



## KEY STEPS FOR PHYSICIANS IN RESPONDING TO PRIVACY BREACHES

June 2006

The most common privacy breach happens when personal information of your patients or employees is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal information is stolen or personal information is mistakenly emailed or faxed to the wrong person.

You must respond at once to a privacy breach. You should take Steps 1, 2 and 3 below immediately after a privacy breach in order to mitigate the effects of a privacy breach.

Rapid action after a privacy breach is part of your responsibility for protecting personal information. British Columbia law requires private and public sector organizations to take reasonable security measures to protect personal information against unauthorized disclosure or use.

This is a summary guide to responding to privacy breaches.

### Step 1 Contain the Breach

- Immediately contact your privacy officer or the person responsible for security in your organization
- Notify the police if the breach involves theft or other criminal activity
- Immediately contain the breach by seeking return of the records, shutting down the system that was breached, correcting weaknesses in physical security, etc.

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

To determine what further steps are immediately necessary, first assess the risks associated with the breach considering the following factors:

- What kinds of personal information are involved? (The more sensitive the information, the greater the risks.)
- What is the cause of the breach? Is there a risk of ongoing or further exposure? Was it stolen, lost or mistakenly disclosed (if the last, to which kind of organization?)

- Approximately how many individuals are affected by the breach? Are they inside or outside your organization?
- Is the information encrypted or otherwise not easily exploited?
- Can the information be used for fraudulent or otherwise harmful purposes?
- What kind and extent of harm to individuals might result from the breach (including risk to public health, identity theft, loss of business or employment opportunities, hurt, humiliation, damage to reputation or relationships)
- What harm might your organization suffer due to the breach (e.g., loss of trust, loss of business, loss of assets or other financial exposure)

### **Step 3 Notification**

The key consideration is whether you should notify affected individuals of the breach to avoid or mitigate harm to them. You should review the risk assessment under Step 2 to assess whether notification is required and to address the following notification considerations.

#### **Who you should notify**

There are four groups of individuals that may require notification:

- Individuals whose personal information is involved in the breach.
- Other organizations that may be affected by the breach.
- Other groups may require notice based on legal, professional or contractual obligations. In the case of self-governing professions, contact the regulatory body. The regulatory body may receive calls from the public concerning the breach.
- The Office of the Information and Privacy Commissioner for British Columbia (OIPC)<sup>1</sup>.

#### **How to notify individuals affected by the breach**

You can notify affected individuals directly or by a substitute method. Choose the method that will most effectively mitigate the harm you have identified. Also consider whether the direct approach could be too privacy-invasive in the particular case. Substitute notification can include sending a general notice to groups that include affected individuals or publication of a notice through the media.

#### **What to include in the notification**

Notifications should include the following pieces of information:

---

<sup>1</sup> 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 and whether the information was fully recovered without further disclosure.

- 
- The fact that a privacy breach occurred and a description of it
  - The elements of personal information involved
  - The steps you have taken to mitigate the harm and any likely further steps
  - Advice to affected individuals on what they can do to further mitigate the risk of harm
  - The fact that affected individuals have a right to complain to the OIPC or the BC College of Physicians and Surgeons.

#### **Step 4 Preventing Future Breaches**

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 (including through a security audit of both physical and technical security). This should drive development of adequate long-term safeguards to prevent further breaches. You should review and update your policies to reflect the lessons learned and should refresh staff training on privacy obligations under British Columbia's applicable privacy law.

\* \* \*