Privacy and Security Incident Management Protocol

Canadian Institute for Health Information
Institut canadien d'information sur la santé

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.

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

Phone: 613-241-7860
Fax: 613-241-8120
www.cihi.ca
copyright@cihi.ca

Cette publication est aussi disponible en français sous le titre *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information*.

Table of contents

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.

What is an incident?

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; or
- May result in unauthorized use, access, copying, modification, disclosure or disposal of CIHI's information assets.

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 constitute an incident; however, a targeted, large-scale phishing attack would.

Some examples of incidents include

- Non-compliance with CIHI's published *Privacy Policy, 2010* and the procedures related to disseminating personal health information;
- Compromised information, such as passwords, software levels, IP addresses and security infrastructure information;
- Lost or stolen laptops or removable media, such as CDs, DVDs and 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.

What is a breach?

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 fashion, either deliberately or inadvertently (**privacy breach**); or
- Compromises CIHI's information security controls (**security breach**).

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.

Some examples of breaches include

- 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 systems or network.

What is your responsibility under this protocol?

You must **immediately** 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.

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.

Containment measures, such as shutting down systems or services, may need to occur simultaneously or in quick succession with reporting. Preserving evidence needs to be considered when containment measures are being implemented (e.g., in cases where the incident may be the result of a malicious act).

You've reported the incident — What happens next?

The Incident Response Team (IRT) will be assembled and will start managing the incident. The IRT will notify you if you are required to participate.

> You are expected to cooperate immediately and fully with the IRT and to make incident management activities a high priority.

The IRT will determine what immediate activities need to occur, including any internal or external communication.

> Never share details of an incident externally, as this type of information could potentially pose a security risk or could harm CIHI's reputation.

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.

Containment and preliminary assessment

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]; and
- The Chief Privacy Officer and General Counsel (CPO GC) [or delegate].

The Core IRT will assess the nature of the incident and determine whether it is major or minor (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.

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 departments or branches; and
- A representative from the Service Desk (for incidents involving CIHI's applications or technologies).

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.

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;
- Communication requirements, both internal and external;
- Potential or actual harm done as a result of the incident;
- Any other requirements dictated by the nature of the incident; and
- A schedule for further calls or meetings as required.

At any time during the investigation, if the IRT determines that a privacy or security *breach* has occurred, in addition to containment, consideration must be given to preservation of evidence. The CISO and CPO maintain guidelines for such situations.

> The incident owner represents the IRT and has ultimate authority to speak on its behalf during investigation and containment activities. The incident owner may direct staff in containment activities and will have the sole authority to approve re-enabling any applications or services that needed to be shut down.

The IRT will perform a preliminary assessment of the incident and ensure that all necessary containment measures are taken. The goal of containment is to minimize damage or potential damage as a result of the incident.

The purpose of the preliminary assessment is to determine the immediate scope of the incident — the affected data, systems, users and stakeholders.

> If it is suspected that the incident is the result of hostile, illegal, criminal or other unlawful acts, the decision to contact authorities, and responsibility for doing so, rests with the Chief Privacy Officer and General Counsel.

Containment measures may include activities such as

- Securely retrieving or destroying affected data or copies of data;
- Shutting down applications or services;
- Removing access to applications or services for specific individuals or groups of individuals;
- Implementing a temporary or permanent work-around to contain/avoid the incident;
- Implementing temporary or permanent changes to processes; and
- Implementing a temporary freeze on application releases or production activities.

If the required containment measures risk seriously disrupting business continuity, the IRT should consider informing or involving the President and CEO, Corporate Communications or others as deemed necessary.

The IRT must notify the President and CEO at the earliest opportunity of a suspected privacy breach. The President and CEO, in consultation with the IRT, will determine whether a privacy breach has occurred, considering any legislative requirements or contractual arrangements that the information may be subject to.

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.

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, communications, etc., 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 breach — then priority should be given to containing the incident. The CPO and CISO will advise.

Communication/notification

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.

The IRT, in consultation with others as deemed necessary, will direct internal and external communication as required. **Do not** communicate any incident details externally unless you have been directed to by the IRT.

In the event of a privacy 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.

Major privacy breaches will be reported to CIHI's Board of Directors (refer to Appendix D: Classifying privacy breaches).

Investigation/remediation/prevention of future incidents

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.

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.

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.

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.

Appendix A: Glossary

availability

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.

Core Incident Response Team

- 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*.

incident owner

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

Incident Response Team (IRT)

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

information asset

Any electronic file or physical document containing information, including databases and data sets.

information security control

Any measure designed to mitigate risk in information security. Controls may be administrative (e.g., processes and procedures), logical (e.g., technical controls, such as firewalls and passwords) or physical (e.g., environmental controls, such as perimeter access and fire prevention) in nature.

integrity

Integrity means that data may not be created, altered or deleted without authorization, allowing us to trust that the data is true.

personal health information (PHI)

Health information about an individual that

- Identifies the specific individual; or
- May be used or manipulated by a reasonably foreseeable method to identify the individual, or may be linked by a reasonably foreseeable method to other information that identifies the individual.

personal information (PI)

Personal information means recorded information about an identifiable individual including, but not limited to, information related to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital status of the individual; the education or the medical, criminal or employment history of the individual; any identifying number, symbol or other particular assigned to the individual; and the address, fingerprints or blood type of the individual.

Appendix B: Incident Management Checklist

People responsible	Activity	Action taken
Core IRT	Send initial email containing • Schedule for initial conference call, including bridge telephone number and access code that will be used for all meetings • Details of incident • Composition of IRT	n/a
Core IRT	Identify and assemble IRT	n/a
Core IRT	Categorize incident	Major versus minor
Core IRT	Enter incident ticket in Service Desk	n/a
IRT	Assign incident owner	n/a
IRT	Identify containment measures	n/a
IRT	Identify internal communication requirements	n/a
IRT	Identify external communication requirements	n/a
IRT	Schedule follow-up calls as needed	n/a
CPO GC	Contact authorities regarding illegal, criminal or other unlawful activity	n/a
IRT	Notify the President and CEO (required for suspected privacy breaches or at the discretion of the IRT)	n/a
IRT	Complete incident/breach report	n/a

Notes
IRT: Incident Response Team.
CPO GC: Chief Privacy Officer and General Counsel.
n/a: Not applicable.

Appendix C: Incident classification — Major versus minor

Classifying an incident is a subjective activity. The IRT will consider factors such as

- Actual or potential harm;
- Incident scope and duration;
- Nature of required containment measures, if any;
- Root cause; and
- Sensitivity of information involved.

Examples of incident classification

Incident	Classification	Rationale
Single instance of disclosing de-identified information inappropriately due to human error	Minor	• Not personal health information • No harm to individuals or CIHI clients • Not recurring • Not an application error
Malware infection on a single computer that was successfully contained	Minor	• Not widespread • No harm to CIHI's systems or information
Disseminating information by other than approved methods	Minor	• Information was successfully disseminated to the correct individual • No harm to individuals or CIHI clients • Not recurring • Not an application error
Any privacy breach or security breach	Major	• By definition, all privacy and security breaches are considered major incidents
An application error resulting in disclosure of electronic reports to the wrong facility	Major	• Potential harm to individuals or CIHI clients • Potentially widespread • Containment generally requires shutting down systems

Appendix D: Classifying privacy breaches

Privacy Breach Risk Assessment Tool

Purpose: To enable CIHI to assess the impact of a privacy breach and the likelihood that harm will stem from it.

Step 1

Impact of breach		Negligible	Low	Medium	Very high	Extreme
A	Magnitude of breach (number of individuals, number of jurisdictions, within or outside Canada)					
B	Nature and sensitivity of information involved (clinical data)					
C	Number of different data elements involved (approximate total)					
D	Other considerations/factors					

Overall impact of breach Low/Medium/High	L	M	H

Step 2

Likelihood of harm		Rare	Unlikely	Moderate	Likely	Almost certain
E	Known recipient: **public at large**; **known individual**; **known community of individuals (confidentiality agreement)**; or **known community of individuals (subject to legislation)**					
F	Cause of breach: **accidental** (human error); **systemic**; or **intentional** (malicious intent, risk of identity theft)					

Likelihood of harm		Rare	Unlikely	Moderate	Likely	Almost certain
G	Foreseeable harm (probability that the information was or could be misused for fraudulent or other harmful purposes: physical, financial, security, reputation and/or other harm to the individual)					
H	Other considerations/factors					

Overall likelihood of harm Low/Medium/High	L	M	H

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

14949-0417