Protocol Objective

The objective of this Protocol is to identify, manage, and resolve privacy breaches and suspected privacy breaches which occur as the result of unauthorized use, access, copying, modification, disclosure or disposal of personal health information (PHI) or health workforce personal information.

Effective Date

The following Privacy Breach Management Protocol is in effect as of June 2008.

The Policy Custodian

This policy forms part of CIHI's privacy and security program. CIHI's Chief Privacy Officer (CPO) is the custodian of this protocol.

Definitions

"Personal Health Information" (PHI) means information that identifies an individual or could identify an individual by a reasonably foreseeable method, as defined in CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*, and as amended by CIHI from time to time.

"*Health Workforce Personal Information* " means information about a health service provider that identifies an individual or could identify an individual by a reasonably foreseeable method, as defined in CIHI's *Privacy Policy on the Collection, Use, Disclosure and Retention of Health Workforce Personal Information and De-Identified Data, 2011.*

What is a Privacy Breach?

A privacy breach occurs when personal health information or health workforce personal information in CIHI's custody or control is accessed, used, copied, modified, disclosed or disposed of in an unauthorized fashion, be it deliberately or inadvertently.

A privacy breach may be internal (within the confines of CIHI) or external (outside the confines of CIHI).

Examples of the most common external privacy breaches include but are not limited to instances where PHI is lost (a disk is misplaced), stolen (the theft of a laptop computer) or inadvertently disclosed (information meant for one person or organization is mistakenly sent to, or accessed by, another). An example of an internal privacy breach would be the inappropriate browsing by employees of data files containing PHI for non-work related purposes.

What is a Privacy Incident?

A privacy incident is defined as any occurrence that impacts or has the potential to impact or compromise personal health information or health workforce personal information held by CIHI. An example of a privacy incident would be non-compliance with CIHI's published Privacy Policy Procedures related to the methods of dissemination for personal health information.

It is important to note that a privacy incident may or may not result in a privacy breach. In the example above, although a means of transmitting personal health information may have been used that did not comply with CIHI's procedures, where it did not result in unauthorized use, access, copying, modification or disclosure of personal health information, it would not be considered a privacy breach.

All CIHI staff is responsible for immediately reporting privacy breaches or suspected privacy breaches or incidents. CIHI staff can report privacy breaches without fear of reprisal.

Protocol Procedures

Many of the following steps need to be carried out simultaneously or in quick succession.

Step 1: ***Discovery and Reporting – Implement the privacy breach protocol***

Upon learning of a privacy breach or a suspected privacy breach or incident, immediate action must be taken. Reporting may occur through different means – it may be done verbally initially but is to be followed-up by an e-mail to Incident@cihi.ca

1.1 Report all privacy breaches or suspected privacy breaches or incidents immediately to Incident@cihi.ca, with a copy to your supervisor/manager. By using this centralized mailbox, both the CPO and the Senior Program Consultant, Information Security are informed immediately, so that the required breach management steps can be put in place.

1.2 Include a description of the compromised data, when the privacy breach or suspected privacy breach or incident was discovered, how it was discovered, the location, the cause of the privacy breach or suspected privacy breach (if known), the individuals involved and any other relevant information, and any immediate steps taken to contain the breach or suspected privacy breach.

1.3 The Breach Response Team is assembled by the Chief Privacy Officer. It is comprised of the Chief Privacy Officer, the Chief Technology Officer, designated Vice-President(s), and others as required. The composition of the Breach Response Team may differ from time to time depending on the circumstances.

1.4 The Breach Response Team works in partnership and collaboration with the Director(s) of the areas affected by the breach, or suspected privacy breach, to implement the Protocol.

Step 2: ***Breach Containment and Preliminary Assessment – Identify the scope of the privacy breach, or suspected privacy breach, and take steps to contain it.***

Suspend the process or activity that caused the privacy breach or suspected privacy breach or incident. Reporting and containment should occur simultaneously where possible.

2.1 The process of containment is to be initiated upon discovery of the breach or suspected breach or incident in order to prevent further theft, loss or unauthorized access, use, disclosure, copying, modification or disposal of information. The following steps are intended to illustrate the actions that may be required to contain the breach or suspected breach (but they are not exhaustive). Individual circumstances will dictate the particular requirements.

a) Ensure that additional privacy breaches cannot occur through the same means (e.g., change passwords, identification numbers, and/or temporarily shut down a system).
b) Determine what, if any, data have been stolen, lost or accessed, used, disclosed, copied, modified or disposed in an unauthorized manner.
c) Securely retrieve the data to ensure that they are protected against theft and loss and are protected against further unauthorized access, use, disclosure, copying, modification or disposal, or have securely destroyed all or as much of the breached data as possible in order to ensure that reconstruction of the records is not reasonably foreseeable in the circumstances.
d) Ensure no copies of the data have been made or retained by the individual or organization involved in the privacy breach or suspected privacy breach.
e) Where the data have been securely destroyed rather than being returned to CIHI, obtain confirmation in writing from the individual or organization that the secure destruction has taken place, including the date, time and method of secure destruction employed.
f) Determine whether the privacy breach or suspected privacy breach would allow unauthorized access to any other data (e.g., an electronic information system involving multiple databases where other PHI could be compromised) and take whatever steps are necessary and appropriate.

Remember, containment should occur simultaneously with the reporting step, where possible.

2.2 The Breach Response Team reviews the containment measures to determine if the breach has been effectively contained and whether further action is necessary.

2.3 The Breach Response Team:

- identifies the compromised data; and
- identifies affected individuals and/or organizations and jurisdictions.

2.4 The Breach Response Team notifies the President and CEO of the breach, or suspected privacy breach, at the earliest opportunity.

2.5 The President and CEO, in consultation with the Breach Response Team, determines whether a privacy breach has occurred. For example, one factor that will be taken into consideration in the case of lost or stolen mobile computing equipment is whether the PHI was encrypted in accordance with CIHI standards. In situations involving health workforce personal information, some jurisdictions may deem health workforce information to be public. Consideration will be given, therefore, to any legislative requirements or contractual arrangements to which the information may be subject.

2.6 If the breach is found to have been intentional or the result of grossly negligent work practices, the Breach Response Team will immediately contact the Vice-President, Corporate Services to determine the appropriate action and/or consequences. The protection afforded to employees reporting privacy breaches, or suspected privacy breaches, does not extend to actions that have caused the breach itself.

2.7 If the breach involves actual or suspected theft or other criminal activity, CIHI will notify the police.

Step 3*: Notification*

Where appropriate, CIHI will notify (a) the Privacy Commissioner(s); and/or (b) the Ministry of Health or other data providers of the affected jurisdictions.

3.1 For notification to be effective, it must be given in a timely fashion to allow those affected to effectively mitigate the risks potentially flowing from the breach. Because CIHI is a secondary user of personal health information, notification should be to the original data provider where appropriate.

3.2 The Breach Response Team will discuss notification with the President and Chief Executive Officer. The notification process (i.e., when to notify, how to notify, who should notify, and what should be included in the notification) will be determined on a case-by-case basis, with consideration of guidelines or other material published by privacy commissioners or other regulators, and in keeping with any specific requirements for notification that may be found in Agreements with data providers.

3.3 These privacy breaches will be reported to the CIHI's Board of Directors.

Step 4: ***Investigation / Prevention of Future Breaches***

Once the immediate steps have been taken to mitigate the risks associated with the breach, the Breach Response Team investigates the breach and develops a privacy risk management plan.

4.1 The Breach Response Team will investigate the breach and may issue recommendations for corrective measures, as required.

4.2 The Breach Response Team's investigation report(s) will be submitted for approval to the Senior Management Committee and any other body as deemed necessary, including CIHI's Board of Directors as per section 3.3 above.

4.3 Approved recommendations are subsequently submitted and monitored by the Operations Committee to ensure they are addressed accordingly.

4.4 Where the Breach Response Team's investigation report includes recommendations, the Vice-President of the relevant program area is responsible for ensuring that a plan to implement the recommendations is drafted. The implementation plan shall include prioritized action items with responsibilities and time lines.

4.5 "Near misses" may also be investigated by the Breach Response Team and lessons-learned documented and implemented as necessary.

4.6 An audit may be carried out at any time to ensure that the recommended corrective measures have been implemented.