Canadian Institute for Health Information

Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

Unless otherwise indicated, this product uses data provided by Canada's provinces and territories.

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6

Table of contents

1.0 What is the purpose of the *Privacy and Security Incident Management Protocol*?

This protocol allows CIHI to identify, manage and resolve privacy and information security incidents and breaches.

It applies to all of CIHI's information assets — such as personal health information, health workforce personal information and employee personal information — and information systems. All workers at CIHI must follow this protocol, including all full-time and part-time employees, contract employees, contractors (including external consultants), people on secondment, temporary workers and students.

2.0 What is an incident?

2.1 An incident is any event that

- Affects or has the potential to affect the confidentiality, integrity or availability of CIHI's information assets;
- Compromises or has the potential to compromise CIHI's information security controls;
- May result in unauthorized use, access, copying, modification, disclosure or disposal of CIHI's information assets; or
- Is a suspected privacy or security breach.

You are expected to report all events that meet this definition. Not all events will ultimately become incidents; however, a collection of events might. For example, a single unsuccessful phishing event may not

- The loss of CIHI assets such as laptops, phones, security access cards or removable media (e.g., CDs, DVDs, USB keys);
- Computer application bugs that compromise the confidentiality, integrity or availability of information;
- Hacker attacks or other hostile activities;
- Known application, infrastructure or process weaknesses that could reasonably lead to compromised information security;
- Compromised physical security, such as perimeter access controls; and
- Corrupted data due to faulty processing logic or human or programmatic errors.

3.0 What is a breach?

3.1 A breach is any event that

- Results in CIHI's information assets that contain personal health information, health workforce personal information, personal information or employee personal information being accessed, used, copied, modified, disclosed or disposed of in an unauthorized or unlawful (i.e., contrary to applicable legislation such as Ontario's *Personal Health Information Protection Act* and its regulations) fashion, either deliberately or inadvertently ( ); or
- Compromises CIHI's information security controls with a resulting negative impact on the confidentiality, integrity or availability of CIHI's information assets ( ).

It is important to note that an incident may or may not result in a breach. For example, returning personal health information or de-identified data to a data provider via email **without** zipping, encrypting and password-protecting violates CIHI's *Secure Information Transfer Standard*. This is always classified as an incident, even when the information reaches the intended recipient safely.

- A USB key with unencrypted personal health information being lost or stolen;
- Personal health information meant for one person or organization being sent to or accessed by another person or organization;
- Employees inappropriately browsing data files containing personal health information for non–work related purposes; and
- Hackers engaging in malicious activity, resulting in the compromise of CIHI's

4.0 What is your responsibility under this protocol?

4.1 You must report incidents and breaches to incident@cihi.ca and copy your supervisor or manager; you do not need your supervisor's or manager's approval first. Sending an email to incident@cihi.ca informs both Privacy and Information Security personnel about the incident so that they can start managing it.

4.2 In your email, describe the incident, including

- When it was discovered;
- How it was discovered;
- Its location;
- Its cause (if known);
- The individuals involved; and
- Any other relevant information, including any immediate steps taken to contain it.

4.3 You must initiate containment measures

6.0 Incident management activities

Refer to Appendix A for the glossary of terms and definitions used in this document.

Refer to Appendix B for the Incident Management Checklist.

6.1 Containment and assessment

6.1.1 The Core IRT will be assembled when an incident is reported. CIHI's Core IRT consists of the following 2 people:

- The Chief Information Security Officer (CISO) [or delegate], who is delegated day-to-day authority to manage CIHI's Information Security Program; and
- The Chief Privacy Officer and General Counsel (CPO/GC) [or delegate], who is delegated day-to-day authority to manage CIHI's Privacy Program.

6.1.2 The Core IRT will assess the nature of the incident and determine whether it is a major or minor incident, which may include a privacy or security breach (refer to Appendix C: Incident classification — Major versus minor).

> Minor incidents can be dealt with by the Core IRT; the team may involve others at its discretion. The remaining incident management activities listed here are not mandatory for minor incidents.
>
> Major incidents require a formal incident management response, which includes all incident management activities set out in this protocol.

6.1.3 Major incidents require additional staff members to join the IRT. Who is part of the IRT beyond the core team will depend on the nature of each incident; however, at minimum, the following staff members (or their delegates) must be included:

- A management/senior management representative from all affected program areas within CIHI, even if not directly required for incident management activities;
- A management/senior management representative from all affected ITS dep84g[n⁄AL57

6.1.5 The Core IRT will send an email to everyone involved with

- A description of the incident;
- A phone number that will be used for an immediate conference call as well as for any other calls needed during the incident management activities; and
- A list of members of the IRT.

6.1.6 During the initial conference call, the IRT will determine the scope of the incident and identify

- The incident owner;
- Any other staff members who should be on the IRT;
- Containment measures that may be required, including the need to shut down systems or services;
-

6.1.13 A member of the IRT may verbally request that any staff member implement a containment measure without following current change management processes; however, in all such cases, change management process requirements should be met retrospectively as soon as possible.

6.1.14 The IRT is responsible for

- Determining the process to be followed when reviewing the containment measures implemented, and for determining whether the privacy or security breach has been effectively contained or whether further containment measures are necessary; and
- Identifying, on a case-by-case basis, the documentation that must be provided to the IRT for its review of the containment measures and the required content of the documentation.

Preserving evidence should be considered while investigating and containing incidents. In particular, if an incident may have been the result of malicious acts, or any time an incident may reasonably be expected to result in legal action, CIHI will engage the assistance of independent third-party forensic experts. In all cases, staff must take all reasonable measures to ensure evidence such as log files, cache files, bit stream backups and communications is preserved. However, if preservation measures would increase the harm or potential harm of the incident — for example, by increasing the scope or probability of a privacy or security breach — then priority should be given to containing the incident. The CPO and CISO will advise.

6.2 Communication/notification

6.2.1 Communication is a key aspect of incident management. Internal communication helps staff fully understand the situation, its impact and mitigation activities. External communication ensures stakeholders are informed of the scope and expected duration of the incident.

6.2.2 The IRT will direct internal and external communication as required, consulting with Communications and others as deemed necessary. communicate any incident details externally unless you have been directed to by the IRT.

In the event of a privacy or security breach, 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 by the President and CEO, in consultation with the IRT. This determination will be made on a case-by-case basis, considering 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 legislation or agreements with data providers.

6.2.3 In the case of personal health information from the province of Ontario, as determined by the President and CEO, CIHI must

- Notify the health information custodian or other organization that disclosed the personal health information to CIHI at the first reasonable opportunity whenever personal health information is or is believed to be stolen, lost or accessed by unauthorized persons and whenever required pursuant to the agreement with the health information custodian or other organization;
- Advise the health information custodian or other organization of the extent of the privacy or security breach, the nature of the personal health information at issue, the measures implemented to contain the privacy or security breach and further actions that will be undertaken with respect to the privacy or security breach, including investigation and remediation; and
- Notify the health information custodian or other organization, following the format of the notification and including the information that must be provided, as determined by the President and CEO in consultation with the IRT.

6.2.4 Any privacy or security breach will be reported to CIHI's Board of Directors (refer to Appendix D: Classifying privacy or security breaches). CIHI's Board of Directors must also be advised of the results of any recommendations arising from investigations of any privacy or security breaches, and the status of implementation of the recommendations.

6.3 Investigation/remediation/prevention of future incidents

6.3.1 It is important to fully understand the events that led to an incident in order to

- Avoid similar incidents in the future; and
- Continually improve our privacy and security posture by learning from incidents.

6.3.2 The IRT is responsible for determining, where possible, the root cause of the incident, as well as any remediation activities required to minimize the likelihood of a recurrence. These remediation activities may be included in formal recommendations in an incident report.

6.3.3 The IRT must produce an incident report for all major incidents, or when it deems one necessary. Incident reports must be produced in a timely manner, usually within 3 months of the incident occurring.

6.3.4 The IRT will submit incident reports containing recommendations to the Privacy, Confidentiality and Security Committee for review; reports will then be submitted to the Senior Management Committee for inclusion of any recommendations in the Master Log of Action Plans. This includes identifying who is accountable for addressing the recommendations, for establishing timelines to address the recommendations, and for monitoring and ensuring that the recommendations are implemented within the stated timelines.

6.3.5 The CISO/CPO may in their discretion request that action items for completion be completed prior to the closure of any incident. The CISO/CPO shall identify opportunities for training and/or awareness from the incident management process and act accordingly.

- Where applicable, the date that the health information custodian or other organization that disclosed the personal health information to CIHI was notified;
- The date that the investigation of the privacy breach was completed; and
- Responsibility for conducting the investigation.

6.4.2 As well, Privacy and Legal Services maintains a log of all privacy-related recommendations that includes the following elements:

- Recommendations arising from the investigation;
- Responsibility for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

6.5 Log of security breaches

6.5.1 Information Security has set up a log of information security breaches that includes the following elements:

- The date of the information security breach;
- The date that the information security breach was identified or suspected;
- The nature of the personal health information, if any, that was the subject matter of the information security breach, and the nature and extent of the information security breach;
- The date that the information security breach was contained and the nature of the containment measures;
- The date that the health information custodian or other organization that disclosed the personal health information to CIHI was notified, if applicable;
- The date that the investigation of the information security breach was completed; and
- The agent(s) (employee[s]) involved in conducting the investigation.

6.5.2 As well, Information Security maintains a log of all security-related recommendations that includes the following elements:

- The recommendations arising from the investigation;
- The agent(s) (employee[s]) responsible for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

6.6 Compliance, audit and enforcement

CIHI's Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information — including personal health information — and the workplace. The code requires all staff to comply with the code and with all of CIHI's policies, protocols and procedures. Compliance with privacy and security policies, protocols and procedures is monitored through CIHI's privacy and security audit programs. Violations of the code are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Notification of breach

Instances of non-compliance with privacy and security policies are managed through this protocol, which requires staff to immediately report incidents and breaches to incident@cihi.ca.

Appendices

Appendix A: Glossary

Availability means that the information, the information systems and the various security controls are all functioning correctly and in such a way that authorized users can access the data when and how they need to.

confidentiality

Confidential information may be accessed, used, copied or disclosed only by persons who are authorized to do so. Confidentiality is necessary but not sufficient for maintaining privacy.

- Chief Information Security Officer (CISO) [or delegate]
- Chief Privacy Officer and General Counsel (CPO/GC) [or delegate]

employee personal information

Personal information about an individual that is collected, used or disclosed for purposes of establishing, managing or terminating an employment relationship between CIHI and that individual. It includes, but is not limited to, information related to the hiring process, administration of compensation and benefit programs, performance appraisals, disciplinary proceedings and promotion planning.

health workforce personal information

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*.

The person responsible for managing all aspects of incident containment, response and reporting, including convening the Incident Response Team.

An ad hoc team that acts as a steering committee for all aspects of incident containment, response and reporting.

Appendix B: Incident Management Checklist

Appendix D: Classifying privacy or security breaches

Privacy or Security Breach Risk Assessment Tool

Purpose: