

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 1 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

PURPOSE

This policy outlines what Scarborough Health Network (SHN) and its agents must comply with under the Personal Health Information Protection Act (PHIPA).

POLICY STATEMENT

SHN is committed to providing patients and families with a positive patient experience. PHIPA sets out rules that health information custodians must follow when collecting, using, disclosing, retaining and disposing personal health information (PHI). These rules apply to all health information custodians operating within the province of Ontario, including SHN, and to individuals and organizations that receive PHI from health information custodians.

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

SHN recognizes that PHI 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 the risk of inappropriate access or disclosure is reduced significantly. Our hospital respects privacy as a fundamental patient right and recognizes that 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. 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 whom the hospital authorizes to collect, use or disclose PHI.

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

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

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 2 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

Personal Health Information (PHI): Identifying information about an individual (living or deceased) in oral or recorded form as it relates to, but is 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, and marital or family status of the individual. This policy does not apply to personal information (PI) unrelated 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.

Substitute decision-maker: A substitute decision-maker is a person authorized to give or refuse consent to a treatment on behalf of a person who is incapable with respect to treatment.

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 3 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

PROCEDURE

1.0 Accountability

SHN is a health information custodian responsible for collecting, using and disclosing PHI in its custody or control. SHN is obliged to have information practices in place that comply with PHIPA. SHN has designated a Chief Privacy Officer (CPO) as the contact person accountable for SHN's compliance with this Policy.

1.1 Accountability: Even though accountability for SHN's compliance with this policy and with PHIPA rests with the CPO, other individuals within SHN may be responsible for the day-to-day collection and processing of personal information. Every agent acting for, on behalf of, or for the benefit of SHN must comply with this Policy.

1.2 Responsibilities: The CPO is an agent of SHN and is authorized on behalf of the hospital to:

- a) facilitate the hospital's compliance with this policy and with PHIPA generally;
- b) ensure that all agents of the hospital are appropriately informed of their duties under this policy and with PHIPA generally;
- c) respond to inquiries from the public about the hospital's information practices;
- d) respond to requests of an individual for access to or correction of a record of PHI about the individual that is in custody or under the control of the hospital; and
- e) receive and respond to complaints from the public about the hospital's alleged contravention of this policy and with PHIPA generally or its regulations.

1.3 Public Record of Contact Person: The identity of the CPO and the individual(s) designated by SHN to oversee compliance with this policy and with PHIPA generally will be made known as a matter of public record in a written statement as detailed below. The CPO can be contacted via telephone at 416-284-8131 ext. 7782, via email at privacy@shn.ca, or by writing to Attention Privacy Contact Person, 3030 Birchmount Road, Scarborough, ON M1W 3W3.

1.4 Openness: SHN will be open about its information practices concerning the management of PHI. Individuals can acquire information about SHN policies and procedures without unreasonable effort. This information will be made available in a generally understandable form.

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 4 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

1.5 Description of Information Practices: A written statement will be made available to the public that:

- a. provides a general description of SHN's information practices
- b. describes how to contact the contact person
- c. describes how an individual may obtain access to or request correction of a record of PHI about the individual that is in the custody or control of the custodian; and
- d. describes how to make a complaint to SHN and the Information Privacy Commissioner.

1.6 Third Party Confidentiality Contracts: SHN is responsible for PHI in its custody or control, including information that has been disclosed under contract and will use contractual or other means to ensure a comparable level of privacy protection while the information is being used or otherwise processed by any third party including, where appropriate, agents of the hospital.

1.7 Duration of Custodial Duty: SHN does not cease to be a health information custodian with respect to a record of PHI until complete custody and control of the whole record passes to another health information custodian.

2.0 Identifying Purposes for the Collection of Personal Information

SHN will identify the purposes for which personal information is collected at or before the time the information is collected. PHI will not be used for purposes other than those for which it was collected, except with the individual's express consent or as permitted or authorized by law.

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

- To treat and care for our patients, both inside and outside of the hospital;
- To communicate or consult patient's health care with their doctor(s) and other health care providers;
- To receive payment for patient's health care and hospital services, including from OHIP and private insurance;
- To plan, administer and manage our internal operations;
- To compile statistics;
- To conduct risk management or quality improvement activities;
- To conduct research as approved by the Research Ethics Board;
- To conduct patient surveys;
- To notify patients of an appointment or change an appointment;
- To confirm a patient, their general health status, their room and telephone extension while in hospital;
- To locate a patient or their family in urgent situations using an overhead paging system;
- To fundraise to improve patients' health care facilities, services and programs;
- To report as required or permitted by law;

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 5 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

- To share with prescribed persons/entities who compile or maintain a registry of PHI for purposes of facilitating or improving health care; and/or
- To maintain complete and accurate records of health care services.

2.2 Identification of New Purposes Prior to Use: When personal information collected is to be used for a purpose not previously identified to the individual, the new purpose will be generally identified before use. Unless the new purpose is otherwise permitted or authorized by law, the individual's consent will generally be obtained before their information can be used for the new purpose. In circumstances where obtaining prior consent is impractical, the individual may be notified at the first reasonable opportunity, except as permitted or required by law, and a note of the new use or disclosure will be kept in the record.

2.3 Clarity: Upon request, SHN agents will be able to explain to individuals the purposes for which the information is being collected. This information may be provided in writing and/or orally (depending on the circumstances) in a language known to the patient or substitute decision maker.

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

The knowledge and consent of the individual, or person authorized to consent on behalf of the individual, are generally required for the collection, use or disclosure of PHI, except where otherwise required by law. Generally, consent may be expressed or implied.

For more information regarding patient consent, ***please refer to policies on Consent to Treatment and Access, Disclosure and Correction of Personal Health Information.*** These policies should be consulted for specific instances of SHN obligations regarding the obtaining of patient consent for the use or disclosure of their personal information during and after the regular course of patient care. Below are some key considerations with regard to consent.

3.1 Direct vs. Indirect Collection of PHI: SHN will endeavour to collect all PHI from the individual directly except as otherwise consented to by the individual, or as permitted or required by law. Where the information to be collected is necessary for providing patient care and it is not reasonably possible to collect directly from the individual in an accurate or timely fashion, SHN will collect the information from another person or entity permitted to disclose the information.

3.2 Consent of the Individual: An individual who is assumed capable of giving consent to the collection, use or disclosure of PHI may provide consent or authorize a person to act on their behalf. SHN generally presumes that an individual is capable of consenting to the collection, use or disclosure of PHI unless it has reasonable grounds to believe otherwise. Capable individuals may give, withhold or

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 6 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

withdraw consent. A substitute decision maker or another authorized individual may provide consent on behalf of the patient, as permitted by law.

- 3.3 Knowledgeable:** A consent to the collection, use or disclosure of PHI about an individual is knowledgeable if it is reasonable in the circumstances to believe that the individual knows,
- a) the purposes of the collection, use or disclosure, as the case may be; and
 - b) that the individual may provide or withhold consent.

SHN will make a reasonable effort to ensure that the purposes for which the information will be used are known by the individual by posting a notice describing the purposes where they are likely to come to the individual's attention or by providing information about the purposes orally or in a poster, brochure or other written material. The information will be stated so that the individual can reasonably understand how the information will be used or disclosed.

- 3.4 Non-deceptive, Non-coercive:** SHN will not, as a condition of the supply of a healthcare service, require an individual to consent to the collection, use or disclosure of PHI beyond that required to fulfill the explicitly specified and legitimate purposes, nor will SHN obtain consent through deception.
- 3.5 Revocable:** In circumstances where the individual's consent is required for the collection, use or disclosure of PHI, the individual may withdraw the consent, whether the consent is express or implied, by providing written notice to SHN's Privacy Office. The withdrawal of consent will not have a retroactive effect.

3.6 Limited Consent and Conditional Consent:

Limited Consent: When disclosing PHI with a consent that has been limited by an express instruction from the individual, SHN will notify the custodian to whom the information is being disclosed of the limitation.

Conditional Consent: Any condition an individual places on their consent to SHN's collection, use or disclosure shall not prohibit or restrict SHN from recording PHI as required by law or established standards of practice.

- 3.7 Persons Who May Consent:** SHN will follow applicable laws when determining whether an individual may consent. For more information, **please refer to policies on Consent to Treatment and Access, Disclosure and Correction of Personal Health Information.**

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 7 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

4.0 Limiting Collection of Personal Information

SHN will limit the collection of personal information to that which is necessary for the purposes identified. Information will be collected by fair and lawful means.

4.1 Limited collection: SHN will not collect personal information indiscriminately. Except as otherwise required by law, the amount and type of information collected will be limited to that which is reasonably necessary to fulfill the purposes for the collection. SHN will not collect PHI if other information serves the purpose.

4.2 Non-deceptive collection: The requirement that personal information is collected by fair and lawful means is intended to prevent SHN from collecting information by misleading or deceiving individuals in any way about the purposes for which information is being collected. This requirement implies that consent concerning collection must not be obtained through deception or via omission of reasonable notification. SHN will endeavour to provide as much detail as is reasonably necessary regarding the purposes for collection for individuals to provide knowledgeable consent regarding collecting of their information.

5.0 Limiting Use, Disclosure, and Retention of Personal Information

Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the individual's consent or as permitted, authorized or required by law. Use or disclosure will be limited to that reasonably necessary to meet those purposes. Personal information will be retained only as long as needed for the fulfillment of those purposes.

5.1 Need-to-know access: Individual access to PHI by agents of SHN will be granted based on therapeutic or administrative duties assigned to that individual. Accessing patient information for any other purpose, including research, will be deemed a disclosure and requires approval in accordance with the policy on Access to and Disclosure of PHI.

5.2 Authorized Disclosure: Disclosure of patient information is generally governed by the policy on **Access, Disclosure, and Correction of Personal Health Information** and should be consulted for specific instances of disclosure policy and procedure.

5.3 Retention and Storage of PHI: 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 different media from time to time. Such transfers will be done only after confidentiality is assured. The policy on Retention and Disposal will be followed for retention and safe destruction of PHI.

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 8 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

5.4 Disclosures for Shared Electronic Health Record Systems: SHN participates in provincially approved shared **electronic health records (EHR)** and may securely share patients' PHI with other health care providers involved in their care through an EHR. Patients have the right to know what PHI has been sent to an EHR and which care providers may have accessed this information. Patients may withdraw their consent for provider access to EHR information at any time.

6.0 Ensuring Accuracy of Personal Information

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

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.

7.0 Ensuring Safeguards for Personal Information

Personal information will be protected by reasonable security safeguards appropriate to the nature and format of the information being stored.

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

7.2 Appropriate Measures: The nature of the security safeguards will vary depending on the amount of information, distribution method, format, and method of information storage employed. Information will be safeguarded using measures appropriate to the personal information involved.

7.3 Measures: The methods of protection will include:

- a) Physical measures: for example, use of lockable filing cabinets and restricting access to offices;
- b) Organizational measures: for example, limiting access to personal information on a "need-to-know" basis;
- c) Technological measures: for example, the use of passwords, system access controls and encryption where appropriate;
- d) Regular audits of system access and use, including appropriate disciplinary action for non-compliance with legal or hospital requirements governing access to information.

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded: ADMIN-PY-0001
Policies:

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 9 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

7.4 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:

- a) Review SHN's privacy policy and procedures.
- b) Sign the Statement of Confidentiality (Appendix A)
- c) Participate in mandatory privacy training
- d) On a regular basis, SHN Management will be provided with a list of staff who are non-compliant with privacy requirements (policy review, statement of confidentiality sign off and privacy training) for follow up.

7.5 Handling, Disposal and Anonymization: SHN's record retention and disposal policies have been established in accordance with the Regulation enacted under the Ontario Public Hospitals Act (Reg. 965, s.20) and are reflected in the policy on Retention/Destruction of Records. It is SHN's Policy to retain and dispose of various records in accordance with applicable legislation and guidelines set out in the Ministry of Health Guidelines for Retention and Disposition of Records by Public Hospitals. Care will generally be used to dispose or anonymize personal information and to prevent unauthorized parties from gaining access to the information during or after its use.

8.0 Individual Access to Personal Information

Except as restricted by law, an individual will be informed of the existence, use and disclosure of their 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 may request to have it amended.

In certain circumstances, SHN 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 and are detailed in the policy on **Access, Disclosure, and Correction of Personal Health Information**. The reasons for denying access will be provided to the individual upon request.

Upon written request of the person to whom the PHI pertains or of their Substitute Decision Maker, SHN will provide the individual access to this information and, upon request, provide a copy of the record to the individual or will inform the individual that, after a reasonable search, the information is not available. Where entitled or required to do so, SHN may withhold the information and give written notice to the individual stating that SHN is refusing the request, giving the reason, and stating that the individual is entitled to make a complaint about the refusal to the Commissioner. Response to a request to access such information may be given within 30 days of the request unless otherwise permitted by law. Copies of such information, along with a schedule of access fees may be provided in accordance with the IPC's fee schedule guidance documents.

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded: ADMIN-PY-0001
Policies:

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 10 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

8.1 Correction/Amending: SHN maintains policies that allow for the amendment to patient PHI in its policy on **Access, Disclosure, and Correction of Personal Health Information**. When an individual to whom SHN has given access to their personal information record believes that the record is inaccurate or incomplete for the purposes for which the information was collected or used, the individual may request in writing that a correction be made to the record.

8.2 Reasonable Response: SHN will respond to an individual's request within a reasonable time and at a reasonable cost to the individual. The fee estimate will be provided in advance. If SHN has custody or control of the information and a decision has been made in respect of granting access, including in relation of any severance of information that may be required, the requested information will be provided or made available in a form that is generally understandable to the requestor. SHN will provide professional interpretation of the terminology, code or abbreviation used in the record at the individual's request.

9.0 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 record by completing an access request through the Health Information Management department or accessing MyChart. [Information relating to requesting your health record can be found here.](#) [Information pertaining to MyChart can be found here.](#)

SHN will ensure compliance with privacy policies and procedures through targeted and random audits of SHN information practices and internal systems. The SHN Privacy Office will reference legislation and privacy auditing best practices to conduct regular audits of our 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 per SHN's privacy breach management protocol.

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 11 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

10.0 Disciplinary Action

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

11.0 Challenging Compliance with SHN's Privacy Policies and Practices

An individual will be able to address a challenge or complaint concerning compliance with the above principles to the Chief Privacy Officer.

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, they can contact the SHN's Privacy Office by phone at 416-495-2400 x5745, or email at privacy@shn.ca, or by mail at: **Attention: Privacy Office Scarborough Health Network, 3030 Birchmount Rd, Scarborough, ON M1W 3W3.**

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.

PATIENT AND FAMILY EDUCATION GUIDELINES:

If patients wish to learn more about general privacy practices within Ontario, please refer patients to the [Privacy Brochure](#) on our [external privacy page here](#).

Category: Privacy
Subject: Privacy of Personal Health Information
Issued By: Chief Privacy Officer
Approved By: Senior Leadership Team
Rescinded Policies: ADMIN-PY-0001

Policy Number: SHN-ADMIN-PY-001
Date: 2017/06
Revision Date (s): 2022/09
Page Page 12 of 14

NOTE: A PRINTED COPY OF THIS DOCUMENT MAY NOT REFLECT THE CURRENT, ELECTRONIC VERSION ON SHN INTRANET. ANY COPIES APPEARING IN PAPER FORM SHOULD ALWAYS BE CHECKED AGAINST THE ELECTRONIC VERSION PRIOR TO USE.

REFERENCES

Canadian Standards Association, (1994). *10 Fair Information Principles of the Canadian Standards Association Model Code for the Protection of Personal Information.*

Information and Privacy Commissioner of Ontario, (2004). *A Guide to the Personal Health Information Protection Act*

Information and Privacy Commissioner of Ontario, (2015). *Circle of Care Sharing Personal Health Information for Health-Care Purposes*

Ontario Statutes, (1996). *Health Care Consent Act (HCCA).*

Ontario Hospital Association, (2004). *Hospital Privacy Toolkit: Guide to the Ontario Personal Health Information Protection Act.*

Ontario Statutes, (2004). *Personal Health Information Protection Act.*

Adopted by the Sunnybrook Health Sciences Privacy and Security of Personal Health Information Policy

REVIEWED BY

Privacy and Risk Management Program (2022/07)
Director, Privacy Program (2022/08)
Director, Professional Practice (2022/09)
Policy Working Group (2022/09)

APPROVED BY

Operations Committee (2022/09)

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. I will take all reasonable measures to ensure that sensitive information (personal, patient and corporate) is collected, used and disclosed only in the circumstances necessary by law and authorized for patient care, research, or education, or as required in the conduct of the business of SHN and compliance with the *Personal Health Information Protection Act, 2004*.
3. I shall not remove confidential information from SHN premises except when I must 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 authorized by the Chief Privacy Officer or their 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 I 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 username 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 the 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 416-495-2400 x5745 or privacy@shn.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. 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 the following applies:
 - An individual guilty of committing an offence under PHIPA can be liable for a fine of up to \$200,000 or up to one year in prison, or both. An organization or institution can be liable for a fine of up to \$1,000,000.
 - If a corporation commits an offence under PHIPA, every officer, member, employee or agent of that corporation found to have authorized the offence or who had the authority to prevent the offence from being committed but knowingly refrained from doing so can also be held personally liable.

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 I have questions about this Agreement or my duties regarding privacy and confidentiality, I am to speak to my immediate supervisor or the Privacy Office at any time..

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)