cpsa

COLLEGE OF PHYSICIANS
& SURGEONS OF ALBERTA

Privacy Breach Response

Contents

Section 17, "Incident Response", of CPSA's *Privacy and Confidential Information Policy* includes CPSA's responsibility and basic steps to respond to any incident, real or potential, involving confidential information under its control which could significantly impact CPSA operations.

However, it is not always easy to identify when a breach occurs, or determine if it is serious enough to report. This document outlines CPSA's privacy breach response plan, including required steps and staff responsibilities.

PRIVACY BREACH RESPONSE AT-A-GLANCE

IDENTIFY BREACH

A privacy breach is any incident involving unauthorized access to, or disclosure of, personal or confidential information in the custody or control of CPSA, including information managed by individuals or organizations CPSA contracts. Most commonly, breaches occur when the personal/confidential information of physicians, Albertans, patients, clients, or employees is stolen, lost, mistakenly disclosed, or accessed by unauthorized persons.

The Office of the Privacy Commissioner of Alberta (OIPC) lists the following causes of breaches[1]:

1) Human Error
    a. Email, mail, and faxes sent to the wrong individual(s)
    b. Email address viewable in the "CC" line to all individuals in a mass email, emailing too much or unauthorized information
    c. Faxes sent to an unsecure fax
    d. Mail or couriers sent to the wrong person
    e. Documents lost on public transport or gone missing
    f. Documents disposed of in the trash, or intended for shredding and disposed of improperly
    g. Computer hard drive given to the wrong person
    h. Verbal disclosure

2) Theft
    a. Information taken by a former team member
    b. Office and car break-ins resulting in the loss of files and computer devices, including laptops and hard drives

3) System Compromise
    a. Targeted network attacks by external hackers seeking to extract large amounts of data or ethical-hackers hacking a system
    b. Information viewable on the Internet due to a system upgrade
    c. System glitch misdirected faxes

4) Inadequate Access Control
    a. Improper access controls to electronic and paper files resulting in the files being accessible to those not authorized to have access

The following Directives provide more information on how you can prevent these breaches from occurring: *Protecting Confidential Information*, *Protecting*

[1] OIPC, 2012; *Cause of Breaches and Breach Prevention Recommendations*.

Information when Contracting for Services, and *Acceptable Uses of Networks and Electronic Devices*.

RESPOND AND CONTAIN

If you suspect a privacy breach, the first steps are to determine whether an actual breach has occurred and contain the situation as soon as possible to minimize harm to the affected individual(s) or CPSA.

Report:

1) If you suspect a breach has occurred but you are not sure, report your concerns as soon as possible to your Leadership Team member. If they are unavailable, report to the Privacy Team (i.e., Privacy Coordinator and Privacy Officer). Do not disclose the breach occurred to any other individual until it is reported to the Leadership Team member and the Privacy Team.

2) It is far better to report a possible breach and discover there was no concern, than to ignore a situation which later surfaces via a third party (e.g., evening news).

3) Once you report the situation to your Director, he/she will work with the Privacy Team (and possibly the Director of IT) to assess and manage the situation. The Privacy Team may notify the Communications Director in serious cases, or where media may become involved.

Assess:

Assess the situation by asking these questions:

1) Is personal or confidential information involved?
    a. Personal information is information about an identifiable individual
    b. Confidential information is:
        i. personal information
        ii. health information
        iii. protected team member information
        iv. business information deemed to be confidential

2) Has unauthorized disclosure occurred?
    a. Whether it is the result of human error, malicious intent, or criminal activity, an unauthorized disclosure is a privacy breach.

If you answer "yes" to both questions, then a privacy breach has occurred; continue with containment of the situation. If you answer "no" to either question, a breach has not occurred and the response process can end here.

Contain:

Take corrective action immediately to contain the breach, such as:

1) Isolating or suspending the activity, process, or system if it was an electronic breach or data security incident
2) Retrieving the released personal/confidential information
3) Requesting the unauthorized party to securely destroy the disclosed information, and receive written confirmation this has occurred
4) Ensuring corrected documents are re-issued as need, etc.

The main goal is to minimize any consequences/harm to the affected individual(s) and CPSA.

Document:

Documenting the details of a privacy breach, including the containment strategy, allows the Privacy Team to determine reporting requirements, respond to an OIPC investigation, evaluate the breach response to identify opportunities for improvement, and help implement remedial measures.

If you find yourself in a breach situation, document details using the Privacy Breach Response Form (located on the Privacy Matters page on CORE). Details collected include:

1) The individual(s) affected by the breach:
    a. person(s) whose information was disclosed
    b. person(s) who received the information in error
2) Description of the personal information released
3) What happened, when and how the breach was discovered, including spread of information beyond the person who received it in error
4) What action was taken to contain the breach
5) What corrective action will be taken to help prevent the breach from reoccurring
6) Details of communication with the individual(s) affected by the breach:
    a. the information provided by them
    b. instructions provided to them
    c. their contact information, so we can follow up

If you are the Leadership Team member, ensure details of the breach and corrective action are appropriately documented. Forward a report to the Privacy Team as soon as possible to facilitate next steps.

INVESTIGATE

Once you've contained and documented the breach, the Privacy Team will review the Privacy Breach Response Form, or may meet with you, to:

1) Identify and analyze the events that led to the privacy breach
2) Evaluate how the breach was contained
3) Conduct a Risk of Harm Assessment to determine whether individuals, third parties, or the OIPC need to be advised of the privacy breach
4) Recommend remedial action to help prevent future breaches

The Risk of Harm Assessment analyzes the following:

1) The amount and sensitivity of personal/confidential information
2) The Risk of Harm (low, medium, high) is calculated via an assessment of the:
    a. Likelihood of risk: how real is the risk and what is the probability this could happen again?
    b. Severity of impact: what is the magnitude of the risk—how will it impact individuals, CPSA, and/or Albertans?

The Privacy Officer will handle the documentation at this point, but any assistance you can give during the investigation is helpful to fulfill CPSA's requirements under the *Personal Information Protection Act* (PIPA). The Privacy Officer will include the following information when notifying the OIPC:

1) The nature and scope of the privacy breach
2) What steps have been taken, or will be taken, to manage the breach
3) What steps have been taken, or will be taken, to help prevent the breach from reoccurring
4) Notification of the individual(s) affected by the privacy breach
5) Notification of third parties (e.g. law enforcement, media, etc.)
6) Analysis of the risk of harm to the individual(s) affected

NOTIFICATIONS

Once the Privacy Team has completed the Risk of Harm Assessment, they will work with you and/or your Leadership Team member to notify the individual(s) whose personal information was affected. Occasionally, it may be inappropriate or impossible to notify the individual; for example, if the identity of the individuals

affected are unknown, contact information is unavailable, or if notice would interfere with a law enforcement investigation.

1) The purpose of notifying the individual is to provide them with sufficient information about:
    a. what happened, and when
    b. the types of personal information involved in the breach, including whether any unique identifiers or sensitive personal information were involved
    c. the nature of potential or actual risks of harm
    d. what action we have taken to address the situation
    e. what appropriate action the individual(s) may take to protect themselves against harm

2) Notify the individual(s) as soon as is reasonably possible

3) Consider the following during the notification process:
    a. ensure the facts of the situation are confirmed and documented to avoid providing false information
    b. ensure you are notifying the correct individual(s)
    c. prepare a "script" before contacting the individual via telephone to ensure accuracy
    d. use registered mail when sending mail notification to document a signature and proof of receipt

4) Forward notification details to the Privacy Team, as well as copies of the notification letter(s)

If there is high risk of harm, the Privacy Officer will notify the OIPC, who may initiate an external investigation. Legal counsel, Communications, and the Chief Information Officer may become involved, depending on the seriousness of the situation.

IMPLEMENT CHANGE

The breach reporting process is an opportunity for CPSA to learn from our mistakes, understand what went wrong, and avoid future breaches. Determining what improvements and remedial actions are necessary may require CPSA to:

1) Review relevant information management systems to enhance compliance with PIPA
2) Amend or reinforce existing policies and practices for safeguarding personal information
3) Develop and implement new security or privacy measures

4) Modify staff training about legislative requirements, policies, practices, and procedures
5) Test and evaluate remedial actions to determine if they have been implemented correctly