



## KEY STEPS IN RESPONDING TO PRIVACY BREACHES

June 2008

### **Purpose**

The purpose of this document is to provide guidance to public bodies and organizations when a privacy breach occurs.<sup>1</sup> Organizations and public bodies should take preventative steps prior to a breach occurring. See the OIPC personal information security guidelines for ideas on how to help prevent security breaches:

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

### **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 *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. Examples include when a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong person.

### **Privacy Breach Checklist**

The OIPC has created a privacy breach checklist that allows public bodies and organizations to complete an analysis of the privacy breach using the four key steps described below. The privacy breach checklist is available at: [http://www.oipc.bc.ca/pdfs//Policy/Privacy\\_Breach\\_Checklist\(June2008\).pdf](http://www.oipc.bc.ca/pdfs//Policy/Privacy_Breach_Checklist(June2008).pdf).

### **Four key steps in responding to a privacy breach**

The most important step you can take is to respond immediately to the breach. You should undertake steps 1, 2 and 3 below immediately following the breach

---

<sup>1</sup> These key steps can assist both public bodies that are subject to the *Freedom of Information and Protection of Privacy Act* and organizations that are subject to the *Personal Information Protection Act*.

and do so simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies.

### **Step 1: Contain the Breach**

You should take immediate common sense steps to limit the breach. These steps would include:

- 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.<sup>2</sup> 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 Director/Manager of Information and Privacy (DMIP) or your privacy officer and/or the person responsible for security in your organization. Determine others who need to be made aware of the incident internally at this preliminary stage.
  - Determine whether a breach response team must be assembled which could include representatives from appropriate business areas and should include the Director/Manager of Information and Privacy (DMIP) or your 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.

---

<sup>2</sup> The OIPC has created a template breach management policy that public bodies and organizations may use to develop their own breach management policy at: [http://www.oipc.bc.ca/pdfs/Policy/Privacy\\_Breach\\_Management\\_Policy\\_Template\(June2008\).pdf](http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Management_Policy_Template(June2008).pdf)

## **Step 2: Evaluate the Risks Associated with the Breach**

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following factors in assessing the risks:

### **(i) 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.

### **(ii) 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?

### **(iii) 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?

**(iv) 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. The key consideration overall in deciding whether to notify should be 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 or not notification is appropriate. The OIPC has created a breach notification assessment tool to assist public bodies and organizations in determining when and how to notify individuals. The tool is available at: [http://www.oipc.bc.ca/pdfs/Policy/ipc\\_bc\\_ont\\_breach.pdf](http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf).

**(i) 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.

**(ii) When and How to Notify**

**When:** Notification of individuals affected by the breach 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.

**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.

**(iii) 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 contract 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.

#### (iv) 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.

#### (v) 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, complete the Privacy Breach Checklist located at:

[http://www.oipc.bc.ca/pdfs/Policy/Privacy\\_Breach\\_Checklist\(June2008\).pdf](http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Checklist(June2008).pdf)

#### **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*. For further ideas on how to prevent privacy breaches, see the personal information security guidelines at:

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

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.