TIMISKAMING
HOME SUPPORT / SOUTIEN À DOMICILE

POLICY AND PROCEDURE

Title: **Privacy Breach**	Date Issued: June 24, 2015
Approved by: Board of Directors	Review due: June 2017
Location: All	Revision# NEW
Signature: Betty Stone	Date signed: June 24th, 2015.
Policy #: HR 2015-15	Union X Non-Union X

1. INTRODUCTION

a) Purpose

The purpose of this policy is to provide direction in the event of a privacy breach of the personal or confidential information of Timiskaming Home Support (THS) clients or personnel. It will provide guidance on reasonable steps necessary to limit the breach, support an effective investigation and to assist with remediation.

b) Scope

This policy applies to all individuals who work for or are acting on behalf of THS, including employees, volunteers, students and members of the Board of Directors, and who are privy to personal or confidential information.

c) Definitions

i. **Privacy Officer:** The member of the THS team who is appointed with the responsibility for managing the risks and business impacts of privacy laws and policies.

ii. **Confidentiality:** The obligation of all THS personnel is to keep personal information secret. Confidentiality arises in the course of a relationship in which private information is shared. As the sharing of personal information is essential for accurate assessment, diagnosis, provision of services and/or treatment of THS clients, this ethical duty of confidentiality is imposed upon THS to ensure that client information obtained in the course of providing services is kept secure and confidential.

iii. **Confidential Information:** Any information of a sensitive matter that should remain confidential.

iv. **Disclosure:** Personal information of a sensitive matter that should remain confidential.

v. **Containment:** Containment involves taking immediate corrective action to put an end to the unauthorized practice that lead to a privacy breach.

vi. **Disclosure:** Personal information about an individual being provided to someone other than the individual or his/her substitute decision-maker or when confidential information is shared.

vii. **THS Personnel:** Every individual working or volunteering at THS including, but not limited to employees, managers, directors, senior management, casual and contract workers, volunteers, students, consultants, Board members, and Third Party Service Providers.

viii. **Personal Information:** Section 2(1) of the Personal Information Protection and Electronic Documents Act (2000, c.5) (PIPEDA) states that "personal information" 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.

ix. **Privacy:** The right of the individual to control the collection, use and disclosure of information about the individual, limiting it to what information is collected, how it is used, and the ability to access collected information to review its security and accuracy. Privacy means having the right to choose the conditions and extent to which one's information is shared.

x. **Privacy Breach:** An inappropriate access, use or disclosure of personal or confidential information including, without limitation:

- Unauthorized collection: collected coercively or without consent or for purposes not approved by THS or the individual
- Unauthorized use: used for purposes not supported by THS
- Unauthorized disclosure: disclosure without consent or legal authority, security breaches or loss of equipment containing personal unauthorized or unsecured disposal of personal information.

Other breach examples include inappropriate access into client information (snooping), independently accessing one's own personal information or that of a colleague, members of management or other THS personnel, family members, friends and acquaintances.

xi. **Security:** Preventing unauthorized access to personal or confidential information through physical, organizational or technological means. In other words, security is the measures taken to ensure the confidentiality, integrity and availability of personal information.

xii. **Third Party Service Providers:** Contracted third parties used to carry out or manage programs or services on behalf of THS and for the purposed of privacy

breach reporting include all parties that receive personal or confidential information from THS or collect personal information on behalf of THS.

d) Related Policies

i. Privacy Polices

- Client Records Collection & Disclosure Policy
- THS Personnel Records Collection & Disclosure Policy
- Records Retention & Destruction Policy

ii. Additional Policies

- Internet & Email Policy
- Mobile Device Policy

e) Legislative Context

- Child and Family Services Act
- Ontario's Health Care Consent Act
- Personal Health Information Act (PHIPA)2004
- Privacy and Personal Information Act ([IPA)
- Social Work and Social Service Work Act
- The Mental Health Act
- Home Care and Community Services Act

2. POLICY

It is THS policy to prevent privacy breaches by following a "culture of privacy" in adhering to all privacy protocols as detailed in THS's privacy policies. Should a privacy breach occur through the loss, theft or unauthorized access of personal or confidential information of THS personnel or client, then the impact of the breach must be contained, and a prompt, reasonable, and coordinated response to the breach must be taken consistent with this policy.

NOTE: The following section, 3, "RESPONSIBILITY AND PROCEDURE" represents best practices as determined by THS and is largely designed to provide guidance to designated THS representatives. However, it is understood that, where appropriate, these representatives may adopt modified procedures in response to any given circumstance.

3. RESPONSIBILITY & PROCEDURE

a) Privacy Breach Prevention & Containment

i. THS Personnel

Be alert to the potential for personal or confidential information to be compromised.

1) The program manager should be notified immediately, or in his/her absence the CEO (Chief Executive Officer) of THS, when THS personnel become aware of a breach or suspected breach.
2) Where possible, the personnel will contain the suspected breach by suspending the process or activity that caused the breach or potential breach.

ii. THS Managers

Be alert to the potential for personal or confidential information to be compromised.

1) Where possible, contain the suspected breach by suspending or confirming suspension of the process or activity that caused the breach or potential breach.
2) Alert the CEO and the Privacy Officer of the suspected breach, and work with him/her to implement the five steps of response protocol.
3) Inform the affected individuals, if required, and respond to questions or concerns.
4) Obtain all available information about the nature of the breach or suspected breach, and determine the events involved.
5) Ensure the details of the breach and corrective actions are documented using the Privacy Breach Report Form. (Attached)

iii. CEO & Managers

1) Ensure that the five steps of the Privacy Breach Protocol are implemented.
2) Notify THS Privacy Officer and ensure that the situation is discussed with the Privacy Officer prior to final resolution.
3) Support the THS manager responding to the breach.
4) Once the breach has been resolved, support the development of a prevention plan.
5) Make a report of findings and actions for the Privacy Officer.

iv. Privacy Officer

1) Brief the CEO and the Executive Management Team as necessary and appropriate.
2) Review the internal investigation reports and approve the recommended remedial action.
3) Monitor the implementation of the remedial action pertaining to privacy breaches.
4) Ensure that those whose personal information has been compromised are informed as required.

v. Third- Party Service Providers

1) Take reasonable steps to monitor and enforce their compliance with the privacy requirements defined in the contract or service agreement and inform their THS contact of all actual and suspected privacy breaches.
2) With support from the THS contact, follow the steps outlined in **SECTION 3 b) Privacy Breach Protocol.**

b) Privacy Breach Protocol

The following five steps will be initiated as soon as a privacy breach, or suspected breach, has been reported. The Privacy Breach Report Form will be used to document the breach and guide the manager through the breach management process.

STEP 1 Report and Assess

1) Report

Upon becoming aware of a possible breach of personal or confidential information, the suspected breach shall be promptly reported to the program manager. This shall occur even if the breach is suspected and not yet confirmed. The report shall attempt to capture:

- What happened?
- Where did it occur?
- When did the suspected incident occur?
- How was the potential breach discovered?
- What kind of information was breached eg> technology, paper files, shared through people?
- What corrective action was taken when the possible breach was discovered?

2) Assess

The manager shall assess the breach by asking the following questions:

Q1) Is personal or confidential information involved?

☐ Yes ☐ No

Q2) Has unauthorized collection, use, disclosure or retention of personal or confidential information occurred?

☐ Yes ☐ No

Q3) Has Personal or confidential information been lost or stolen?

☐ Yes ☐ No

If the answer is "yes" to question 1, and "yes" to either Question 2 or 3, then it can be assumed that a breach has occurred.

STEP 2 Containment

Containment involves taking immediate corrective action to put an end to the unauthorized practice that lead to a breach. For example, corrective action could include recovering the lost or stolen records; revoking/changing access codes or correcting weaknesses in an electronic security system. The main goal is to alleviate any consequences for both the individual(s) whose personal or confidential information was involved and THS. All containment activities or attempts to contain the privacy breach shall be documented on the Privacy Breach Report Form.

STEP 3 Investigate

Once the privacy breach is confirmed and contained the manager shall conduct an investigation to determine the cause and extent of the breach by:

1) Identify and analyze the events that led to the privacy breach. Did THS take reasonable precautions to prevent the breach?
2) Evaluate if the breach was an isolated incident or if there is a risk of further privacy breaches.
3) Determine who was affected by the breach e.g. clients or personnel, and how many individuals were affected.
4) Evaluate the effect of containment activities
5) Evaluate who had access to the information.
6) Evaluate if the information was lost or stolen.
7) Evaluate if the personal or confidential information has been recovered.

STEP 4 Notify

The manager shall consult with the CEO who will determine what notifications are required. Some considerations include:

1) Notification to authorities/other organizations. Examples include: Privacy Commissioner of Canada - https://www.priv.gc.ca/ , the police if theft or other crimes is suspected; credit card companies, financial institutions, the union, etc.
2) Does the loss or theft of information place any individual at risk of physical harm, stalking or harassment?
3) Is there a risk of identity theft? How reasonable is the risk?
4) Could the loss or theft of information lead to hurt, humiliation or damage to an individual's reputation?
5) Could the loss or theft of information result in damage to an individual's reputation, affecting his/her business or employment opportunities?

Timeline

Affected individuals should be promptly notified and receive the initial notification as soon as possible after the breach has occurred. Further communication with the affected individuals may occur during the process as updates occur.

Method

The method of notification shall be guided by the nature and scope of the breach and in a manner that is reasonable to ensure that the affected individual will receive it. Direct notification e.g. by phone, letter, email or in person shall be used where the individuals are identified. Where affected individuals are not fully known, media releases, website notices or letters to clients shall be considered. A report of findings and actions taken will be made by the CEO, Managers and Privacy Officer.
Portions or all of the report may be shared with the affected party or parties whose information has been breached.

Responsibility for Notification
If the breach was client information the manager of that program will provide the notification. In the event that the breach was personal information of THS personnel, the CEO along with the Human Resources Coordinator will provide the notification.

In the instance where there is a high risk of adverse publicity as a result of the breach the CEO will be responsible for the notification. As necessary, a determination will be made if external media/public relations support is required due to the severity of the breach.

Notification shall 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

STEP 5 Prevention of Future Breaches

Once the breach has been resolved, the CEO, Privacy Officer and Managers will work together to develop prevention plan or take corrective actions as required. Prevention activities might include: audits; review of policies, procedures and practices; employee training or a review of service delivery.

c) Supporting Documentation

Form – Privacy Breach Report (see attached)

TIMISKAMING
HOME SUPPORT / SOUTIEN À DOMICILE

PRIVACY BREACH INCIDENT REPORT FORM

Date:	
Name of Organization	
Contact Information (contact name, telephone number, address	
Sector affected	
Third Party reporting the breach (if applicable)	
Identification of the third party (contact name, telephone number, address)	
Details of the Incident	
Location, date of incident and discovery	
Description of incident	
Cause (if known)	
Estimated number of individuals affected (e.g. customers, employees)	
Types of personal information involved	
Brief Description of action take to contain the breach	
Has anyone been notified of incident (e.g. affected individuals, law enforcement, other)	

and when (date)?	