	☒ Policy ☐ Procedure ☐ Protocol ☐ Terms of Reference	Section Privacy	Number 19-001
Privacy			
Date Issued: Dec. 2004 **Date Review/Revised: Dec. 2006, Apr. 2010, Aug. 2013, Sept. 2017** **Next Review Date: Sept. 2020**			
Owner: Chief Financial Officer	**Reviewer(s):** Privacy Officer		**Approver:** Chief Financial Officer
Cross Reference:			

This is a CONTROLLED document for internal use only. Any documents appearing in paper form are not controlled and should be checked against the document (titled as above) on the file server prior to use.

Purpose

South Huron Hospital Association (SHHA; the Hospital) has implemented a number of shared services, including some consolidated clinical services, common medical staff, laboratory services and integrated information systems. To the extend that personal information is collected, used, disclosed, and retained within the shared services, the Hospital recognizes that each organization has both independent and joint obligations with respect to fair information practices.

The privacy policy is the foundation for other policies and procedures, setting the principles upon which the Hospital will collect, use and disclose personal information and personal health information (PHI).

Policy

The Hospital is responsible to comply with the Personal Health Information Protection Act (PHIPA, 2004). SHHA, as the Health Information Custodian (HIC), is therefore responsible for PHI under its custody and control and is committed to a high standard of privacy for information practices. The Hospital adopts the following 10 Principles set out in the National Standard of Canada Model Code for the Protection of Personal Information.

1. Accountability for Personal Information
2. Identifying Purposes for the Collection of Personal Information
3. Consent for the Collection, Use, and Disclosure of Personal Information
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention of Personal Information
6. Ensuring Accuracy of Personal Information
7. Ensuring Safeguards for Personal Information
8. Openness about Personal Information Policies and Practices
9. Individual Access to Own Personal Information
10. Challenging Compliance with the Hospital's Privacy Policies and Practices

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

Principle 1 – Accountability for Personal Information

The Hospital is responsible for PHI under its control and has a designated individual (Privacy Officer) to set privacy and confidentiality standards, as well put measures in place to make employees and affiliates aware of their privacy and confidentiality obligations.

- Accountability for the Hospital's compliance with the policy rests with the Chief Executive Officer, Leader of Health Information and Privacy, and the Privacy Officer of the organization. In the circumstance of a privacy breach, Human Resources where applicable.
- The name of the Privacy Officer designated by the Hospital to oversee compliance with these principles is a matter of public record.
- The Hospital is responsible for PHI 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.
- The Hospital will:
    - Implement policies and procedures to protect PHI, including information relating to patients, staff and agents.
    - Establish policies and procedures to receive and respond to complaints and inquiries.
    - Train and communicate to staff and agents information about the Hospital's privacy policies and practices.
    - Mandatory annual Privacy Training for staff
    - Develop plans and communicate to the public and key hospital stakeholders' information to explain the Hospital's privacy policies and procedures.

Principle 2 – Identifying Purposes for the Collection of Personal Information

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

A patient has the right to consent, refuse, or place restrictions on the collection, use an disclosure of PHI.

The Hospital meets these requirements by the following policies and processes:

- Policy #19-019 Access to Personal Health Information for Patient/SDM.
- Policy #19-003 Access to Personal Health Information for Research, Education and Quality Assurance.
- Posted notices and brochures inform patients/SDMs about purposes for the collection, use and disclosure of their PHI.
- Information on the Hospital website.

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

The knowledge and consent of the individual is required for the collection, use, or disclosure of PHI, except where inappropriate. PHI can be collected, used or disclosed without knowledge and consent of patient/SDM only where permitted or required by law.

A patient/SDM may withdraw or restrict 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.

The Hospital meets these requirements by the following policies and processes:

- Policy #19-019 Access to Personal Health Information for Patient/SDM.
- Policy #19-003 Access to Personal Health Information for Research, Education and Quality Assurance.
- Policy #19-004 Anonymous Patient Policy.
- Policy #19-008 Management of Requests to Restrict Collection, Use and Disclosure of Personal Health Information.

The form of the consent sought by the Hospital may vary, depending upon the the purpose of collection, use and/or disclosure.

Principle 4 and Principle 5 – Limiting Collection, Use, Disclosure and Retention of Personal Information

The collection of PHI will be limited to that identified to the patient/SDM and for which consent was obtained, except with the consent of the patient/SDM or as required by law.

PHI will be retained only as long as necessary for the fulfillment of the above purposes.

Principle 6 – Ensuring Accuracy of Personal Information

PHI will be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. A patient/SDM has the right to request correction if they feel their PHI is inaccurate or incomplete.

SHHA meets these requirements by the following policies and processes:

- Policy #19-007 Request to Amend Personal Health Information.

Principle 7 – Ensuring Safeguards for Personal Information

The Hospital is responsible for ensuring reasonable security measures are in place to protect PHI against risks of loss, theft, unauthorized access, use or disclosure, or unsecure disposal in any format which it is held.

SHHA meets these requirements by the following policies and processes:

- Policy #19-011 Auditing of the Electronic Patient Record (EPR).
- Policy #19-016 Confidential Faxing Policy.
- Policy #19-015 Confidential Waste Policy.
- Policy #19-009 Information Security Policy.
- Policy #19-012 Privacy Breach Policy and Procedure.
- Policy #18-008 Retention of Patient Records.

Principle 8 – Openness about Personal Information Policies and Practices

The Hospital will make readily available to individuals specific information about their policies and practices relating to the management of PHI. Information Includes:

- Contact information posted of Privacy Officer including private e-mail and extension number.
- Patient Directory explaining how to access information.

- Posted notices informing patients/SDM of the purpose for the collection, use and disclosure of their PHI.

The Hospital is responsible for patient notification in the event their PHI has been lost, stolen, accessed or disposed in an un-secure manner.

- Policy #18-011 Loss of Patient Information
- Policy #19-012 Privacy Breach Policy and Procedure

Principle 9 – Individual Access to Own Personal Information

A Patient/SDM has the right to request access to their PHI and will be given access to that information except in limited situations outlined by PHIPA. SHHA is responsible to respond to the patient's/SDM's request within the timeline set by PHIPPA. The Hospital has determined fees for access as determined in partnership with their regional partners.

- Policy #19-019 Access to Personal Health Information for Patient/SDM.

Principle 10 – Challenging Compliance with the Hospital's Privacy Policies and Practices

A patient/SDM has the right to challenge the Hospital concerning compliance with PHIPPA and this policy. Preventive measures are in place to ensure compliance of privacy practices.(i.e., routine audit of electronic health record, confidentiality agreements by staff and affiliates and mandatory privacy training of staff).

- The Privacy Officer, and where appropriate the Director of Human Resources, will investigate all complaints, suspected breaches or privacy concerns. If a complaint is found to be justified, the Hospital will take appropriate measures, including, if necessary, amending their policies and practices, and/or termination of employment or affiliation with the organization.

References

Personal Health Information Protection Act, 2004.
Freedom of Information Act (need to add the date)