the affected individuals may be such that the public body wishes to notify no matter what the other factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach.

- Client/customer/patient
  - Employee
  - Student or volunteer
  - Other (describe)
- 

**Risk Evaluation Summary:**

For each of the factors reviewed above, determine the risk rating.

Risk Factor	Risk Rating		
	Low	Medium	High
1) Containment	Green	Yellow	Red
2) Nature of the personal information	Green	Yellow	Red
3) Relationship	Green	Yellow	Red
4) Cause of the breach	Green	Yellow	Red
5) Scope of the breach	Green	Yellow	Red
6) Foreseeable harm from the breach	Green	Yellow	Red
7) Other factors	Green	Yellow	Red
<b>Overall Risk Rating</b>			

Use the risk rating to help decide whether notification is necessary and to design your prevention strategies. Foreseeable harm from the breach is usually the key factor used in deciding whether or not to notify affected individuals. Step 3 below analyzes this in more detail. In general though, a medium or high risk rating will always result in notification to the affected individuals. A low risk rating may also result in notification depending on the unique circumstances of each case.



### Step 3: Notification

#### 1. Should affected individuals be notified?

Once you have completed your overall risk rating, determine whether or not notification of affected individuals is required. If any of the following factors apply, notification should occur. If the PHIA test is satisfied, notification must occur.

Consideration	Description	Factor applies
<b>Legislation</b>	Health custodians in Nova Scotia must comply with sections 69 & 70 of PHIA which require notification	
<b>Risk of identity theft</b>	Most likely when the breach includes loss of SIN, credit card number, driver's licence number, debit card information, etc.	
<b>Risk of physical harm</b>	When the information places any individual at risk of physical harm from stalking or harassment	
<b>Risk of hurt, humiliation, damage to reputation</b>	Often associated with the loss of information such as mental health records, medical records or disciplinary records	
<b>Loss of business or employment opportunities</b>	Where the breach could affect the business reputation of an individual	
<b>Explanation required</b>	The public body may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low	
<b>Reputation of public body</b>	Where the public body is concerned that the breach will undermine trust of citizens, the public body may decide to notify in order to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks assessed are low	



## 2. When and How to Notify

**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 is direct – by phone, letter, email or in person. Indirect notification via website information, posted notices or 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.

Considerations Favouring <b>Direct</b> Notification	Check If Applicable
The identities of 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 <b>Indirect</b> Notification	
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 individuals resulting from the breach	

## 3. What to Include in Breach Notification Letters

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

Essential elements in breach notification letters	Included
Date of breach	
Description of breach	
Description of personal information affected	
Steps taken so far to control or reduce harm (containment)	
Future steps planned to prevent further privacy breaches	
Steps individuals can take - Consider offering credit monitoring where appropriate	
Review Officer contact information – Individuals have a right to complain to the Review Officer	
Public body, municipality or health custodian contact information – for further assistance	



#### 4. Others to contact

Authority or Organization	Reason for Contact	Applicable
Law Enforcement	If theft or crime is suspected	
Review Officer	<ul style="list-style-type: none"> <li>• For assistance with developing a procedure for responding to the breach, including notification to ensure steps taken comply with obligations under privacy legislation</li> <li>• The personal information is sensitive</li> <li>• There is a risk of identity theft or other significant harm</li> <li>• A large number of people are affected</li> <li>• The information has not been fully recovered</li> <li>• The breach is a result of a systemic problem or a similar breach has occurred before</li> </ul>	
Professional or regulatory bodies	If professional or regulatory standards require notification of the regulatory or professional body	
Insurers	Where required in accordance with an insurance policy	
Technology suppliers.	If the breach was due to a technical failure and a recall or technical fix is required	

**Confirm notifications completed:**

Key contact	Notified
Privacy officer within your public body, municipality or health custodian	
Police (as required)	
Affected individuals	
Review Officer	
Professional or regulatory body – identify:	
Technology suppliers	
Others (list)	



## 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 future breaches.

Consider making improvements in each of the following areas listed below. Also, take the opportunity to revisit your privacy management framework,<sup>4</sup> and assess if any further adjustments are necessary as part of your prevention strategy.

### Physical Controls

What physical controls were in place at the time of the breach? Describe any modifications to physical controls such as locks, alarms, security monitoring, or visitor access control.

### Technical Controls

Was there an IT security strategy in place at the time of the breach? Describe any modification to technical controls intended to prevent future similar breaches.

### Administrative Controls

Administrative controls refer to the procedural safeguards implemented for safe handling of personal information, which includes the enforcement of an institution's policies, directives and process for the protection of personal information throughout its lifecycle. Describe the administrative controls in place at the time of the breach. Describe improvements made to administrative controls in response to the breach. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

### Personnel Security Controls

Personnel security controls refer to a public body's (or health custodian's) management of its employees – suitability, proper training, supervision and disciplinary procedures. What personnel security controls were in place at the time of the breach - for example, security clearances, confidentiality agreements and privacy training requirements? What steps have been taken to improve personnel security controls in this particular case and in general to prevent future similar breaches?

---

<sup>4</sup> For information on what constitutes a privacy management framework visit the tools tab on the Review Office website at: <http://foipop.ns.ca>.







This document was prepared by the Nova Scotia Freedom of Information and Protection of Privacy Review Office. We can be reached at:

PO Box 181 Halifax NS B3J 2M4

Centennial Building, 1660 Hollis Street, Suite 1002, Halifax

Telephone 902-424-4684

Toll-free 1-866-243-1564

TDD/TTY 1-800-855-0511

[www.foipop.ns.ca](http://www.foipop.ns.ca)

