Policy Title: **Privacy Breach of Personal Health Information**	Policy Owner: Privacy Officer	
	Approval By: CEO	
	Effective Date	Revision Date
	January 2010	May 2019
Key Words: personal confidential confidentiality information release protection disclosure divulge protect compliance without authority contravene disciplinary action reveal disclose disobey disregard tell details inappropriate gossip hearsay rumor		

POLICY

1.0 St. Thomas Elgin General STEGH (STEGH) is classified as a Health Information Custodian (HIC) under the Personal Health Information Protection Act 2004 (PHIPA) and is governed by such act to protect all personal information and personal health information (PHI) under its custody and control.

1.1 STEGH is also a partner within regionally shared electronic patient records (EPR) and is accountable for adhering to all requirements set forth in any Memorandum of Understanding (MOA) as it relates to the (EPR).

1.2 In order to ensure compliance with PHIPA, it is STEGH's policy that all employees and affiliates will:

- 1.2.1 Comply with obligations related to privacy and confidentiality;
- 1.2.2 Protect and secure all personal health information (PHI) entrusted to them, to prevent a breach of a patient's privacy;
- 1.2.3 To act immediately if made aware of an actual or potential privacy breach;
- 1.2.4 Participate in the investigation and management of a privacy breach with appropriate representation, as applicable.

1.3 A privacy breach occurs whenever:

- 1.3.1 PHI is lost or stolen;
- 1.3.2 PHI is accessed (including accessing one's own record) disclosed, copied or modified without authority;
- 1.3.3 Disposal of PHI has occurred in an insecure manner;
- 1.3.4 Any other situation where an employee, or affiliate has contravened, or is about to contravene the Personal Health Information Protection Act (PHIPA) 2004.

1.4 A privacy breach can occur via verbal or written communication, via phone, e-mail, fax or any other medium.

1.5 A privacy breach can be actual or potential. (See definitions of actual or potential privacy breaches for examples).

1.6 Pursuant to (PHIPA 2004), STEGH must notify a patient, or the patient's Substitute Decision Maker (SDM), if there has been a breach of privacy related to their PHI. It is the responsibility of the Privacy Officer or delegate, in collaboration with the Service Area/Department Manager or delegate, to notify the patient or SDM.

1.7 A breach of privacy may be cause for disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation with the organization as outlined in the

Privacy Policy, Confidentiality Policy and the Privacy and Confidentiality Agreement signed by all employees and affiliates.

PROCEDURE

2.0 In accordance with guidelines provided by the Office of the Information and Privacy Commissioner of Ontario, STEGH will take the following steps when made aware of a potential or actual privacy breach.

2.1 Step 1: Act Immediately: Contain the Breach and Secure the Personal Health Information

2.2 Employees, and affiliates, upon learning of a potential or actual privacy breach must notify the Privacy Officer or delegate, their manager or delegate, or Manager-on-Call immediately. If the manager or delegate, or Manager On-Call are first notified it will be their responsibility to contact the Privacy Officer or delegate as soon as possible. **The employee is to enter the breach into Risk Monitor Pro.**

2.3 Depending on the severity and nature/type of the breach:

2.3.1 The Privacy Officer or delegate may involve the following individuals as soon as reasonably possible:

- Chief Executive Officer
- Chief of Staff
- Operations Manager in charge of Security
- Risk Management
- Human Resources
- Communications/Public Relations
- Information Management, and/or the Trusted User (if immediate suspension of access is required to further contain the breach)
- Police if the breach may reasonably be considered to result in significant harm to the patient or third party
- Others as deemed necessary

2.4 The Privacy Officer or delegate, Manager or delegate or Manager On-Call will direct employees, and affiliates to immediately contain the breach. Containing the breach may include:

2.4.1 Determining whether the breach would allow unauthorized access to any other personal health information and, if so, take any and all steps necessary to contain the breach, e.g. change passwords, or temporarily shut down a system;

2.4.2 Suspending a users' access to patient care systems or other hospital systems to prevent reoccurrence of the breach. Suspending a user's access will only be done with the authority of both the employee's manager or delegate and their Director in consultation with Human Resources;

2.4.3 Notifying the employee(s) or affiliates involved of the situation, indicating that an investigation is being conducted, and that the Privacy Officer or delegate will be monitoring their access;

2.4.4 In the case of information that has been mailed or faxed to the wrong recipient retrieving the information by:

- Obtaining contact information from the recipient;
- Asking the recipient to place the information in a sealed envelope and place in a secure area;
- Asking the recipient not to make any copies of the information;

- Notify the Privacy Officer or delegate who will arrange a courier to retrieve the information;

3.0 Step 2: Investigate the Potential/Actual Breach and Evaluate the Risks Associated with the Breach

3.1 The Privacy Officer or delegate, in collaboration with the affected Service Area/Department Manager or delegate and others as appropriate (e.g. Risk Management, and/or Human Resources), will conduct an investigation to determine the extent of the breach. Steps that may be taken as part of the investigation include:

3.1.1 Auditing the electronic patient record (EPR);
3.1.2 Hard copy health record review;
3.1.3 Interviews with employees, Physicians, students, volunteers, or affiliates;
3.1.4 Interviews with patients and or Substitute Decision Maker (SDM).

3.2 Depending on the severity of the breach, the Privacy Officer or delegate, in conjunction with the affected Service Area/Department's Manager or delegate and/or Risk Management, may initiate a Breach Management Team to facilitate the investigation and management of the breach.

3.3 **The Breach Management Team** will identify and manage risks associated with the breach, including risk related to:

3.3.1 Reputation of the organization
3.3.2 Patient trust
3.3.3 Media
3.3.4 Legal
3.3.5 Collaborate on determining next steps/actions

3.4 **Outcomes for employee/affiliate:**

3.5 On completion of the investigation, the Service Area/Department Manager, in collaboration with Human Resources or Medical Affairs (depending on whether the individual is an employee or affiliate) determines the most appropriate outcome for the employee/affiliate. Possible outcomes may include one or more of the following:

3.5.1 Education
3.5.2 Verbal warning
3.5.3 Written warning
3.5.4 Suspension of employment or service contract
3.5.5 Termination of employment or service contract

3.6 Several factors will be considered when determining the outcome.

4.0 Step 3: Patient Notification

4.1 The Privacy Officer or delegate, in collaboration with the affected Service Area/Departments Manager's or delegate are legally required to notify a patient, or an incapable patient's Substitute Decision Maker (SDM), if the patient's information has been lost, stolen or accessed without authority.

4.2 Notification of a patient/SDM may be done verbally, or in writing, depending on several factors:

4.2.1 Availability of the patient/SDM, i.e. if the patient is in hospital at the time of notification, or coming into hospital in the near future, it may be appropriate for the physician or manager to notify the patient in person,

4.2.2 Relationship with the patient i.e. if the physician or manager has an established clinical relationship with the patient, it may be appropriate to notify the patient in person.

4.3 When applicable, the notification indicates that an employee has received disciplinary action but does not disclose details of the action, e.g. that the staff received a written warning or a suspension. The initial notification does not disclose the name of the employee who committed the breach, but if the patient requests this information, this information is disclosed. The notification letter is to be attached to the RMPro file.

4.4 Multi-organization Privacy Breach

4.4.1 In the event that an actual, or potential breach is identified as involving or potentially involving another organization(s)' employee/user and/or a patient's Personal Health Information, through the electronic patient record (EPR) within the South West LHIN, the Multi-Org Breach Policy is be followed. STEGH's Privacy Officer will notify the Privacy Officer or delegate from the organization affected by the breach.

4.5 Other Affected Organizations

4.5.1 Depending on the severity of the breach, the Privacy Officer or delegate is responsible to notify other groups, based on legal, professional or contractual obligations (e.g. ONA).

4.6 The Office of the Information Privacy Commissioner of Ontario (IPC)

4.6.1 Depending on the severity of the breach, the Privacy Officer or delegate is responsible to submit a report outlining the breach, the investigation, patient notification and outcome to the Office of the Information Privacy Commissioner of Ontario and work with the Commissioner's staff to ensure the organization has met its legal obligations under PHIPA.

5.0 Step 4: Managing the Risk of Future Breaches

5.1 Depending on the severity of the breach, those involved in managing the breach will review the breach and information obtained as part of the investigation with an aim to take measures to reduce the risk of reoccurrence.

5.2 These measures may include, but are not limited to:

5.2.1 Changes to processes, policies or procedures;

5.2.2 Additional education and training for employees and/or affiliates related to personal health information and their accountabilities for confidentiality and the protection of patients privacy rights;

5.2.3 Reviewing and enhancing the programs or department's security of personal health information.

DEFINITIONS

Affiliates: Individuals who are not employed by the organization but perform specific tasks at or for the organization, including appointed professionals (e.g., physicians/midwives/dentists), students, volunteers, researchers, contractors, or contractor employees who may be members of a third-party contract or under direct contract to the organization, and individuals working at the organization, but funded through an external source.

Health Information Custodian: Listed persons or organizations under the Personal Health Information Protection Act such as hospitals, who have custody or control of personal health

information as a result of the work they do. As a public hospital, STEGH is considered to be a Health Information Custodian.

Personal health information is any identifying information with respect to an individual, whether living or deceased and includes:

- Information concerning the physical or mental health of the individual;
- Information concerning any health service provided to the individual;
- Information concerning the donation by the individual of any body part or any bodily substance of the individual;
- Information derived from the testing or examination of a body part or bodily substance of the individual;
- Information that is collected in the course of providing health services to the individual; or
- Information that is collected incidentally to the provision of health services to the individual.

Privacy Breach – Actual - *includes, but is not limited to:*

(a) Accessing patient personal health information when it is not required to provide or maintain care to a patient or in the performance of duties, for example:

- Directly accessing the electronic health record of oneself without following Health Records Department procedure;
- Accessing the health record of an employee, family member, friend, or anyone for whom there is no requirement to view information based on providing care or performing duties;
- Accessing any patient information (e.g. address, date of birth, next of kin, etc.) of an employee, family member, friend, or anyone for whom there is no requirement to view information based on providing health care or performing duties.

(b) Discussing patient information with:

- Another person who is not involved in the direct care of the patient or does not require the information to perform their job functions; or
- Within range of other people in a non-patient care area of the hospital. (For example: discussing information related to patient care with another employee in the elevator or cafeteria).

(c) Failing to ensure the security of patients' PHI, for example:

- Faxing or e-mailing PHI to the wrong recipient;
- Theft of electronic devices containing identifiable patient information.

Privacy Breach – Potential – *occurs when an individual's personal health information is at high risk of being accessed, used or disclosed inappropriately by or to individuals or for purposes other than consented to by the patient. A potential privacy breach includes, but is not limited to:*

- Allegations of a privacy breach by a patient or employee/affiliate;
- Concerns related to security of PHI raised by a patient or employee/affiliate;
- Request by a patient for additional security around their PHI (e.g. Lock Box);
- Leaving patient information in unattended or unsecured locations where it may be accessed by unauthorised persons;
- Leaving access to electronic patient information unattended on an open log in;
- Storing electronic patient identifiable information on portable information devices or un-secure drives, e.g. hard drives that have not been encrypted;
- Loss of a hard copy health record or other identifiable patient information.

Substitute Decision Maker (SDM) is defined as a person who is:

- At least 16 years of age, unless he or she is the incapable patient's parent;
- Capable with respect to the treatment;
- Not prohibited by court order or separation agreement from having access to the incapable patient or giving or refusing consent on the incapable patient's behalf;
- Available; and
- Willing to assume the responsibility of giving or refusing consent.

In descending order of priority, an incapable patient's SDM may be:

i. The incapable patient's **"guardian of the person"**, appointed under the Substitute Decisions Act, 1992, if the guardian has authority to give or refuse consent to the treatment;
ii. The incapable patient's **"attorney for personal care"**, given under the Substitute Decisions Act, 1992, if the power of attorney confers authority to give or refuse consent to treatment;
iii. The incapable patient's **"representative"** appointed by the Consent and Capacity Board, if the representative has authority to give or refuse consent to the treatment;
iv. The incapable patient's **spouse or partner**;
v. A **child or parent (custodial)** of the incapable patient, or a Children's Aid Society or other person who is lawfully entitled to give or refuse consent to the treatment in the place of the parent;
vi. A **parent (who has only a right of access)** of the incapable patient;
vii. **A brother or sister** of the incapable patient;
viii. **Any other relative** of the incapable patient;
ix. The **Public Guardian and Trustee**.

REFERENCES

Thames Valley Hospital Planning Partnership (TVHPP) Memorandum of Understanding, Privacy and Security Schedule
Personal Health Information Protection Act, 2004
Public Hospitals Act 1990 (as amended)
Regulated Health Professions Act 1991 (as amended)
College of Nurses of Ontario, Standards of Practice – Confidentiality and Privacy - Personal Health Information
College of Physicians and Surgeons of Ontario – Confidentiality and Access to Patient Information
Anonymous Patient Policy
Confidentiality Policy
Corrective Action Policy
Privacy Policy
Acceptable Use of Information Technology Resources Policy