Category:	Privacy	**Policy Number:**	SHN-ADMIN-PY-001
Subject:	**Privacy of Personal Health Information**	**Date:**	2017/06
Issued By:	Chief Privacy Officer	**Revision Date (s):**	
Approved By:	Senior Leadership Team	**Page**	**Page 1 of 9**
Rescinded Policies:			

PURPOSE

Scarborough Health Network (SHN) is committed to providing patients and families with a positive patient experience. Our hospital respects privacy as a fundamental patient right and recognizes that personal health information (PHI) belongs to the patient and that the hospital is its custodian. We are committed to protecting the PHI that we create or obtain about our patients. The *Personal Health Information Protection Act* (PHIPA) sets out rules that health information custodians must follow when collecting, using, disclosing, retaining and disposing of personal health information. This policy outlines what is required for our hospital and its agents, to comply with PHIPA.

POLICY STATEMENT

The *Personal Health Information Protection Act* (PHIPA) sets out rules that health information custodians must follow when collecting, using, disclosing, retaining and disposing of personal health information. These rules apply to all health information custodians operating within the province of Ontario, including SHN, and to individuals and organizations that receive personal health information from health information custodians.

With limited exceptions, the legislation requires health information custodians to obtain consent before they collect, use or disclose personal health information. In addition, patients have the right to request access or correction of their own personal health information.

SHN recognizes that personal health information is one of the most sensitive types of information for an individual and as such takes the protection of such information seriously by implementing safeguards to ensure risk of inappropriate access or disclosure is reduced significantly. This policy applies to every person who works with PHI including, but not limited to directors, employees, volunteers, students, affiliates, privileged staff (physicians, dentists, midwives), researchers, contractors, sub-contractors and other agents. From here on, these individuals are referred to as “SHN staff”.

DEFINITIONS

Agent: A person who is authorized by the hospital to collect, use or disclose personal health information.

Health Information Custodian (HIC): Persons or organizations described in PHIPA who have custody or control of personal health information as a result of the work they do. For example, Scarborough Health Network is a health information custodian.

Identifying information: Information that identifies an individual, either alone or with other information.

Personal Health Information (PHI): Identifying information about an individual (living or deceased) in oral or recorded form as it relates to, but not limited to:

- Physical or mental health
- Provision of health care
- Plan of service
- Payment or eligibility for health care
- Donation of body parts or bodily substances
- Health card number or medical record number
- Substitute decision maker

Personal Health Information Protection Act (PHIPA): An Ontario health privacy law that establishes rules for the management of PHI and protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services.

Personal Information: Recorded information about an identifiable individual including information relating to the name, address, telephone number, age, race, national or ethnic origin, colour, religion, sex, sexual orientation, marital or family status of the individual. This policy does not apply to personal information (PI) not related to a person's health. Personal information that is not PHI is protected under the *Freedom of Information and Protection of Privacy Act (FIPPA).* FIPPA is an Act that legislates access to information held by public institutions. FIPPA allows individuals to access information under the control of institutions and to protect the privacy of individuals with respect to personal information about themselves in the custody or the control of the institution.

Policy Breach: Includes any non-compliance with this policy, other privacy-related policies, procedures and protocols, or with PHIPA.

Privacy Breach: A privacy breach occurs whenever a person has contravened a provision of PHIPA or its regulations. A breach occurs when information is stolen, lost or inappropriately accessed, used or disclosed without patient consent.

PROCEDURE

Section 12(1) of PHIPA requires health information custodians to take steps that are reasonable to ensure personal health information in their custody or control is protected against theft, loss and unauthorized access, use, disclosure, copying, modification or disposal.

Collection and Use of Personal Health Information

When practical, patient data is to be collected directly from the patient/Substitute Decision Maker (SDM) with consent. If necessary with the consent of the patient/SDM, data can be collected from secondary sources such as relatives or friends, as appropriate.

To the extent practical, patient data will be collected, used and/or disclosed only for purposes that have been identified to the patient at, or before, the time of patient registration.

Legitimate purposes include but may not be limited to the following:

- Patient care;
- Maintaining complete and accurate records of healthcare services (including psychosocial, spiritual and physical) at SHN;
- Compliance with laws, government regulations, legitimate law enforcement, forensic and public health requests;
- Population-based healthcare research;
- Education of health professionals;
- Improving and assuring the quality of clinical care;
- Improving the efficiency of service administration, management and delivery;
- Billing and making expense claims to government agencies and other SHN-approved billable agencies (such as private insurers) for services rendered;
- Supplying information to recognized Canadian institutions of health information; management, such as the Canadian Institute of Health Information (CIHI) and/or
- Fundraising for the SHN Foundation.

PHIPA requires that health information custodians not collect, use or disclose more personal health information than is reasonably necessary to satisfy the purpose.

All media containing patient data (e.g., medical records, films, ECG strips, patient wrist bands, disks, computers, whiteboards, mail, labels, computer screens, requisitions, forms, reports) must be carefully positioned, packaged, stored, encrypted, transported and/or disposed of to prevent unauthorized viewing or other access.

Authorized access is limited to only the required patient information. Each user is responsible for maintaining the confidentiality of any assigned passwords and for ensuring that no other person knows his or her assigned passwords.

Disclosure of Personal Health Information

SHN uses and shares information with others for the purposes of providing care or for permissible use under the law. This includes disclosure to the patient's care providers, for example the patient's family doctor, to ensure continuity and coordination of care.

The patient can instruct us if he or she does not want his/her physician or care provider to be notified or provided information about the patient's hospital visit.

There are some situations in which PHI may be disclosed by the Hospital without consent, either because it is required for the provision of care and/or permitted by law.

For example PHI may be disclosed by the Hospital without consent for the following reasons:

- To care providers within the circle of care to improve/maintain the quality of the patient's care and of those provided similar care
- Use for quality improvement and risk management purposes as defined by the Act
- When responding to a request from the College of Physicians and Surgeons or to a request from Workers Safety and Insurance Board
- In compliance with a court order, through the execution of a search warrant.
- In compliance with a duly authorized request from the coroner's office.
- When fulfilling the duty to report suspected child abuse or gunshot wounds to police
- To the patient or the patient's legal guardian or substitute decision-maker upon request
- To Registries and entities prescribed in PHIPA
- To Ministry of Health and Long-Term Care
- To researchers if the research has been approved by the SHN Research Ethics Board
- To the Medical Officer of Health to report communicable diseases

If the third party to which patient data are disclosed is not a recognized health information custodian (e.g. a health professional, a healthcare organization, Ontario Health Insurance Plan (OHIP), CIHI), etc., then before patient data is disclosed, the third party must sign an agreement with SHN to hold the patient data in confidence, and use it only for the agreed upon purpose.

Faxing of Confidential Patient Personal Health Information:

Caution must be exercised whenever personal health information is to be faxed. The destination fax number should be double checked for accuracy. Whenever practical the recipient should be notified ahead of time when the fax is being sent. The appropriate SHN fax cover sheet should be used.

Retention and Storage of Personal Health Information

SHN must ensure that, during the retention period of records, patient data remains usable and unaltered, This may require storing records in a controlled environment and may require transferring records to fresh and/or different media from time to time. Such transfers will be done only after confidentiality is assured. The Hospital's Retention and Disposal Policy will be followed for retention and safe destruction of personal health information.

Education and Awareness

SHN will provide programs to educate and inform SHN staff of the importance of maintaining the confidentiality of PHI, and their respective responsibilities.

Prior to the start of employment, the granting of hospital privileges or entering into any direct affiliation with the hospital, and on an annual basis thereafter, SHN staff are required to:

- Review SHN's privacy policy and procedures.
- Sign the Statement of Confidentiality (Appendix A)
- Participate in mandatory privacy training

On a quarterly basis, each Vice President will be provided with a list of SHN staff who are non-compliant with privacy requirements (policy review, statement of confidentiality sign off and privacy training) for follow up.

Privacy Incident Management

It is prohibited and against the law to access patient data unless such access is required to perform duties assigned or sanctioned by SHN. Anyone found accessing patient data outside these parameters has committed a serious breach of privacy, and will be subject to disciplinary action. SHN staff are also required to follow the correct procedure for accessing their own record by completing an access request through the Health Records/ Health Information Management department.

SHN will ensure compliance with privacy policies and procedures through targeted and random audits of SHN information practices and internal systems.

SHN promotes transparency and encourages staff to report privacy and data protection concerns, including suspected breaches of PHI and privacy policies and procedures to the Privacy Office, in confidence, and assures that measures will be taken to ensure reporting personnel suffer no reprisals when suspected breaches are reported in good faith.

All suspected privacy incidents will be managed as per SHN's privacy breach protocol.

Disciplinary Action

Any person who breaches this policy is subject to disciplinary actions including suspension/deactivation of access to PHI and/or internal systems, termination of employment, contract termination or termination of hospital privileges and a report to their respective regulatory college, if applicable.

Role of the Privacy Office

The Chief Privacy Officer (CPO) is accountable for privacy policies and PHIPA at SHN. The SHN Privacy Office will strive to ensure that privacy, confidentiality and security measures are incorporated into the design and delivery of programs, services, agreements and technology initiatives to achieve compliance with information practices and legislation.

Inquiries/ Compliance with SHN's Privacy Policies and Practice:

The CPO is the initial point of contact for complaints and inquiries related to compliance with PHIPA at SHN. If any individual has a question, concern or complaint about SHN's compliance with privacy obligations under PHIPA, he or she can contact the SHN's Privacy Office by phone at 416-284-8131 x4302, or email at privacy@rougevalley.ca, or write to

Scarborough Health Network,
2867 Ellesmere Road,
Toronto ON M1E 4B9,
Attention: Privacy Office, Mailbox 10.

Inquiries and complaints may also be made to the Information and Privacy Commissioner of Ontario. The Commissioner is located at

2 Bloor Street East, Suite 1400,
Toronto ON M4W 1A8.
Telephone: (416) 326-3333 or toll-free at 1 800 387-0073.
Website: www.ipc.on.ca.

REFERENCES

- Personal Health Information Protection Act, 2004
- Health Information Protection Act, 2016
- 10 Fair Information Principles of the Canadian Standards Association Model Code for the Protection of Personal Information, 1994.
- Privacy and Security Working Group, Harmonized Privacy Protection Policies (Version 10). Connecting GTA, May 2012
- Hospital Privacy Toolkit, Guide to the Ontario Personal Health Information Protection Act, September 2004
- A Guide to the Personal Health Information Protection Act, Information and Privacy Commissioner of Ontario, December 2004
- Privacy Incident Protocol, Women's College Hospital (2015)

REVIEWED BY

SHN Vice President, Performance, Strategy and Innovation (2017/06)
SHN Chief Privacy Officer (2017/06)
SHN Information Technology (2017/06)
SHN Information Management (2017/06)
Legal Counsel (2017/06)
HIROC (2017/06)

APPROVED BY

Senior Management Team (2017/06)

STATEMENT OF CONFIDENTIALITY

1. I understand that during my association with SHN I may have access to information and material relating to patients, credentialed staff, other hospital personnel or other confidential information. At all times, this information will not be accessed, used or disclosed for purposes other than for which the information is intended and for which I am authorized.

2. All reasonable measures will be taken by me to ensure that sensitive information (personal, patient and corporate) is collected, used and disclosed only in circumstances necessary by law and authorized for patient care, research, or education, or as necessary in the conduct of the business of SHN and in compliance with the *Personal Health Information Protection Act, 2004.*

3. I shall not remove confidential information from SHN premises except when it is necessary for me to do so for a legitimate purpose related to my association with SHN. I shall not remove patient records or other personal health information from the SHN premises unless I am authorized to do so by the Chief Privacy Officer or his or her delegate. If I am required to remove information from SHN premises, I will take all necessary measures to safeguard this information.

4. I understand that my information system user ID is equivalent to my signature, and will take all reasonable steps necessary to safeguard my password from disclosure to others. If I have any reason to believe that the security of my user name and/or password is at risk or has been compromised, I will immediately notify my supervisor and contact the Information Services department for reassignment of a new password.

5. I understand that the use of my information system access will be strictly limited to accessing information on a need-to-know basis for direct patient care or performance of one's duties. I will not attempt to access any unauthorized information including information about myself, my family, friends, colleagues, neighbours or any other person whose information is not required to perform my work duties.

6. I understand and agree that in order to deter the unauthorized access, use or disclosure of personal health information in the Hospital's electronic information systems, SHN will conduct audits to ensure compliance with privacy practices and policies on the use of my information systems access. I understand and agree that I will be accountable for access to any records where I do not have a need to know.

7. If I believe that there may have been a breach of confidentiality, if I have committed a breach of confidentiality or if I believe there may have been a breach of SHN's privacy policies or procedures, I agree to notify the Hospital's Privacy Office at (416) 284-8131 x 4302 or privacy@rougevalley.ca and my supervisor at my first reasonable opportunity.

8. I understand that a breach of confidentiality includes, but is not limited to, accessing personal health information without authorization to do so. Confirmed breaches may result in any or all of the following:

- Deactivation of my information systems access,
- Discipline including termination of employment, hospital privileges, hospital association or contractual relationship
- A report to my regulatory college where applicable
- A report to the Information and Privacy Commissioner where applicable
    - I understand that the Information and Privacy Commissioner of Ontario may investigate violations and has the authority to fine individuals $100,000 and corporations $500,000 for any violations of the privacy legislation in effect in Ontario.

9. I understand and agree to abide by this agreement, and I understand that this Agreement remains in force, even if I cease to have an association with SHN.

10. I have had the opportunity to review this Agreement and any questions I may have were answered to my satisfaction. I understand that if at any time I have questions about this Agreement or about my duties regarding privacy and confidentiality, I am to speak to my immediate supervisor or the Privacy Office.

I, _____, agree that I have read and will observe and comply with the Scarborough Health Network (SHN) privacy policy, procedures and Statement of Confidentiality.

_____ _____

Signature Date (dd/mm/yyyy)