Responding to a Privacy Breach—Key Steps for Physicians

This section will:
• Explain what constitutes a privacy breach. • Identify whistle-blower protections in the regulations. • Identify the four steps that physicians in private practice need to take following a suspected or confirmed breach. • Explain the role of the Information and Privacy Commissioner for BC in regards to breaches.

A privacy breach occurs when there is unauthorized access to, collection, use, disclosure, retention, or destruction of personal health information. The following are some common examples of privacy breaches:

- Personal information is stolen or misplaced.
- A paper chart is lost or stolen.
- A letter is inadvertently mailed to an incorrect address or faxed to the wrong person.
- An electronic portable device (e.g., laptop, handheld electronic device, USB storage device) is lost or stolen where appropriate security controls such as passwords or encryption have not been implemented.
- Inappropriate access to personal information is stored in an electronic system.
- Personal information is not disposed of appropriately.
- A person who legitimately accesses records gains unintended access to information that he or she is not authorized to see.

Suspected or real privacy breaches can come to a practice's attention through a complaint by a patient or member of the public, through the Office of the Information and Privacy Commissioner for BC (OIPC) as a result of a formal complaint, or through compliance monitoring mechanisms such as audit trails in electronic systems alerting to unusual access.

Anyone who reports a privacy breach is protected under whistle-blower protection embedded in privacy legislation. This protects an individual from being dismissed, suspended, demoted, disciplined, harassed, or otherwise disadvantaged for having reported the breach.

Once a breach is reported, it must be responded to immediately. There are four key steps in responding:[1]

Step 1: Contain the breach

1. Contact the designated Privacy Officer.
2. Notify law enforcement if the breach involves theft or criminal activity.
3. Immediately contain the breach, which could involve suspending a user account to an electronic system, shutting down the system that was breached, and/or retrieving the documents.

Step 2: Evaluate the risks associated with the breach

Within two days of discovering a breach, to determine what further steps are necessary, consider the following factors:

1. What kinds of personal information are involved?
2. What format was the information in (paper, electronic) and how was it protected (encrypted, anonymized, password protected)?
3. Was it lost or stolen or mistakenly disclosed?
4. Can the personal information be misused?
5. What is the cause of the breach?
6. Is it an isolated event or is there a risk of ongoing or further exposure?
7. Who and how many individuals are affected by the breach?
8. Is there a relationship between the unauthorized recipients and the data subject? A close relationship between the victim and the recipient could increase the likelihood of harm.
9. Is there risk to public health and/or safety as a result of the breach?
10. Has the information been recovered?

A Privacy Breach Checklist is available from the Office of the Information and Privacy Commissioner for BC (OIPC) to support a response to a privacy breach (go to www.oipc.bc.ca).

Step 3: Implement notification procedures

Contact the OIPC prior to establishing any next steps for breaches that appear to be media-sensitive and/or carry risks of identity theft. The following factors are relevant in deciding whether to report a breach to the OIPC:

[1] Key Steps in Responding to Breaches, Office of the Information and Privacy Commissioner for BC, June 2008, www.oipc.bc.ca

1. The sensitivity of the personal information.
2. Whether the disclosed information could be used to commit identity theft.
3. Whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses.
4. The number of people affected by the breach.
5. Whether the information was fully recovered without further disclosure.

Individuals affected by a privacy breach should be notified to avoid or mitigate harm to them. The decision to notify is determined by responding to the questions in Step 2. This step, if appropriate, should take place within one week of discovering the breach. A standard Breach Notification Assessment Tool[2] is also available to assist in determining if notification is necessary.

Who should be notified:

1. Individuals (whether patients or staff) whose personal information is involved in the breach.
2. Other organizations that are or may be affected by the breach.

Other groups may also require notice based on legal, professional, or contractual obligations. In the case of self-governing professions, contact the regulatory body as it may receive calls from the public concerning the breach. It may also be prudent to notify the College of Physicians and Surgeons of BC.

What to include in the notification:

1. A description of what occurred.
2. The elements of personal information involved.
3. The steps taken to mitigate the harm.
4. Advice to affected individuals on what they can do to further protect themselves and mitigate the risk of harm.
5. A statement of their right to complain to the College of Physicians and Surgeons of BC or the Office of the Information and Privacy Commissioner for BC (OIPC) .

Step 4: Prevent future privacy breaches

Once immediate steps are taken to mitigate the risks, the practice, including the staff, should take time to investigate the cause of the breach. Long-term safeguards should be developed to prevent further

[2] Breach Notification Assessment Tool. Office of the Information and Privacy Commissioner for BC and Information and Privacy Commissioner of Ontario, December 2006, www.oipb.c.ca or www.ipc.on.ca

breaches. Privacy and security policies may need to be updated and staff should be refreshed on their privacy obligations through training and education. **This process should take place within two months of the breach.**