Policy Title:	**Privacy Policy**	
Policy Author:	**Privacy Officer**	
Policy Owner (approver):	**VP Corporate Services & CFO**	
Original Effective Date: August 2004		**Reviewed/Revised Date: September 2024**
Policy Cadence: ☐**Yearly** ☒**Every 2 years**		
Key Words: *Privacy, potential breach, actual breach, legal obligation, accountability, consent, limited use, safeguards, compliance, Information Privacy Commissioner, IPC, containment, Privacy Officer*		

POLICY STATEMENT

St. Thomas Elgin General Hospital (STEGH) is deeply committed to safeguarding the privacy and confidentiality of personal health information (PHI) within its care. As a designated Health Information Custodian (HIC) under the Personal Health Information Protection Act (PHIPA), STEGH upholds the responsibility of managing patient PHI in strict accordance with PHIPA regulations, internal policies, and other pertinent privacy protocols.

Privacy rights under PHIPA are firmly granted to patients or their Substitute Decision Makers (SDMs). This comprehensive policy extends to all individuals affiliated with STEGH, encompassing employees, physicians, volunteers, students, consultants, vendors, and contractors.

Central to our approach are the following guiding principles:

1. Respect for Individual Privacy: Individuals possess the right to control the collection, use, disclosure, retention, and disposal of their personal health information, subject to specified exceptions.
2. Legal Obligation to Confidentiality: STEGH is legally bound to maintain the confidentiality of personal health information, with disclosure only permissible under law or with individual consent.
3. Legal Authorization for Data Handling: STEGH is lawfully authorized to collect, use, and disclose personal health information for healthcare provision, service delivery, administrative functions, and other specified purposes, with some disclosures mandated by law.

It is expected that any staff who comes into contact with personal health information of a patient as part of their work at STEGH (clinical or non-clinical) shall abide by this policy and PHIPA.

STEGH strives to be PHIPA compliant and is committed to a high standard of privacy for its information practices and has adopted the following National Standard of Canada Model Code for the Protection of Personal Health Information:

1. Accountability for Personal Health Information
2. Identifying Purposes for the Collection of Personal Health Information
3. Consent for the Collection, Use, and Disclosure of Personal Health Information
4. Limiting Collection
5. Limiting Use, Disclosure and Retention of Personal Health Information
6. Ensuring Accruacy of Personal Health Information
7. Ensuring Safeguards for Personal Health Information

8. Openness Regarding Policies and Practices related to Personal Health Information
9. Patient Access to Personal Health Information
10. Challenging Compliance with STEGH Privacy Policies and Practices

Failure to uphold privacy standards may result in disciplinary measures, including termination of employment/contract or loss of organizational affiliation.

PROCEDURE

1.0 Guiding Principles

1.1 Principle 1 - Accountability for Personal Health Information

1.1.1 The Privacy Officer's (PO) responsibility includes setting privacy and confidentiality standards and putting measures in place to make employees and affiliates aware of their privacy and confidentiality obligations.

1.1.2 STEGH as a health information custodian under PHIPA is responsible for protecting the privacy and security of personal health information in its custody and control and as such, it shall:

1.1.2.1 Implement policies and procedures to ensure the protection of personal health information

1.1.2.2 Educate staff regarding their responsibilities under STEGH privacy policies when collecting, using, disclosing, retaining and disposing patient personal health information.

1.1.3 Implement policies and procedures outlining the responsibility of the PO to:

1.1.3.1 Receive and respond to complaints

1.1.3.2 Receive and respond to inquiries and requests on privacy-related matters

1.1.3.3 Review the privacy policy, practices and processes on a regular basis

1.1.3.4 Investigate alleged privacy breaches to ensure remedial action is taken and reoccurrences are prevented

1.2 Principle 2 - Identifying Purposes for the Collection of Personal Health Information

1.2.1 STEGH informs the patient of the purposes for which PHI is collected.

1.2.2 STEGH collects PHI for the delivery of patient care, the administration of the health care system, research and education, quality assurance, fundraising, and legal and regulatory requirements.

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

1.3.1 STEGH will rely on implied consent from patients or their legally authorized representative for the collection, use and disclosure of personal health information if the purpose is for provision of health care and the other legal requirements are met

1.3.2 STEGH will obtain express consent to collect, use and disclose PHI when required. The manner in which STEGH seeks consent may vary depending on the circumstances and the type of information being collected, used or disclosed

1.3.3 STEGH will ensure that patients are aware that consent may be withdrawn at any time, but the withdrawal cannot be retroactive for information already disclosed. STEGH informs the patient of the implications of such withdrawal.

1.3.4 STEGH can collect, use and disclose PHI without consent where PHIPA specifically requires or authorizes it. (e.g. duty to report, serious risk of significant harm to self or others)

1.4 Principle 4 - Limiting Collection

1.4.1 The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization

1.4.2 Information is collected directly from the individual unless the law permits or requires collection from third parties

1.4.3 STEGH is authorized to collect personal health information from third parties without consent in order to examine, assess, observe or detain someone under the *Mental Health Act* and subject to relevant provisions of the *Criminal Code*.

1.5 Principle 5 – Limiting Use, Disclosure and Retention of Personal Health Information

1.5.1 STEGH will collect, use and disclose only the amount of personal health information required to meet the specific purpose or as otherwise authorized.

1.5.2 Disclosure from the STEGH Health Record can be directed to the Health Information Department for consideration and processing.

1.5.3 Personal health information will be retained in accordance with STEGH policy Records Retention and Destruction Policy and as required by law.

1.6 Principle 6 - Ensuring Accuracy of Personal Health Information

1.6.1 To the extent possible, STEGH will ensure patient personal health information is as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

1.6.2 A patient has the right to challenge the accuracy of their PHI and to request amendment or correction if they feel their PHI is inaccurate or incomplete.

1.6.3 Requests for correction for records of personal health information in the custody and control of STEGH will be directed to the Privacy Officer (PO) or delegate. The PO will review such requests and determine if a correction to the record will be made. The PO will respond to the requestor in accordance with PHIPA.

1.7 Principle 7 - Ensuring Safeguards for Personal Health Information

1.7.1 STEGH is responsible to put reasonable security measures in place to protect personal health information against such risks. Some of these risks include loss, theft, unauthorized access, copying, modification, use or disclosure or un-secure disposal, regardless of the format in which the personal health information is held and appropriate to the sensitivity of the information.

1.7.2 Staff are expected to be knowledgeable of and abide by this policy and other related privacy and security policies and practices and to obtain clarification of such policies and practices where necessary.

1.8 Principle 8 - Openness Regarding Policies and Practices related to Personal Health Information

1.8.1 Information about STEGH's policy and practices regarding the management of patient personal health information is available to the public on STEGH's external website.

1.9 Principle 9 – Patient Access to Personal Health Information

1.9.1 A patient has the right to request access to their personal health information under STEGH's custody and control. STEGH grants access to that PHI, except in limited situations outlined by PHIPA and is responsible to respond to a patient request within the timeline set by PHIPA.

1.9.2 STEGH establishes fees for access on a cost recovery basis which can be accessed on the hospital's website.

1.10 Principle 10 - Challenging Compliance with STEGH Privacy Policies and Practices

1.10.1 STEGH investigates all complaints and suspected breaches of privacy or confidentiality. When a complaint or suspected breach, if found to be justified, the organization takes appropriate measures, including if necessary, amending policies and practices and/or disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation with the organization.

1.10.2 An individual may raise a concern or complaint regarding compliance with the privacy law, this policy or STEGH privacy practices to the PO

2.0 Breach of Privacy

STEGH may become aware of a potential or actual privacy breach by:

a) Complaints from patients, employees, or affiliates, who believe PHI has been breached or compromised to the caregiver, leader or delegate, or the Privacy Officer

b) Notification from a representative of the Information Privacy Commissioner (IPC) to the Privacy Officer or delegate, requesting a response within a specified period of time following a patient complaint to the IPC.

c) An audit of the organization's electronic patient record system (EPR) or other systems containing PHI, giving the reason to believe that there may have been an inappropriate access to a patient's PHI

d) Reports from Health Information Custodians (HIC), private homes, businesses or individuals who are not health care providers, regarding a potential or actual breach to the Privacy Officer or delegate or their Leader or delegate

e) A secondary breach identified through the initial investigation of another breach

In accordance with guidelines provided by the Office of the Information and Privacy Commissioner of Ontario, St. Thomas Elgin General Hospital 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

2.1.1 Employees, and affiliates, upon learning of a potential or actual privacy breach must notify the Privacy Officer or delegate, their leader or delegate, or Administrator-on-Call immediately. If the leader or delegate, or Administrator-on-Call are first notified it will be their responsibility to contact the Privacy Officer or delegate as soon as possible.

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

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

- **a)** Chief Executive Officer
- **b)** Chief of Staff
- **c)** Security Manager
- **d)** Risk Manager
- **e)** Human Resources
- **f)** Communications Manager
- **g)** Information Technology, and/or the Local Registration Authority (LRA) (if immediate suspension of access is required to further contain breach)
- **h)** Police (if the breach may be reasonably be considered a threat to significant harm to the patient or third party)
- **i)** Others as deemed necessary

2.1.2.2 The Privacy Officer or delegate, Leader or delegate, or Administrator-on-Call will direct employees and affiliates to immediately contain the breach

2.1.2.3 Containing the breach may include:

- **a)** Determining whether the breach would allow unauthorized access to any other PHI and, if so, take any and all steps necessary to contain the breach e.g. Change passwords, or temporarily shut down system
- **b)** Suspending users' access to patient care systems or other hospital systems to prevent reoccurrence of the breach (only with the authority of both the employee's Leader or delegate, and Human Resources, or the CEO or delegate if Human Resources is unavailable)
- **c)** Notifying the employee(s) involved of the situation, indicating that an investigation is being conducted, and that the Privacy Officer or delegate will be monitoring their access

d) In the case of information that has been mailed or faxed to the wrong recipient, the Privacy Officer will work to retrieve the misdirected information, by ways such as:

i. Asking the recipient to place the information in a sealed envelope and place in a secure area for pickup, PO will arrange retrieval of the information

ii. Asking the recipient not to make any copies of the information and destroy in confidential manner

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

2.2.1 The Privacy Officer or delegate in collaboration with the affected Leader 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:

2.2.1.1 Auditing the electronic patient record (EPR)

2.2.1.2 Reviewing hard copy health records

2.2.1.3 Interviews with employees, Physicians, students, volunteers, or affiliates

2.2.1.4 Interviews with patient/SDM's

2.2.1.5 Reviewing each step in the handling, processing, and storage of the health record

2.2.2 Depending on the severity of the breach, the Privacy Officer or delegate in conjunction with the affected Leader or delegate and/or Risk Management may initiate a Breach Management Team to facilitate the investigation and management of the breach

2.2.2.1 The Breach Management Team will identify and mange risks associated with the breach, including risk related to:

2.2.2.1.1 Reputation of the organization

2.2.2.1.2 Patient trust

2.2.2.1.3 Media

2.2.2.1.4 Legal

2.2.3 Then collaborate on determining next steps/actions.

2.2.4 Outcomes for employee/affiliate:

2.2.4.1 On completion of the investigation, the \leader, in collaboration with Human Resources or Chief of Medical Staff (depending on whether the individual is an employee or affiliate) determines the most appropriate outcome for the employee/affiliate. Possible outcomes include one or more of the following:

2.2.4.1.1 Education

2.2.4.1.2 Verbal warning

2.2.4.1.3 Written warning

2.2.4.1.4 Suspension

2.2.4.1.5 Termination

2.2.4.2 Factors to consider when considering the outcome include:

2.2.4.2.1 History of work performance or any prior discipline (Note the time lapse between disciplinary infractions and the employee's tendency to respond favorably to discipline)

2.2.4.2.2 Years of service

2.2.4.2.3 Employee/affiliate's response to investigation

2.2.4.2.4 Whether the employee/affiliate understands the concept of privacy and confidentiality and understands the seriousness of the breach

2.3 Step 3: Notification

2.3.1 PATIENT NOTIFICATION

2.3.1.1 The Privacy Officer or delegate in collaboration with the affected Leader or delegate are legally required to notify:

2.3.1.1.1 A patient or patient's Substitute Decision Maker (SDM), if the patient's information has been lost, stolen, or accessed inappropriately

2.3.1.1.2 A patient/SDM as soon as possible and preferably within a two week timeframe upon completion of step 2

2.3.1.1.3 A patient/SDM if the lost PHI has been found, notification may be done verbally or in writing depending on several factors:

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

ii. Relationship with the patient i.e. If the physician or leader has an established clinical relationship with the patient, it may be appropriate to notify the patient in person

2.3.1.2 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.

2.3.2 SHARED EPR

2.3.2.1 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 PHI, through the EPR within the Thames Valley Hospital Planning Partnership (TVHPP) the Privacy Officer will IMMEDIATELY:

2.3.2.1.1 Notify **the Privacy Officer, or delegate, or the Administrator-on-Call of the organization(s) that are affected by the breach**

2.3.2.1.2 REGIONAL PRIVACY OFFICER CONTACT INFORMATION

Alexandra Hospital	519-485-1700
Listowel Memorial Hospital	519-291-3120
London Health Sciences Centre	519-685-8500
Middlesex Health Alliance	519-245-5295
South Huron Hospital Alliance	519-235-5176
Tillsonburg District Memorial Hospital	519-842-3611
Wingham and District Hospital	519-357-3210
Woodstock Hospital	519-421-4233

2.3.3 CLINICAL CONNECT

2.3.3.1 STEGH contributes to the integrated electronic health record (EHR) in south west Ontario (SWO), Regional Clinical Viewer, ClinicalConnect™ which is funded through eHealth Ontario. In the event actual or potential breach is identified as involving or potentially involving Clinical Connect the Privacy Officer will immediately notify Service Center Support at eHealth Ontario at 1-866-250-1554.

2.3.3.2 It is extremely important that you do not disclose any PHI and/or personal information to the eHealth Ontario Service Desk Agent when reporting a suspected or confirmed Privacy Breach

2.3.4 THE OFFICE OF THE INFORMATION PRIVACY COMMISSIONER FOR ONTARIO (IPC)

2.3.4.1 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 IPC of Ontario and work with the Commissioner's staff to ensure the organization has met its legal obligations under PHIPA.

2.4 Step 4: Managing the Risk of Future Breaches

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

2.4.2 These measures may include:

2.4.2.1 Changes to processes, policies, or procedures,

2.4.2.2 Additional education and training for employees and/or affiliates related to PHI and their accountabilities for confidentiality and the protection of patients' privacy rights,

2.4.2.3 Reviewing and enhancing the programs or department's security of PHI.

DEFINITIONS

Access

Under the Personal Health Information Protection act refers to the ability of patients or their substitute decision makers to examine or obtain personal health information about themselves.

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.

Amendments

Refer to the correction, deletion, or the addition of information in a document.

Confidentiality

The obligation upon an organization or person to protect information that has been entrusted to its care for a specific purpose and to ensure that information is only accessible to those authorized to have access (refers to the moral, ethical, professional and employment obligation).

Confidential information

May include, but not limited to:

1. Identifiable personal health information.
2. Identifiable information about staff or affiliates. Note – a staff/affiliate's business contact information is not confidential.
3. Information regarding the organization's business, which is not publicly disclosed by the organization that individuals may come across during the performance of their roles at the organization that is not generally known by the public. Examples of this would be:
   a. legal matters that involve the organization that are not public knowledge,
   b. financial information that would not be available in the organization's Annual Report
4. Information that is protected by written confidentiality restrictions in contracts with external organizations and individuals,
5. Information related to intellectual property held by the organization, for example, information directly included in patents or other intellectual property applications, prior to publication of those patents or applications in public format,

6. Information related to the organization's information technology security and access to systems, including:
    a. information leading to improper access to the organization's computing resources, both internal and external to the hospital network (e.g. "guest" access to systems, remote access credentials),
    b. information pertaining to negotiated product discounts with partner vendors that is considered confidential and proprietary to the vendor,
    c. hardware and software vendor names for products, which may be vulnerable to external access attacks, or products that are part of our security infrastructure.

Disclose/Disclosure

Under the Personal Health Information Protection Act, refers to release or making available of personal health information to another person, (other than patients or their substitute decision-makers) organization or health information custodian; it does not mean the use of the information.

Education

Includes activities related to teaching/learning, professional development instruction, and training, e.g., academic/scholarly/professional publication, presentations, poster displays, and the development and distribution of educational materials.

Express Consent

Can be given in writing, or verbally. Verbal consent must be documented.

Health Information Custodian

Means any person or organization who controls other people's personal health information as part of their role as:

1. A health care practitioner or operator of a group practice of health care practitioners,
2. A service provider who provides a community service under the Long-Term Care Act,
3. A community care access corporation under the Community Care Access Corporations Act,
4. A hospital under the Public Hospitals Act, a private hospital under the Private Hospitals Act, a psychiatric facility under the Mental Health Act, an institution under the Mental Hospitals Act or an independent health facility under the Independent Health Facilities Act,
5. An approved charitable home for the aged under the Charitable Institutions Act, a placement co-coordinator under the Charitable Institutions Act, a home or joint home under the Homes for the Aged and Rest Homes Act, a placement co-coordinator under the Homes for the Aged and Rest Homes Act, a nursing home under the Nursing Homes Act, a placement co-coordinator under the Nursing Homes Act or a care home under the Tenant Protection Act,
6. A pharmacy under the Drug and Pharmacies Regulation Act,
7. A laboratory or specimen collection centre under the Laboratory and Specimen Collection Centre Licensing Act,
8. An ambulance service under the Ambulance Act,

9. A home for special care under the Homes for Special Care Act, or
10. A centre, program or service for community health or mental health whose primary purpose is to provide health care,
11. An evaluator under the Health Care Consent Act or an assessor under the Substitute Decisions Act,
12. A medical officer of health or a board of health under the Health Protection and Promotion Act,
13. The Minister or Ministry of Health and Long-Term Care, and
14. Any other person described as a health information custodian under the regulations to the Act (PHIPA) with custody or control of personal health information as part of performing powers, duties or work.

Health record

Refers to the capture of personal health information (PHI) acquired or maintained within the organization, regardless of the medium, and is the property of the Health Information Custodian. The personal health information contained in the Health Record is owned by the patient and is considered confidential. For the purposes of this policy "records" will include an accurate legible copy of an original paper or other hard copy document which has been transferred into an archived medium such as microfilm, scanned digital image, or other electronic storage medium. When records are transferred into a verified copy, these shall be retained as the 'original' record.

Identifying information

Refers to information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

Implied Consent

Permits you to conclude from surrounding circumstances that a patient would reasonably agree to the collection, use or disclosure of the patient's personal health information.

Knowledgeable Consent

As it relates to this policy, consent is knowledgeable if the person receiving the following information understands;

1. Why the information/sample/belongings are being requested by The law enforcement agency,
2. The expected benefits of the release,
3. The implications of the release, e.g., that it could be used against him or her,
4. The likely consequences of not releasing, e.g., that a warrant could be issued and the information/sample/belongings would have to be released,
5. The person received responses to his/her inquiries.

Law Enforcement Agency

For the purpose of this policy includes Ontario Provincial Police (OPP), Royal Canadian Mounted Police (RCMP), Canadian Military Services, and other municipal Police Services.

Leader

For the purposes of this policy, a Leader may be one or more of the following:

i. Chief Executive Officer
ii. Chief of the Medical Staff
iii. Department Chief

iv. Director, Manager, or delegate

Local Registration Authority (LRA)

Designated individual who has special privileges and responsibilities regarding granting access to and managing EPR accounts and applications (e.g. PowerChart, InfoMed, etc.), security and other related administrative matters.

Medium

Medium of the organization's health records includes verbal, written, electronic, visual, microfilm, diagnostic images, sound recordings, etc.

Patients

Refer to persons registered at the organization as inpatients and/or ambulatory (outpatient/emergency).

Patient identifying information

Information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify any individual. Patients do not have to be named for information to be considered identifying. Information is identifying if an individual can be recognized using it, or when it can be combined with other information to identify an individual. Anonymous or de-identified personal health information cannot be linked back to the individual either directly or indirectly.

Patient/Substitute Decision Maker or Patient/SDM

Refers to the patient (if the patient is capable with respect to the collection, use and disclosure of his or her personal health information) or the patient's Substitute Decision Maker (SDM) (if the patient is incapable with respect to the collection, use and disclosure of his or her personal health information).

Personal Health Information

The *Personal Health Information Protection Act, 2004* ("PHIPA") defines "Personal Health Information" as:
Oral or recorded identifying information about someone that relates to:

a) An individual's physical or mental health, or family health history, or
b) Health care an individual receives, including who provided the health care, or
c) A plan of service for an individual under the Long-Term Care Act, or
d) An individual's eligibility for health care payments or the payments made for an individual's health care, or
e) An individual's donation of any body part or bodily substance or anything derived from testing or examining a donated body part or bodily substance

Personal Health Information also includes:

a) An individual's health number
b) Anything that identifies an individual's substitute decision-maker,
c) Anything that identifies an individual and that is contained in a personal health record

Personal health information **does not** include records maintained for human resources purposes.

Personal information

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

Privacy Breach (Actual)

includes but is not limited to:

a) Accessing patient PHI when it is not required to provide or maintain care to a patient or in the performance of duties, for example:
   1. Directly accessing the health record of one self without following Health record Services procedure
   2. Accessing the health record of an employee, family member, friend, or anyone for whom you do not have a requirement to view information based on providing care or performing duties
   3. Accessing any patient information (e.g. address, date of birth, next of kin, etc.) of an employee, family member, friend, or anyone for whom you do not have a requirement to view information based on providing health care or performing duties

b) Discussing patient information with:
   4. Another person who is not involved in the direct care of the patient or does not require the information to perform their job function, or
   5. Within range of other people in a non-patient care area of the hospital (e.g. 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:
   6. Loss of a health record or identifiable patient information
   7. Faxing or emailing PHI to the wrong recipient,
   8. Theft of electronic device containing identifiable patient information

Privacy Breach (Potential)

Occurs when an individual's PHI is at high risk of being accessed, used, or disclosed inappropriately by or to individuals or for the purposes other than consented to by the patient. A potential privacy breach includes, but is not limited to:

i. Allegations of a privacy breach by a patient or employee/affiliate
ii. Concerns related to security of PHI raised by a patient or employee/affiliate
iii. Request by a patient for additional security around their PHI (e.g. Lockbox)
iv. Leaving patient information in unattended or unsecured locations where it may be accessed by unauthorized persons
v. Leaving access to electronic patient information unattended on an open log in, or storing electronic patient identifiable information on portable information devices or unsecure drives (e.g. hard drives that have not been encrypted)

Professional Standards

An authoritative statement that sets out the legal and professional basis of practice. Professional Standards provide an overall framework for practice. Examples of health care providers with professional standards are: College of Nurses of Ontario, the Ontario College of Social Workers and Social Service Workers and the College of Physicians and Surgeons of Ontario.

Quality Assurance	Refers to activities that involve the use of personal health information to improve or maintain the quality of care, or to improve or maintain the quality of any related programs or services of the hospital.
Record	Refers to an information record in any form or media, including written, printed, photographic or electronic form, but excluding computer programs and other mechanisms that produce a record.
Secure area/location	Refers to a locked filing cabinet or password-protected electronic storage to prevent accidental loss or unauthorized viewing of images and video recordings.
Staff Members	For the purposes of this policy refer to individuals who are employed and paid by the hospital.
Storage location	Storage location of the organization's health record includes Health Information and other departments e.g., Radiology. Electronic Patient Records are stored on the STEGH server and are accessible internally.
Substitute Decision Maker (SDM)	With respect to correction requests, refer to individuals who act on behalf of a patient, whether that patient is incapable or capable. An SDM is defined as a person who is: a) At least 16 years of age, unless he or she is the incapable patient's parent, b) Capable with respect to the treatment, c) 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, d) Available, and e) Willing to assume the responsibility of giving or refusing consent. In descending order of priority, a patient's SDM may be: a) The 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, b) The 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 c) The patient's "representative" appointed by the Consent and Capacity Board, if the representative has authority to give or refuse consent to the treatment d) The patient's spouse or partner e) Child or parent (custodial) of the 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 f) A parent (who has only a right of access) of the patient g) A brother or sister of the patient
Third party	Vendors or other individuals or agencies that do not have an employment, educational, privilege association with the organization.

Third Party Information	In relation to a patient's health record, means personal information about an identifiable individual or individuals, other than the patient.

REFERENCES

Related Corporate Policies:
Access or Disclosure of Personal Health Information
Anonymous Patient Policy
Confidentiality Policy
Freedom of Information and Protection of Privacy Policy (FIPPA)
Restrict Use or Disclosure of Personal Health Information (Lockbox) Policy
Patient Requests to Amend Personal Health Information Policy
Use of PHI for Research, Education and Quality Assurance Policy
Acceptable Use of Information Technology Resources Policy
Bring Your Own Device Policy
Information Security Policy
Password Policy
Remote Access Policy
System Access Policy

Legislation:
Personal Health Information Protection Act (PHIPA), 2004
Public Hospitals Act
Mental Health Act
Criminal Code
Health Care Consent Act
Personal Information Protection and Electronic Documents Act (PIPEDA), 2000
Regulated Health Professionals Act

Standards:
College of Nurses of Ontario, Standards of Practice – Confidentiality
College of Physicians and Surgeons of Ontario – Confidentiality and Access to Patient Information

Others:
The Guide to the Ontario Personal Health Information Protection Act
Thames Valley Hospital Planning Partnership (TVHPP) Memorandum of Understanding, Privacy and Security Schedule