Policy Title:	Policy Owner: Privacy Officer	
Privacy Policy	**Approval By:** CEO	
	Effective Date	**Revision Date**
	August 2004	May 2019
Key Words: personal confidential confidentiality information release protection disclosure protect		

POLICY

St. Thomas Elgin General Hospital (STEGH) (hereafter referred to as "the Hospital") is responsible for personal information under the organization's custody and control and is committed to a high standard of privacy for its information practices.

The privacy policy is the foundation for other policies and procedures, setting the principles upon which the Hospital collects, uses and discloses personal information and personal health information.

PROCEDURE

The Hospital adopted the following10 Principles set out in the National Standard of Canada Model Code for the Protection of Personal Information:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

This policy will apply to personal information and personal health information collected, used, disclosed and retained by the Hospital, subject to legal requirements.

1.0 Principle 1 - Accountability for Personal Information

1.1 The Hospital is responsible for personal information under their control and have a Privacy Officer who is accountable for compliance at the Hospital using the following principles:

1.2 Accountability for the Hospitals' compliance with the policy rests with the Chief Executive Officer, and, ultimately the Board, of each organization, although other individuals within the Hospital are responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the Hospital are delegated to act on behalf of the Chief Executive Officer, such as the Privacy Officer.

1.3 The name of the Privacy Officer designated by the Hospital to oversee compliance with these principles is a matter of public record.

1.4 The Hospital is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The Hospital will use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

1.5 The Hospital will:
- 1.5.1 Implement policies and procedures to protect personal information, including information relating to patients, staff, and agents.
- 1.5.2 Establish policies and procedures to receive and respond to complaints and inquiries.
- 1.5.3 Train and communicate to staff and agents information about the Hospitals' privacy policies and practices.
- 1.5.4 Develop plans and communicate to the public and key hospital stakeholders' information to explain the Hospital's privacy policies and procedures.

2.0 Principle 2 - Identifying Purposes for the Collection of Personal Information

At or before the time personal information is collected, the Hospital will identify the purposes for which personal information is collected. The primary purposes for collecting personal information are the delivery of direct patient care, the administration of the health care system, research, teaching, statistics, fundraising, and meeting legal and regulatory requirements.

2.1 Identifying the purposes for which personal information is collected at or before the time of collection allows the Hospital to determine the information they need to collect to fulfill these purposes.

2.2 The identified purposes are explained at or before collection (of the information) to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this explanation can be given orally or in writing: for example, an admission form, or posted notice, may give notice of the purposes. A patient who presents for treatment, and receives an explanation, is also giving implied consent for the use of his or her personal information for authorized purposes. Patients will be given the option to accept or reject each such use.

2.3 When personal information, that has been collected, is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.

2.4 Persons collecting personal information will be able to explain to individuals the purposes for which the information is being collected.

3.0 Principle 3 - Consent for the Collection, Use, and Disclosure of Personal Information

3.1 The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

3.2 ***Note***: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual: for example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, if the Hospital does not have a direct relationship with the individual, it may not be possible to seek consent.

3.3 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, the Hospital will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use

or disclosure may be sought after the information has been collected, but before use (for example, when the Hospital wishes to use information for a purpose not previously identified).

3.4 The principle requires "knowledge and consent". The Hospital will make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

3.5 The Hospital will not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

3.6 The form of the consent sought by the Hospital may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, the Hospital will take into account the sensitivity of the information.

3.7 In obtaining consent, the reasonable expectations of the individual are also relevant. The Hospitals can assume that an individual's request for treatment constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to the Hospitals would be given to a company selling health-care products.

3.8 The way in which the Hospital seeks consent may vary, depending on the circumstances and the type of information collected. The Hospital will generally seek express consent when the information is likely to be considered sensitive (e.g., genetic testing). Implied consent would generally be appropriate when the information is less sensitive. An authorized representative such as a substitute decision maker if the patient is not capable, a legal guardian or a person having power of attorney can also give consent.

3.9 Individuals can give consent in many ways, for example:

- 3.9.1 An admission form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- 3.9.2 A check-off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
- 3.9.3 Consent may be given orally when information is collected over the telephone, or
- 3.9.4 Consent may be given at the time that individuals use a health service.

3.10 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The Hospital will inform the individual of the implications of such withdrawal.

4.0 Principle 4 - Limiting Collection of Personal Information

4.1 The collection of personal information will be limited to that which is necessary for the purposes identified by the Hospitals. Information will be collected by fair and lawful means.

4.2 The Hospital will not collect personal information indiscriminately. Both the amount and the type of information collected will be limited to that which is necessary to fulfill the purposes identified.

4.3 The requirement that personal information be collected by fair and lawful means is intended to prevent the Hospital from collecting information by misleading or deceiving individuals about the

purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

5.0 Principle 5 - Limiting Use, Disclosure, and Retention of Personal Information

5.1 Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information will be retained only as long as necessary for the fulfillment of those purposes.

5.2 If using personal information for a new purpose, the Hospital will document this purpose.

5.3 The Hospital will develop guidelines and implement procedures with respect to the retention of personal information. These guidelines will include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual will be retained long enough to allow the individual access to the information after the decision has been made. The Hospital is subject to legislative requirements with respect to retention periods.

5.4 Personal information that is no longer required to fulfill the identified purposes will be destroyed, erased, or made anonymous. The Hospital will develop guidelines and implement procedures to govern the destruction of personal information in accordance with applicable legislative requirements.

6.0 Principle 6 - Ensuring Accuracy of Personal Information

6.1 Personal information will be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

6.2 The extent to which personal information will be accurate, complete, and up to date will depend upon the use of the information, taking into account the interests of the individual. Information will be sufficiently accurate, complete, and up to date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

6.3 The Hospital will not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

6.4 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, will generally be accurate and up to date, unless limits to the requirement for accuracy are clearly set out.

7.0 Principle 7 - Ensuring Safeguards for Personal Information

Security safeguards appropriate to the sensitivity of the information will protect personal information.

7.1 The security safeguards will protect personal information against loss, theft, unauthorized access, disclosure, copying, use, or modification. The Hospital will protect personal information regardless of the format in which it is held.

7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. A higher level of protection will safeguard more sensitive information, such as health records.

7.3 The methods of protection will include:
- 7.3.1 Physical measures, for example, locked filing cabinets and restricted access to offices;
- 7.3.2 Organizational measures, for example, limiting access on a "need-to-know" basis, and
- 7.3.3 Technological measures, for example, the use of passwords, encryption and audits.

7.4 The Hospital will make its staff and agents aware of the importance of maintaining the confidentiality of personal information. As a condition of employment, appointment, or agency, all hospital staff and agents must complete the hospital Privacy & Security Training which includes signing the Hospital's Confidentiality Agreement annually. In addition, those with access to electronic health records must sign individual User Agreements and complete an annual Privacy Learning Module System

7.5 Care will be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

8.0 Principle 8 - Openness About Personal Information Policies and Practices

8.1 The Hospital will make readily available to individuals specific information about its policies and practices relating to the management of personal information.

8.2 The Hospital will be open about their policies and practices with respect to the management of personal information. Individuals will be able to acquire information about the hospital's policies and practices without unreasonable effort. This information will be made available in a form that is generally understandable.

8.3 The information made available will include:
- 8.3.1 The contact information to reach members of the Privacy Office who are accountable for the Hospital's privacy policies and practices, and to whom complaints or inquiries can be forwarded;
- 8.3.2 The means of gaining access to personal information held by the Hospital;
- 8.3.3 A description of the type of personal information held by the Hospital, including a general account of its use;
- 8.3.4 A copy of any brochures or other information that explains the Hospital's policies, standards, or codes, and
- 8.3.5 What personal information is made available to related organizations.

8.4 The Hospitals will make information on their policies and practices available in a variety of ways to address varied information needs and to ensure accessibility to information: for example, the Hospital may choose to make brochures available in their places of business, mail information to their clients, post signs, provide online access, or through the Internet and Intranet.

9.0 Principle 9 - Individual Access to Own Personal Information

9.1 Upon request, an individual will be informed of the existence, use, and disclosure of his or her personal information and will be given access to that information. An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

9.2 ***Note:*** *In certain situations, the Hospital may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that*

contains references to other individuals, information that cannot be disclosed for legal, security, or proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

9.3 Upon request, the Hospital will inform an individual whether or not it holds personal information about the individual. The Hospital will seek to indicate the source of this information and will allow the individual access to this information. However, it may choose to make sensitive health information available through a medical practitioner. In addition, the Hospital will provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

9.4 An individual will be required to provide sufficient information to permit the Hospital to provide an account of the existence, use, and disclosure of personal information. The information provided will only be used for this purpose.

9.5 In providing an account of third parties to which it has disclosed personal information about an individual, the Hospital will attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the Hospital will provide a list of the organizations to which it may have disclosed information about the individual.

9.6 The Hospital will respond to an individual's request within a reasonable time and at a reasonable cost to the individual. Fees will be established on a cost recovery basis. The requested information will be provided or made available in a form that is generally understandable. For example, if the Hospital uses abbreviations or codes to record information, an explanation will be provided.

9.7 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the Hospital will amend the information as required, in accordance with professional standards of practice. Depending upon the nature of the information challenged, amendment may involve the correction, deletion, or addition of information. Information contained within health records will not be deleted, but rather, the original must be maintained, with any amendments or corrections being made in a transparent manner. Where appropriate, the amended information will be transmitted to third parties having access to the information in question.

9.8 When a challenge is not resolved to the satisfaction of the individual, the Hospital will record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

10.0 Principle 10 - Challenging Compliance with the Hospitals' Privacy Policies and Practices

10.1 An individual will be able to address a challenge concerning compliance with this policy to the Chief Executive Officer.

10.2 The Hospital will put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

10.3 The Hospital will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist.

10.4 The Hospital will investigate all complaints. If a complaint is found to be justified, the Hospital will take appropriate measures, including, if necessary, amending its policies and practices.

DEFINITIONS

Agent - a person who acts on behalf of the organization in exercising powers or performing duties with respect to personal/private information whether or not employed (or remunerated) including volunteers, students, physicians, consultants, nurses, vendors and contractors.

Patients – includes inpatients, outpatients, residents and clients.

Personal information - information about an identifiable individual, but does not include the name, title or business address or telephone number of a staff member of an organization.

Personal Health Information - personal information with respect to an individual, whether living or deceased and includes:

(a) information concerning the physical or mental health of the individual;

(b) information concerning any health service provided to the individual;

(c) information concerning the donation by the individual of any body part or any bodily substance of the individual;

(d) information derived from the testing or examination of a body part or bodily substance of the individual;

(e) information that is collected in the course of providing health services to the individual, or

(f) information that is collected incidentally to the provision of health services to the individual.

REFERENCES

Personal Information Protection and Electronic Documents Act, (PIPEDA) (2004)
Personal Health Information Protection Act (PHIPA) (2004)
Acceptable Use of Information Technology Resources Policy