Policy Title:	Privacy Policy	
Policy Author:	Manager, Health Information	
Policy Owner: *(Approval)*	CFO & Privacy Officer	
Version #:		
Original Effective Date: August 2004		**Reviewed/Revised Date:** May 2023
Key Words: *Breach of Privacy, Confidentiality, Photography, Video and Audio Recording, Use of Personal Health Information for Research, Education and Quality Improvement, Patient Request to be Anonymous, Disclosure to Law Enforcement, Correction of Personal Health Information, Protecting Personal Health Information During Billing, Freedom of Information Requests, Patient Requests to Restrict Use and Disclosure of Personal Health Information, Access and Disclosure of Personal Health Information*		

POLICY STATEMENT

The purpose of this policy is to establish expectations for the collection, use, disclosure and retention of Personal Health Information (PHI) at St. Thomas Elgin General Hospital (STEGH) as per Personal Health Information Protection Act (PHIPA). STEGH is committed to maintaining a high standard of privacy and has implemented policies and procedures to ensure PHI is kept confidential and secure while allowing for the effective delivery of health care.

AUDIENCE

This policy applies to all STEGH staff, including individuals working at STEGH funded through an external source, physicians, residents, volunteers, learners and contract workers with access to PHI at STEGH. It applies to work conducted both onsite on STEGH owned and rented properties and remote work.

DEFINITIONS

Affiliates – Individuals who are not employed by the organization but perform specific tasks at or for the organization, including:

- Credentialed Professional Staff with a hospital appointment (e.g. physicians, midwives, dentists),
- Learners,
- Volunteers,
- Contractors or contracted workers who may be members of a third-party contract or under direct contract with the organization, and
- Individuals working at the organization but funded through an external source.

Health Information Custodian – A listed individual or organization under the Personal Health Information Protection Act (PHIPA) that, as a result of its powers or duties, has custody or control of personal health information.

Personal Health Information – As defined by the Personal Health Information Protection Act (PHIPA), identifying information about an individual, in oral or recorded form, if the information:

- Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- 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,
- Is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual,
- Relates to payments or eligibility for health care in respect of the individual,
- 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,
- Is the individual's health number, or
- Identifies an individual's substitute decision-maker.

Personal Information – As defined by the Freedom of Information and Protection of Privacy Act (FIPPA), recorded information about an identifiable individual, including:

- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- Any identifying number, symbol or other particular assigned to the individual,
- The address, telephone number, fingerprints or blood type of the individual,
- The personal opinions or views of the individual except where they relate to another individual,
- Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- The views or opinions of another individual about the individual, and
- The individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Personal information does not include:

- Information about an individual who has been dead for more than thirty years, and
- The name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.

Substitute Decision Maker (SDM) – If an individual is determined to be incapable of consenting to the collection, use or disclosure of personal health information by a health information custodian, the Personal Health Information Protection Act (PHIPA) lists in order of rank the following deciders:

- The individual's guardian of the person or guardian of property, if the consent relates to the guardian's authority to make a decision on behalf of the individual,

- The individual's attorney for personal care or attorney for property, if the consent relates to the attorney's authority to make a decision on behalf of the individual,
- The individual's representative appointed by the Board under section 27, if the representative has authority to give the consent,
- The individual's spouse or partner,
- A child or parent of the individual, or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent. This paragraph does not include a parent who has only a right of access to the individual. If a children's aid society or other person is lawfully entitled to consent in the place of the parent, this paragraph does not include the parent,
- A parent of the individual with only a right of access to the individual,
- A sibling of the individual, and
- Any other relative of the individual.

PROCEDURE

STEGH protects the privacy of individuals and their Personal Information (PI) and PHI. As a health information custodian, STEGH, staff and affiliates are responsible for complying with the Personal Health Information Protection Act (PHIPA).

Patients/substitute decision makers (SDMs)/ Power of Attorney (POA) have the right to request access to the patient's own PHI under STEGH's custody and control. STEGH staff/affiliates may not access their own paper and/or electronic health records outside of this process. (Refer to Access or Disclosure of Personal Health Information Policy.)

STEGH takes reasonable steps to ensure that PHI is as accurate, complete, and up-to-date as is required for the purpose(s) for which it is to be used.

- Limitations on the accuracy and completeness of PHI disclosed will be clearly set out to the recipient where possible.
- An individual will be able to challenge the accuracy and/or completeness of their PHI and have it amended, as appropriate (refer to Patient Requests to Amend Health Information Policy).

In compliance with PHIPA, STEGH will inform individuals of the loss, theft and/or the unauthorized use or disclosure of their PHI as soon as reasonably possible (refer to Privacy Breach of Personal Health Information Policy).

An individual has the right to challenge STEGH's compliance with PHIPA and this policy.

STEGH monitors patient care systems for compliance with legislative and organization requirements. Noncompliance to the act will be considered a breach of privacy and can lead to fines under the act (refer to Privacy Breach of Personal Health Information Policy).

STEGH investigates all complaints and suspected breaches of privacy or confidentiality. If a complaint or suspected breach is found to be justified, STEGH will take appropriate measures, including, amending policies and procedures, if necessary. Breaches of this policy and privacy-related policies and procedures may be subject to disciplinary action, as outlined in Privacy Breach of Personal Health Information Policy and Confidentiality Policy. STEGH, staff and affiliates are subject to the fines and penalties set out in PHIPA.

STEGH has established requirements related to the secondary use of PHI for education, research and quality assurance purposes to ensure its compliance with the rules under PHIPA (refer to Use of Personal Health Information for Research, Education and Quality Assurance Policy).

STEGH will retain PHI only as long as necessary for the fulfillment of legal and regulatory requirements. STEGH has established timelines and requirements for the retention of records of PHI and the appropriate practices for the timely and secure disposal of PHI (refer to Records Retention and Destruction Policy).

STEGH will make specific information about its policies and practices relating to the management of PHI readily available to individuals (see STEGH's Privacy Program).

For information about STEGH's PI practices and obligations under the Freedom of Information and Protection of Privacy Act (FIPPA), refer to Freedom of Information and Protection of Privacy Policy.

ROLES AND RESPONSIBILITIES

1.0. Employer will:

1.0.1. Ensure all staff/affiliates and others working on its behalf are aware of their duties related to privacy by requiring them to sign confidentiality agreements before gaining access to PHI, complete corporate privacy training on an annual basis and/or include privacy-related terms and conditions in agreements with STEGH.

1.0.2. Ensure legislative compliance with appointment of a Corporate Privacy Officer/delegate(s) who are responsible for overseeing STEGH's privacy program.

1.0.3. Protect the safety and respect the confidentiality of PHI through appropriate access safeguards, as per the Information Security Policy and Acceptable Use of Information Technology Resources Policy.

1.0.4. Implement safeguards to protect PHI against loss or theft as well as unauthorized access, disclosure, copying, use or modification, regardless of the format in which the PHI is held, appropriate to the sensitivity of the information.

1.0.5. Ensure consent of the individual is obtained for the collection, use, or disclosure of PHI, as required by law.

1.0.6. Ensure the collection of PHI is limited to what is necessary for the purposes identified to the patient/SDM/POA.

1.0.7. Ensure PHI is collected by fair and lawful means.

2.0. Privacy Office will:

2.0.1. Monitor adherence to privacy related policies and procedures using a risk-based model and other methods (e.g. auditing user activity in electronic health systems, etc.) and report concerns to the most responsible leader.

2.0.2. Provide guidance materials to promote privacy standards (e.g. emails, brochures and other communications).

3.0. Area Leadership will:

3.0.1. Provide communication and education for privacy policies, procedures and best practice expectations, as per the Privacy Officer.

3.0.2. Ensure all staff and affiliates are compliant with privacy policies and procedures.

3.0.3. Notify the Privacy Officer immediately of all concerns of suspected breaches of privacy policies and procedures. (privacyofficer@stegh.on.ca)

3.0.4. Participate in investigations in collaboration with the Privacy Officer for any suspected breaches to privacy at STEGH.

4.0. Staff/affiliates will:

4.0.1. Adhere to STEGH's privacy standards and their responsibilities as set out in the privacy related policies and procedures.

4.0.2. Limit the collection of PHI to what is necessary and permitted, including:

4.0.2.1. Delivery of patient care,

4.0.2.2. Administration of the health care system,

4.0.2.3. Research,

4.0.2.4. Education,

4.0.2.5. Quality improvement and quality assurance,

4.0.2.6. Fundraising, and

4.0.2.7. Meet legal and regulatory requirements as described in PHIPA.

4.0.3. Ensure patients/SDMs/POAs are aware of the purpose(s) for the collection of their PHI.

4.0.4. Identify the new purpose and intended use of previously collected PHI before using the PHI. Contact the Privacy Officer (privacyofficer@stegh.on.ca) for further information, as required.

4.0.5. Ensure consent of the individual is obtained for the collection, use, or disclosure of PHI, as required by law.

4.0.6. Comply with the Personal Health Information and Protection Act (PHIPA) and its regulations.

4.0.7. Become familiar with and follow the organization's policies and procedures regarding the collection, use, disclosure, storage, security and destruction of confidential information.

4.0.8. Collect, access, use, disclose, copy, transmit or release confidential information only as authorized and required to provide care or perform their assigned duties.

4.0.9. Report to their leader actual or suspected breaches of privacy policies, procedures and practices implemented by the hospital, or a breach of PHIPA. If the leader is the individual suspected of the breach, staff/affiliates may contact the Privacy Officer or privacyofficer@stegh.on.ca , as applicable.

4.0.10. Securely return all property of the hospital including keys and records of PHI, if any, at the conclusion of their employment/affiliate relationship.

REFERENCES

Legislation
Personal Health Information Protection Act

Corporate
Information Security Policy
Acceptable Use of Information Technology Resources Policy
Records Retention and Destruction Policy
Remote Access Policy
System Access Policy
Personal Use of Mobile and Electronic Devices in the Workplace Policy

Other Resources
Information and Privacy Commissioner of Ontario
privacyofficer@stegh.on.ca