Key Steps in Responding to Privacy Breaches

The purpose of this document is to provide guidance to private sector organizations, health custodians and public sector bodies on how to manage a privacy breach.

For more information on how to help prevent privacy breaches, see *Securing Personal Information: A Self-Assessment Tool for Organizations* available at **www.oipc.ab.ca**.

What is a Privacy Breach?

A privacy breach is a loss, or unauthorized access to or disclosure of personal or individually identifying health information (see *Personal Information Protection Act*, section 34.1; *Health Information Act*, section 60.1).

The most common privacy breaches happen when personal information of customers, patients, clients or employees is stolen, lost, improperly accessed or mistakenly disclosed. Examples include when a computer containing personal or individually identifying health information is stolen, computers, servers or websites are hacked, or when information is mistakenly emailed to the wrong person.

Four Key Steps in Responding to Privacy Breaches

1. Contain the Breach
2. Evaluate the Risks Associated with the Breach
3. Breach Notification and Reporting
4. Prevention

The most important step you can take is to respond immediately to the breach. You should undertake steps one, two and three immediately following the breach and do so simultaneously or in quick succession. Step Four provides information for longer-term prevention strategies.

Office of the Information and Privacy Commissioner of Alberta

Issued December 2006; last updated August 2018

Step One: Contain the Breach

Take immediate steps to limit the breach, including:

- Containing the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached or correcting weaknesses in physical security
- Contacting your Privacy Officer, FOIP Coordinator, Responsible Affiliate or Custodian, and/or the person responsible for privacy and security in your organization
- Notifying the police if the breach involves theft or other criminal activity

Step Two: Evaluate the Risks Associated with the Breach

To determine what other steps are necessary, you should assess the risks associated with the breach by considering the following:

- **Personal or health information involved**
    - What data elements have been breached?
    - What possible use is there for the personal or individually identifying health information? Can the information be used for fraudulent or otherwise harmful purposes?
- **Cause and extent of the breach**
    - What is the cause of the breach?
    - Is there a risk of ongoing or further exposure of the information?
    - What was the extent of the loss or unauthorized access to or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
    - Is the information encrypted or otherwise not readily accessible?
    - What steps have you already taken to minimize the harm?
- **Individuals affected by the breach**
    - How many individuals are affected by the breach?
    - Who was affected by the breach (e.g. employees, customers, patients, clients, contractors, service providers or other organizations)?
- **Possible harm from the breach**
    - Is there any relationship between the unauthorized recipients and the data subject?
    - What harm to the individuals will result from the breach? Some examples of harm that could flow from a breach of personal or individually identifying health information are:
        - A breach of an individual's name and credit card number could result in identity theft and financial fraud.
        - A breach of an individual's name, driver's licence and social insurance number (SIN) could result in identity theft and fraud.

- A breach of an individual's diagnostic, treatment and care information could result in hurt or humiliation.
- A breach of name and subscription to an adult magazine or website could result in reputational harm.
- A breach of an individual's disciplinary letter could result in humiliation.

Step Three: Breach Notification and Reporting

Notification of the affected individuals can be an important mitigation strategy in the right circumstances. The key consideration in deciding whether to notify should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal or individually identifying health information has been lost or accessed or disclosed without authorization. Legislation may require notification based on an assessment of risk of harm to individuals as a result of the breach.[1,2] Review your risk assessment to determine whether notification is required.

Organizations, custodians or public bodies that collect and hold personal or individually identifying health information are responsible for notifying affected individuals when a privacy breach occurs. If the breach occurs at a third party entity that has been contracted to maintain or process personal or health information, the breach should be reported to the originating entity, which has primary responsibility for notification.[3] Organizations subject to PIPA are not precluded from notifying affected individuals on their own accord prior to reporting a breach to the Commissioner (section 37.1(7)).

- **Notifying affected individuals**

  As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

  - **Legislation requires notification:** Is your organization, custodian or public body covered by legislation that requires notification of the affected individual? If you are uncertain, contact the OIPC. Does the legislation permit you to not notify an affected individual because of risk of harm to the individual that notice of the breach might present?[4]

  - **Contractual obligations require notification:** Does your organization, custodian or public body have a contractual obligation to notify affected individuals in the case of a privacy breach?

  - **Risk of identity theft or fraud:** How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with SINs, credit card numbers,

[1] Organizations subject to PIPA are required to report a privacy breach to the Commissioner when a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure (section 34.1) The Commissioner can require organizations to notify affected individuals (PIPA, section 37.1).

[2] Custodians subject to HIA are required to notify affected individuals, the Commissioner and the Minister of Health if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure (sections 60.1(2),(3)).

[3] Under HIA, an affiliate of a custodian must as soon as practicable notify the custodian of any privacy breach of individually identifying health information in the custody or control of the custodian (section 60.1(1)).

[4] A custodian may decide not to notify one or more affected individuals if notification could reasonably be expected to result in a risk of harm the individual's mental or physical health. In such cases, the custodian must immediately notify the Commissioner of the decision not to notify the individual (HIA, section 60.1(5)).

driver's licence numbers, personal health numbers, debit card numbers with password information or any other information that can be used for fraud by third parties (e.g. financial).

- **Risk of physical or mental harm:** Does the loss of information place any individual at risk of physical harm, stalking or harassment, or mental harm?
- **Risk of embarrassment, hurt, humiliation or damage to reputation:** This type of harm can occur with the loss of information such as mental health records, medical records or disciplinary records.
- **Risk of loss of business or employment opportunities:** Could the loss of information result in damage to the reputation of an individual, affecting business or employment opportunities?

- **When and how to notify affected individuals**
  - **When:** Notification of individuals affected by the breach should occur as soon as possible following the breach. Also, legislation may dictate when notification should occur. For example, HIA requires custodians to notify affected individuals "as soon as practicable."

    If you have contacted law enforcement authorities, and those authorities have indicated notification would impede a criminal investigation, please ensure the authorities advise in writing that they have asked for a delay in notification for this reason.
  - **How:** Legislation may establish the requirements for the method of notification.

    PIPA requires organizations to directly notify affected individuals unless the Commissioner determines that direct notification would be unreasonable in the circumstances.

    HIA requires custodians to notify affected individuals in writing by one of the methods specified in section 103 of the Act.
  - Generally, the preferred method of notification is direct to affected individuals.

    Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, contact information is lacking or where a very large number of individuals are affected by the breach such that direct notification could be impractical. Using multiple methods of notification in certain cases may be the most effective approach.

- **What should be included in the notification to affected individuals**

  Note that organizations subject to the PIPA breach notification requirements must include, under section 34.1, the information contained in section 19.1 of the *Personal Information Protection Act Regulation*. This could be important if a breach reported to the Commissioner results in the Commissioner requiring notification. This is because the Commissioner will require the information in section 19.1 of the Regulation to be included in the notification to individuals. If a notification to individuals prior to reporting a breach does not contain the information required by section 19.1 of the Regulation, the Commissioner will (and has) required re-notification.
  Also, the breach notice to be given by custodians to individuals under section 60.1(2) of HIA must include the information set out in section 8.2(4) of the *Health Information Regulation*.

Generally, notifications should include the following information:

- Date of the breach
- Description of the breach (a general description of what happened)
- Description of the information lost or accessed or disclosed without authorization (e.g. name, credit card numbers, SINs, medical records, financial information, etc.)
- The steps taken so far to mitigate the harm
- Steps the individual can take to further mitigate the risk of harm – provide information about how individuals can protect themselves (e.g. how to contact credit reporting agencies to set up a credit watch; information explaining how to change a personal health number or driver's licence number)
- Next steps planned and any long term plans to prevent future breaches
- Contact information of an individual within the organization, custodian or public body who can answer questions or provide further information
- That individuals have a right to complain to the Office of the Information and Privacy Commissioner (i.e. provide contact information).

- **Reporting to the Commissioner**

Reporting a breach to the Commissioner is mandatory in certain circumstances under PIPA and HIA. Reporting a privacy breach is voluntary but recommended for public bodies subject to the FOIP Act.

PIPA organizations having personal information under their control are required to notify the Commissioner of incidents "involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure" (section 34.1).

HIA custodians are required to notify the Commissioner of "any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure" (section 60.1(2)).

For public bodies (and other entities not required by law to report a breach), the following factors are relevant in deciding when to report a breach to the Commissioner:

- The type of information that is involved in the breach
- Whether the disclosed information could be used to commit identity theft, fraud, embarrassment, hurt or humiliation, damage to reputation or relationships, mental or physical harm, or financial harm
- Whether there is a reasonable chance of harm from the breach
- The number of people affected by the breach
- Whether vulnerable individuals, such as seniors or youth, were affected by the breach
- How long the information was exposed and to whom
- Whether there is evidence of malicious intent or purpose, such as theft, hacking or malware
- Whether the information was fully recovered without further disclosure

The OIPC has resources available to assist in reporting a privacy breach, including a Privacy Breach Report Form. The Privacy Breach Report Form is designed to assist organizations, custodians and public bodies report a breach to the Commissioner.

The OIPC has also developed a practice note, Reporting a Breach to the Commissioner, which is designed to assist organizations and custodians in meeting the requirements under section 19 of the *Personal Information Protection Act Regulation* and section 8.2(2) of the *Health Information Regulation* when reporting a breach to the Commissioner.

Public bodies are encouraged to use the above resources when reporting a breach to the Commissioner. The OIPC may be able to provide general advice or guidance for responding to the privacy breach and ensuring steps taken comply with obligations under privacy legislation.

The Privacy Breach Report Form and the Reporting a Breach to the Commissioner practice note are available at **www.oipc.ab.ca**.

- **Others to contact**

  Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed:

  - Police if theft or other crime is suspected
  - Insurers or others if required by contractual obligations
  - Professional or other regulatory bodies

Step Four: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security.

As a result of this evaluation, you should develop or improve as necessary adequate long term safeguards against further breaches. Policies should be reviewed and updated to reflect the lessons learned from the investigation and regularly after that. Your resulting plan should also include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented. Staff should be trained to know about their responsibilities under privacy legislation.

Additional Resources

Additional resources are available at **www.oipc.ab.ca**.

You may also contact the OIPC for general information about responding to a privacy breach, by calling (780) 422-6860 or toll free at 1-888-878-4044. Information provided does not constitute legal advice, is not binding on the Commissioner, and does not mean an organization or custodian has fulfilled its legal obligation to report a privacy breach to the Commissioner.