PRIVACY BREACH PROCEDURES

Privacy Officer: Eric McKay

Date: March 8, 2024

What is a privacy breach?

A privacy breach occurs when there is unauthorized access to or collection, use, or disclosure of personal information (PI). Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation, such as Personal Information Protection and Electronic Documents Act (PIPEDA), or similar provincial privacy legislation. Some of the most common privacy breaches happen when personal information of customers, patients, clients, or employees is stolen, lost, used inappropriately or mistakenly disclosed (e.g., a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong people). A privacy breach may also be a consequence of faulty a business procedure or operational breakdown.

Four Key Steps in Responding to a Privacy Breach

There are four key steps to consider when responding to a breach or a suspected breach: (1) breach containment and preliminary assessment; (2) evaluation of the risks associated with the breach; (3) notification; and (4) prevention. The first three steps must be undertaken as soon as possible following the breach. The fourth step provides recommendations for longer-term solutions and prevention strategies.

Step 1: Breach Containment and Preliminary Assessment

If you discover a privacy breach has occurred or is occurring, notify your organization's Privacy Officer or the individual with that responsibility immediately. The Privacy Officer may take prompt action to contain or limit the breach. Actions that may be required when a breach becomes apparent include:

- Immediately contain the breach (e.g., stop the unauthorized practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security).
- Designate an appropriate individual to lead the initial investigation. This individual should have an appropriate scope within the organization to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.
- Determine the need to assemble a team which could include representatives from appropriate parts of the business, or third parties as required.
- Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage. Escalate internally as appropriate, including informing the person within your organization responsible for privacy compliance.
- If the breach appears to involve theft or other criminal activity, notify the police.
- Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.

Step 2: Evaluation of the Risks Associates with the Breach

To determine what other steps are immediately necessary, the Privacy Officer will assess the risks associated with the breach. The following factors in assessing the level of risk associated with the breach include:

1. Personal Information Involved
    - What data elements have been breached?
    - How sensitive is the information? Generally, the more sensitive the information, the higher the risk of harm to individuals. Some personal information is more sensitive than others (e.g., health information, government-issued pieces of identification such as social insurance numbers, driver's licence and health care numbers, and financial account numbers such as credit or debit card numbers that could be used in combination for identity theft). A combination of personal information is typically more sensitive than a single piece of personal information. However, sensitivity alone is not the only criteria in assessing the risk, as foreseeable harm to the individual is also important. What is the context of the personal information involved? For example, a list of customers on a newspaper carrier's route may not be sensitive. However, the same information about customers who have requested service interruption while on vacation may be more sensitive. Similarly, publicly available information such as that found in a public telephone directory may be less sensitive. Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?
    - How can personal information be used? Can the information be used for fraudulent or otherwise harmful purposes? The combination of certain types of sensitive personal information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.

An assessment of the type of personal information involved will help you determine how to respond to the breach, who should be informed, including the appropriate privacy regulator(s), and what form of notification to the individuals affected, if any, is appropriate.

1 Cause and Extent of the breach
    - To the extent possible, determine the cause of the breach.
    - Is there a risk of ongoing breaches or further exposure of the information?
    - What was the extent of the unauthorized access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?
    - Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
    - Has the personal information been recovered?

- What steps have already been taken to mitigate the harm?
- Is this a systemic problem or an isolated incident?

2 Individuals Affected by the Breach

- How many individuals' personal information is affected by the breach?
- Who is affected by the breach: employees, contractors, public, clients, service providers, other organizations?

3 What harm to the individuals will result from the breach?

- In assessing the possibility of foreseeable harm from the breach, have you considered the reasonable expectations of the individuals? For example, many people would consider a list of magazine subscribers to a niche publication to be potentially more harmful than a list of subscribers to a national newspaper.
- Who is the recipient of the information? Is there any relationship between the unauthorized recipients and the data subject? For example, was the disclosure to an unknown party or to a party suspected of being involved in a criminal activity where there is a potential risk of misuse? Or was the recipient a trusted, known entity or person that would reasonably be expected to return the information without disclosing or using it?
- What harm to the individuals could result from the breach? Examples include:
- security risk (e.g., physical safety);
- identity theft;
- financial loss;
- loss of business or employment opportunities; or
- humiliation, damage to reputation or relationships.

4 What harm to the organization could result from the breach? Examples include:

- loss of trust in the organization;
- loss of assets;
- financial exposure; or
- legal proceedings (i.e., class action suits).

5 What harm could come to the public as a result of the notification of the breach? The harm that could result from includes:

- the risk to public health; or
- the risk to public safety.

Step 3: Notification

Under Canadian privacy law, should a privacy breach cause a real risk of significant harm (or risk of serious injury if Quebec residents), individuals affected must be notified. The real risk of significant harm or risk of serious injury must be determined based on an assessment of the sensitivity of the personal information involved in the breach and the probability the personal information has been/is/will be misused. Significant harm or serious injury includes identity theft, financial loss, negative effects to credit score or credit record, loss of employment, loss of business or professional opportunities, damage to reputation or relationships, humiliation, loss or damage to property, and bodily harm. Once the situation has been evaluated for risk, the Privacy Officer will work to determine which type of notification may be necessary.

When to Notify, How to Notify, and Who Should Notify

At this stage, the Privacy Officer should have as complete a set of facts as possible in order to determine whether to notify individuals and the applicable privacy regulator.

When to notify: Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.

How to notify: The preferred method of notification is direct – by phone, letter, email or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm or the contact information for affected individuals is not known. Using multiple methods of notification in certain cases may be appropriate. You should also consider whether the method of notification might increase the risk of harm (e.g., by alerting the person who stole the laptop of the value of the information on the computer).

Who should notify: Typically, the organization that has a direct relationship with the customer, client or employee should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information. However, there may be circumstances where notification by a third party is more appropriate. For example, in the event of a breach by a retail merchant of credit card information, the credit card issuer may be involved in providing the notice since the merchant may not have the necessary contact information.

Content of Notification

The content of notification will vary depending on the breach and the methods of notification chosen. The notification must contain enough information to allow the individual to understand the significance of the breach to them and to take steps to mitigate that harm. The notification should include the following information:

- date(s) of breach or time period over which it occurred;
- description of the breach;
- description of the personal information that is subject of the breach;

- description of the steps taken to reduce the risk of harm that could result from this breach;
- description of the steps affected individuals can take to avoid or reduce the risk of harm that could result from the breach or to mitigate the harm;
- contact information within the Agency that the affected individual can contact who will answer questions or provide further information;
- That individuals have a right to complain to the Office of the Information and Privacy Commissioner or the applicable provincial privacy regulatory authority; and contact information for the privacy regulator.

Notifying Third Parties

Depending on the breach, a notification may also need to be made to persons other than the individuals whose personal information may have been compromised. It may be necessary to contact the police, insurers, technology suppliers, professionals or regulatory bodies, credit card companies, financial institutions, credit reporting agencies or the applicable privacy regulatory authority, depending on the situation. It may also be prudent to contact other organizations or government institutions to help mitigate the harm caused by the breach.

The Privacy Officer **MUST** inform the applicable privacy regulatory authority if the breach poses a real risk of significant harm or risk of serious injury.

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach and consider whether to develop a prevention plan.

The level of effort should reflect the significance of the breach and whether it was a systematic breach or an isolated instance. This plan may include the following:

- a security audit of both physical and technical security;
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (e.g., security policies, record retention, and collection policies, etc.);
- a review of employee training practices; and
- a review of service delivery partners (e.g., dealers, retailers, etc.).

The resulting plan may include a requirement for an audit at the end of the process to ensure that the prevention has been fully implemented.

Record Keeping

Records must be kept of ALL breaches, even if it has been determined there is no real risk of significant harm and will be kept for a minimum of two years (5 years for incidents occurring in Quebec) for review by the applicable privacy regulatory authority if requested.

Records should include, at a minimum:

- Date(s) or estimated date(s) of breach
- Description of the circumstances of the breach
- Nature of the information involved in the breach
- Whether or not the breach was reported to the privacy commissioner or other that were notified
- If not reported to the privacy commissioner, a brief explanation as to why it was determined that there was no real risk of significant harm.
- The Quebec Commission d'accès à l'information requires that the information be retained in a registry.

Information Resources:

Detailed information on all your privacy obligations can be found at the www.priv.gc.ca.

You should also familiarize yourself with the provincial privacy commissioner website if you are licensed in a province where a provincial privacy commissioner is present.