Privacy Breach Policy

guard.me International Insurance

January 05, 2024

Table of Contents

Privacy Breach Policy

To provide direction and guidance on responding to breaches of personally identifiable information, personal health information or information labelled Confidential or Restricted of guard.me International Insurance's clients, insureds or employees

Information Classification: Public

1.0 Purpose

The purpose of this policy is to provide direction in the event of a breach of the privacy of the personally identifiable information, personal health information, or any other information labelled as Confidential or Restricted of {{organization.name}}'s clients, insureds or employees.

This policy provides guidance on the steps necessary to limit the breach, conduct an effective investigation and assist with remediation.

2.0 Scope

The policy applies to all guard.me International Insurance employees, contractors, consultants, co-op placement students, volunteers and anyone working at or acting on behalf of guard.me International Insurance, and who are privy to such information.

3.0 Definitions

Term	Definition
Confidentiality	Confidentiality arises in the course of a relationship in which personally identifiable information, personal health information, or any other information labelled as Confidential or Restricted is shared. As the sharing of such information is essential for the provision of guard.me International Insurance services, including accurate assessment, diagnosis, and/or treatment of insureds, this ethical duty of confidentiality is imposed upon guard.me International Insurance, employees and all those acting on behalf of guard.me International Insurance to ensure that information obtained in the course of normal business is kept secure and confidential.
Containment	The practice of taking immediate corrective action to put an end to any unauthorized practices that may have led to a privacy breach
Disclosure	When personally identifiable information, personal health information, or any other information labelled as Confidential or Restricted is shared
Personal Health Information (PHI)	Section 4(1) of the Personal Health Information Protection Act (2004, S.O. 2004, c. 3, Sched. A) (PHIPA) states that “personal health information” means “identifying information about an individual in oral or recorded form, if the information, a. Relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family b. Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual c. Is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual d. Relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual e. Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance f. Is the individual’s health number g. Identifies an individual’s substitute decision-maker.” Section 4(2) states “identifying information” means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.”

Term	Definition
Personal Information (PI)	Section 2(1) of the Personal Information Protection and Electronic Documents Act (2000, c. 5) (PIPEDA) states that “personal information” (PI) means “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.” For example, personal information may include performance reviews, doctor’s notes, home address and a record of their sick days. PI includes both PII and PHI.
Personally Identifiable Information (PII)	Any information about an identifiable individual. This includes any data that can be used to identify you individually.
Personnel	Anyone working on behalf of guard.me International Insurance, including full-time, part-time, casual and other employees, volunteers, co-op placement students, contractors and consultants
Privacy	The right of the individual to control the collection, use, and disclosure of information about the individual, limiting it to that which is necessary. This includes having the right to determine what information is collected, how it is used, and the ability to access collected information to review its security and accuracy. It also means having the right to choose the conditions and extent to which one’s information is shared. In some jurisdictions, it also includes the right to have that information deleted
Privacy Breach	Inappropriate access, use, alteration, deletion, or disclosure of PII, PHI, Confidential or Restricted information including, without limitation: • Unauthorized collection, being the collection coercively or without consent or for purposes not approved by guard.me International Insurance or the individual. • Unauthorized use, being used for purposes not supported by guard.me International Insurance. • Unauthorized disclosure, being disclosure without consent or legal authority, security breaches or loss of equipment containing personal information such as laptops and mobile devices, or loss of paper records, or unauthorized or unsecured disposal of personal information. • Denial of client rights being the collection, use, or disclosure without consent, including the denial of access to personal information. Other breach examples include inappropriate access to client information (snooping), independently accessing one’s own PI or accessing the PI of a colleague, members of management or other guard.me International Insurance personnel, family member, friends, acquaintances and people featured in the media without consent.
Privacy Officer	A member of the guard.me International Insurance management team who is given the responsibility for managing the risks and business impacts of applicable privacy legislation and policies
Security	The practice of preventing unauthorized access to PII, PHI, Confidential or Restricted information through physical, organizational or technological means; also, the measures taken to ensure the confidentiality, integrity and availability of PI
Third Party Service Providers	Contracted third parties used to carry out or manage programs or services on behalf of guard.me International Insurance and for the purpose of privacy breach reporting, including all parties that receive PII, PHI, Confidential or Restricted information from guard.me International Insurance or collect PI on behalf of guard.me International Insurance.

4.0 Related Policies

The following are related to the prevention and management of privacy breaches:

- Internal Privacy Policy
- Privacy Policy for Websites
- Email Privacy Statement
- Access Control Policy
- Data Protection Policy
- Business Continuity and Disaster Recovery Policy

5.0 Policy

guard.me International Insurance has created a culture of privacy by embracing the philosophy of “Privacy by Design” and, as such, actively works to prevent privacy breaches by adhering to all privacy protocols set out in the guard.me International Insurance privacy policies. Should a privacy breach occur through the loss, theft, or unauthorized access, unauthorized change, or disposal of PII, PHI, Confidential or Restricted information of guard.me International Insurance personnel, insureds or clients, then the impact of the breach must be reported, contained and investigated, and a prompt, reasonable and coordinated response to the breach must be taken consistent with this policy.

6.0 Responsibilities

Term	Definition
Personnel of guard.me International Insurance	• Be alert to the potential for PII, PHI, Confidential or Restricted information to be compromised • If you become aware of a breach or potential breach, notify your Manager immediately • As appropriate, work to contain the breach by immediately suspending the process or activity that may have caused the breach
Managers	• Be alert to the potential for PII, PHI, Confidential or Restricted information to be compromised • As appropriate, work to contain the breach by immediately suspending the process or activity that may have caused the breach • Alert the Privacy Officer of a breach or suspected breach and work with them to implement the Privacy Breach Procedure (see section 8) • Obtain all available information about the nature of the breach or suspected breach, and determine the events involved • Ensure the details of the breach and any corrective actions are documented using the Privacy Breach Report Form • Inform the affected individuals, if required, and respond to questions or concerns
Privacy Officer	• Brief the Executive Team as necessary and appropriate • Review internal investigation reports and approve recommended remedial actions • Monitor the implementation of remedial actions • Ensure that those whose personal information has been compromised are informed as required • Escalate issues to the CEO and COO when required
Third Party Service Providers	• Take reasonable steps to monitor and enforce compliance with the privacy requirements defined in the contract or service agreement • Inform guard.me International Insurance of all breaches and potential breaches • With support from guard.me International Insurance, follow the steps outlined in the Privacy Breach Procedure (see section 8)

7.0 Privacy Breach Procedure

When a breach or potential breach is reported, initiate the following steps immediately.

1. **Respond & Report** – Complete the Privacy Breach Report Form and deliver it to your Manager. Include all required information:
   a. What happened
   b. Where the breach or potential breach occurred
   c. When it occurred
   d. How it was discovered
   e. The breach method (e.g., technology, paper files, verbally)
   f. Corrective actions taken
2. **Assess** – The Manager should assess the breach by asking the following questions:
   a. Was PII, PHI, Confidential or Restricted information involved?
   b. Has the unauthorized use, disclosure, alteration, or destruction of PII, PHI, Confidential or Restricted information occurred?
   c. Has PII, PHI, Confidential or Restricted information been lost or stolen?

The answers will determine if a breach has occurred. If so, continue with these steps.

1. **Contain** – Take immediate corrective actions to end the unauthorized practice that led to a breach. The main goal is to alleviate any consequences for both the individual(s) whose PII, PHI, Confidential or Restricted information was involved, as well as guard.me International Insurance. All containment activities or attempts to contain the privacy breach are to be documented on the Privacy Breach Report Form.
2. **Investigate** – Once the privacy breach is confirmed and contained, the Manager should conduct an investigation to determine the cause and extent of the breach:
   a. Identify and analyze the events that led to the privacy breach.
   b. Evaluate if the breach was an isolated incident or if a risk of further privacy breaches exists.
   c. Determine who was affected by the breach, e.g., clients or personnel, and how many individuals were affected.
   d. Evaluate the effect of containment activities.
   e. Evaluate who had access to the information.
   f. Evaluate if the information was lost or stolen.
   g. Evaluate if the personal, personal health, or confidential information has been recovered.
3. **Notify** – The Manager should consult with the Privacy Officer to determine what notifications are required. Some considerations include:
   a. Do we need to notify the authorities or other organizations? For example, the police if theft or other crimes are suspected, credit card companies, financial institutions, union, etc.
   b. Does the loss or theft of information place any individual at risk of physical harm, stalking or harassment?
   c. Is there a risk of identity theft? How reasonable is the risk?
   d. Could the loss or theft of information lead to hurt, humiliation, or damage to an individual's reputation, affecting their business or employment opportunities?

8.0 Notification

All individuals affected by a breach or potential breach should be notified as quickly as possible, and within legislated timeframes, of the breach occurring. This could include, but is not limited to, students, faculty and institutions.

8.1 Methods

The method of notification should be guided by the nature and scope of the breach and in a manner that is reasonable to ensure that the affected individual receives it. Direct notification by phone, letter, email or in person should be used where the individuals are identified. Refer to the Privacy Breach Notification Letter if responding via letter.

Where affected individuals are not fully known, media releases, website notices or letters to clients should be considered. A report of findings and actions taken should be made by the Privacy Officer.

Portions of the report or the full contents may be shared with the affected party whose privacy has been breached.

8.2 Responsibilities

- If the breach involved the PII, PHI, Confidential or Restricted information of an insured, the Manager of that program should notify the insured after consultation with the Privacy Officer.
- If the breach involved the PII, PHI, Confidential or Restricted information of guard.me International Insurance personnel, Human Resources should notify the affected personnel.
- If the breach involved the Confidential or Restricted information of clients, the assigned Account Manager should notify the client after consultation with the Privacy Officer.
- If there is a high risk of adverse publicity as a result of the breach, the Privacy Officer should notify those affected. As necessary, a determination should be made if external media / public relations support is required due to the severity of the breach.

Regardless of who is notifying those affected, the notification should include:

- Description of the incident and timing
- Description of the information involved
- The nature of potential or actual risks or harm
- What actions were taken/are being taken
- Any appropriate actions for the individual(s) to take in order to protect themselves against harm
- A contact person for questions or to provide further information

9.0 Corrective Actions to Prevent Further Breaches

Once the breach has been resolved, the Executive Team will work with the Manager to develop a prevention plan or take corrective action as required and will report back to the Privacy Officer for required approvals. Prevention activities can include audits, review of policies, procedures and practices, employee training or a review of service delivery.

10.0 Supporting Documentation

Name	Location
Privacy Breach Report Form.xlsx	Privacy Office SharePoint
Privacy Breach Notification Letter.docx	Privacy Office SharePoint

11.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action in line with the Disciplinary Policy.