Privacy Officer: Keaun Amani
Date: 2024-02-07

Privacy Breach Protocol

Neurosnap Inc.

What is a privacy breach?

A privacy breach occurs when there is unauthorized access to or collection, use, or disclosure of personal information (PI). 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 a faulty business procedure or operational breakdown.

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 are to 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

Upon discovery of a privacy breach, whether occurred or occurring, the organization will notify their Privacy Officer as well as relevant personnel immediately. Preliminary analyses of the breach as well as exposure of the breach will be conducted as well as efforts to ensure the containment of such a breach. 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 will 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 the organization responsible for privacy compliance.
- If the breach appears to involve theft or other criminal activity, notify the police.

Step 2: Evaluation of the Risks Associated 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?
- 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 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.

2. Cause and Extent of the breach

- To the extent possible, the organization will determine the cause of the breach.
- The risk of ongoing breaches or further exposure of the information will be determined.
- 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 will be determined.
- If the information was stolen, can it be determined whether the information was the target of the theft or not?
- Determine whether the personal information has been recovered.
- Determine if this is a systemic problem or an isolated incident.

3. Individuals Affected by the Breach

- Determine how many individuals' personal information is affected by the breach.
- Determine who is affected by the breach: employees, contractors, public, clients, service providers, other organizations.

4. What harm to the individuals will result from the breach?

- In assessing the possibility of foreseeable harm from the breach, the organization will consider the reasonable expectations of the individuals.
- Determine who is the recipient of the information as well as if there are any relationships 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?
- Determine 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.
- Determine 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).
- Determine 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.

Privacy Officer: Keaun Amani
Date: 2024-02-07

Step 3: Notification

Upon the discovery of a privacy breach, the organization will aim to notify all affected users within 72 hours of discovery or as soon as reasonably possible. However, if law enforcement authorities are involved, notification could be delayed to ensure that any investigation is not compromised. Once the situation has been evaluated for risk, the Privacy Officer will work to determine which type of notification may be necessary.

Content of Notification

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

- 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;

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.

Privacy Officer: Keaun Amani
Date: 2024-02-07

Record Keeping

Records will 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.

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 a government body or if similar entities that were notified
- If not reported, a brief explanation as to why it was determined that there was no real risk of significant harm.

Updates to Privacy Breach Protocol

The Privacy Breach Protocol, as detailed in this document, is subject to change and improvement in response to emerging threats and advancements in data protection technologies. It is our commitment to continuously refine and adjust our strategies to ensure the highest levels of security and mitigation are maintained. These modifications are also aimed at enhancing our engagement and transparency with customers, ensuring they are fully informed about how their data is protected and how we respond to potential breaches.