SECTION: A. Organizational Policies, Procedures and Guidelines
SUB-SECTION: Systems And Structures
POLICY: **SS A.6 BREACH OF PRIVACY OF INFORMATION**
CROSS-REFERENCE: CCA-ORG-SS- 2.1 St. Mary's Home Policy – SS – Collection, Use and Release of Personal Information St. Mary's Home Policy – SS – Privacy of Personal Health Information

EFFECTIVE DATE: September 2010; November 2016; July 2017	REVISION DATE: September 2016; October 2016; May 2017

PURPOSE:

- To establish procedures in the event that a breach in the privacy of information occurs

POLICY:

In the event that a privacy of information breach occurs, the Executive Director is responsible for the assessing the situation and the implementing an appropriate action plan.
The key objectives should be to:

- Respond in a timely manner and appropriate to the nature of the breach;
- Contain the breach;
- Develop and implement a notification strategy that is timely and comprehensive (where appropriate); and
- Review existing policies and procedures to ensure that the breach does not happen again.

PROCEDURES:

Proactive Measures

Prior to a privacy breach occurring, St. Mary's Home has implemented the following proactive measures:

- Identify the team that should be assembled to respond to a breach (providing for flexibility depending on units that are affected);
- The team meets occasionally to ensure that the policy remains current and any relevant technologies are still secure;
- When reviewing policy, the team consults with like agencies to share processes; and
- Ensure that front-line staff is adequately trained in privacy policies and procedures and that they are aware of how to report a breach in privacy.

Response Steps

- The breach of privacy team investigates the breach and develops and implements an action plan (including an internal communications plan to communicate to employees);

The team will:

- Investigate the facts surrounding the breach, including:
    - The chain of custody for the information;
    - The date the breach occurred;

    - How the breach occurred;
    - The extent of the breach;
    - When the breach was discovered;
    - The number of individuals affected by the breach;
    - The nature of the information that is the subject of the breach (e.g. personal health information, financial information, contact information, etc.);
    - Whether there are any physical or technological impediments to unauthorized access to the information (e.g., password protection, encryption, etc.);
    - Whether the information has already been inappropriately used or disclosed, and the likelihood that it will be in the future; and
    - Whether other information is at risk.
- Determine the law(s) that may apply to the privacy breach;
- Assess the risk of harm if the information is, in fact, inappropriately used or disclosed (e.g., physical harm, fraud, identity theft, embarrassment, etc.);
- Identify the steps that St. Mary's Home can take to mitigate the effect of the breach, both internal (e.g., retrieve copies, change passwords or access rights, back up databases) and external (e.g., notify affected individuals, law enforcement, privacy commissioners or regulatory authorities, etc.);
- Develop a notification plan to advise clients of the breach (e.g., direct notification of affected individuals or indirect notification through public announcements), and determine what information to provide, including the following:
    - the fact that a privacy breach occurred and a description of it;
    - the sort of personal information that is involved;
    - the steps the organization has taken to mitigate the harm, and any likely further steps;
    - the steps affected individuals can take to further mitigate the risk of harm;
    - a statement that affected individuals may have a right to complain to a privacy commissioner;
    - contact information of the organization where individuals can obtain additional information or assistance;
    - identification and implementation of steps to be taken to prevent a reoccurrence (e.g., changes to procedures, policies and contractual templates, changes to physical or technological safeguards and employee training) and;
    - development and implementation of a communication plan to manage follow-up questions and requests from affected individuals, employees, regulators, law enforcement and the media.