Personal Health Information Privacy Policy

Reviewed Date		**Number**	*IM0101*
Revised Date	September 24, 2020	**Approved Date**	September 20, 2006

Introduction

The Simcoe Muskoka District Health Unit (the Health Unit) is committed to protecting the personal health information under our custody or control. The Health Unit's practices relating to health privacy are governed by:

- the *Personal Health Information Protection Act, 2004* (PHIPA) and its regulations;
- the *Health Protection and Promotion Act*, 1990 and its regulations;
- the *Regulated Health Professions Act, 1991* (RHPA) and its regulations;
- the practice standards of each profession as defined by the professional colleges which guide their practices; and
- the guidance and decisions of the Ontario Information and Privacy Commissioner.

In addition, this policy and associated privacy procedures govern the Health Unit's day-to-day practices and provides a framework that defines the personal health information practices of the Health Unit for the purposes of all applicable privacy legislation. This policy is based on the 10 best practice principles of the *Canadian Standards Association Model Code for the Protection of Personal Information* (CAN/CSA-Q830-96):

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

Purpose

The purpose of this policy is to inform the Health Unit's Board of Health members, employees, students, volunteers, consultants (collectively defined as Health Unit *agents*) and members of the public of the rights and obligations of the Health Unit and the public in relation to the collection, use and disclosure of personal health information.

Legislative Authority

- the *Personal Health Information Protection Act, 2004* (PHIPA) and its regulations;
- the *Health Protection and Promotion Act*, 1990 and its regulations;
- the *Regulated Health Professions Act, 1991* (RHPA) and its regulations;

Policy Definitions and Interpretation

For the purposes of this Policy:

"agent" means a person that, with the authorization of the Medical Officer of Health as a Health Information Custodian (HIC), acts for or on behalf of the HIC in respect of personal health information for the purposes of the HIC, and not for the agent's own purposes, whether or not the agent has the authority to bind the HIC, whether or not the agent is employed by the HIC, and whether or not the agent is being remunerated;

"health information custodian (HIC)" means a person or organization listed in PHIPA that has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or work, and includes a medical officer of health of a board of health within the meaning of the *Health Protection and Promotion Act , 1990.*

"PHIPA" – means *Personal Health Information Protection Act, 2004*

"personal health information" means identifiable information about an individual in oral or recorded form, if the information:

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual,
- relates to payments or eligibility for health care in respect of the individual,
- relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- is the individual's health number, or
- identifies an individual's substitute decision-maker.

Personal health information includes identifiable information that is not personal health information but that is contained in a record that contains personal health information, and is not severed (mixed records).

Policy

Principle 1 – Accountability

The Health Information Custodian of the Health Unit is accountable for the personal health information under the Health Unit's custody or control.

1.1 Accountability for compliance with the principles set out in this Privacy Policy and PHIPA rests with the Health Unit's Medical Officer of Health, however Health Unit agents are responsible for the day-to-day collection, processing, use, storage and disclosure of personal health information.

1.2 The Health Unit will use contractual or other means to provide a comparable level of protection while personal health information is in the custody or control of service providers retained for program or service delivery.

1.3 The Health Unit trains staff on their obligations under this Privacy Policy and PHIPA generally. The Health Unit has also implemented procedures and practices to give effect to the principles set out in this Privacy Policy, including:

a. procedures to protect personal health information against theft, loss and unauthorized collection, use, access, disclosure, disposal, duplication or modification;

b. procedures for receiving and responding to inquiries and complaints from the public as well as managing privacy or security incidents; and

c. information on how to contact the Health Unit and how to obtain access to or request correction of a record of personal health information.

d. All SMDHU employees' volunteers' students and consultants will annually review SMDHU Privacy training PowerPoint and sign SMDHU confidentiality agreement.

Principle 2 – Identifying Purposes

The Health Unit collects personal health information for specific purposes and identifies these purposes at or before the time the information is collected.

2.1 Health Unit agents collect and use personal health information for the following purposes:

- To plan/deliver health services and provide clients with health information/advice;
- To assess current health status and provide public health treatment and interventions to clients;
- To maintain accurate health records, and case/contact information;
- To investigate and manage health hazards and incidents;
- For epidemiological, research and monitoring;
- To respond to complaints or concerns about public health issues or the health unit's practices;
- To contribute to quality improvement processes or research; and
- To comply with legislative and professional requirements.

2.2 Unless otherwise permitted or required by law, the Health Unit shall make reasonable efforts to only collect and use personal health information that is necessary for the purposes identified in section 2.1.

2.3 Upon request, Health Unit agents collecting personal health information must be able to identify to clients the specific purposes for which such information is being collected, or refer the individual to another Health Unit representative who can explain the purposes.

2.4 When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose must first be identified. Unless the new purpose is permitted or required by law, consent is required before the information can be used for that purpose.

Principle 3 – Consent

The Health Unit obtains informed consent for the collection, use or disclosure of personal health information, except where inappropriate.

3.1 Personal health information is collected with the knowledge and consent of the individuals to whom the information relates.

3.2 Personal health information is collected without consent only in instances where the collection is authorized by law, and where it would otherwise be inappropriate in the circumstances to obtain consent.

3.3 Consent may be written or verbal depending on the circumstances and the reasonable expectations of the client.

3.4 Specifically as it relates to personal health information, consent may be express or Implied:

a) **Express consent** is required where personal health information is to be collected, used or disclosed for purposes other than the provision of health care (e.g. disclosures outside the 'circle of care' to an employer or insurance company).

b) **Implied consent** may be appropriate based on the individual's actions or inactions. For example, Health Unit agents can imply consent for specific purposes, such as when an individual requests a program or service, health care, a referral or supportive services. Consent may never be implied if a client specifically states that their personal health information may not be collected, used or disclosed.

3.5 To be valid consent, the following conditions must be met:

- The person must have the mental capacity to consent. Capacity is the ability to understand the information that is relevant to deciding whether or not to consent. A capable person, regardless of age or parental wishes, can consent to the collection, use or disclosure of their own personal health information;
- The consent must be obtained directly from the individual or someone with the legal authority to consent for the individual;
- The consent must be related to the information in question;
- The consent must be obtained voluntarily and without deception or coercion;

- It must be reasonable to believe that the individual understands why you are collecting, using or disclosing the information, and that the individual has the right to withhold or withdraw consent.

3.6 Subject to legal restrictions, an individual to whom the personal health information relates, or their legally authorized representative may place restrictions on their consent or withdraw consent at any time by providing notice to the Health Unit. The withdrawal of consent however, will not have retroactive effect, meaning, Health Unit agents will stop collecting, using and disclosing personal health information as soon as they receive notice of the withdrawal, but will not retrieve personal health information they have already disclosed with consent.

Principle 4 – Limiting Collection

The Health Unit limits the collection of personal information to that which is necessary for purposes identified.

4.1 Vice Presidents ensure that the collection of personal health information is:

- Required for the management and delivery of the programs and services for which they are accountable;
- Limited to the information that is necessary for the purposes identified; and
- Conducted through lawful means and in a manner that does not mislead or deceive the public about the purpose for collection.

4.2 Program Managers define the types of personal health information required for the purposes of delivering each program of the Health Unit.

4.3 Program Managers must ensure that all forms and documents used to collect personal health information include a privacy statement outlining the authority for collection, the purpose for collection, how the information will be used and a contact for questions or concerns regarding information privacy and practices.

4.4 For the most part, personal information is collected directly from the individual who it is about or the individual's legally authorized representative. However, with the consent of the individual or where permitted or required by law, the Health Unit may also collect personal information from others, such as the individual's primary health care provider.

Principle 5 – Limiting Use, Disclosure and Retention

The Health Unit does not use or disclose personal information for purposes other than those for which it is collected, except with the consent of the individual or as required by law. The Health Unit retains personal information only as long as necessary for the fulfillment of those purposes, or as required by law.

5.1 The Health Unit uses or discloses personal information for purposes identified and authorized in Section 2.1.

5.2 Health Unit agents will only access and use personal health information when it is necessary in order to fulfill one's assigned responsibilities.

5.3 Personal health information will be shared between Health Unit agents to the extent necessary for Health Unit agents to fulfill assigned responsibilities or where doing so

will enhance comprehensive and coordinated service provision to the client. De-identified information will be used and shared when this will serve identified purposes.

5.4 Health Unit agents may disclose personal health information to a third party with the express consent of the client or their legally authorized representative.

5.5 Health Unit agents may disclose personal health information to a third party without consent or consultation with management if, in the professional judgment of the agent, the risk of harm to self or others is imminent, or if they are required to do so by law.

5.6 The Medical Officer of Health is responsible for mandatory disclosure of personal health information involving grave environmental, health or safety issues and for discretionary disclosures where they believe on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

5.7 In all other circumstances, personal health information may only be released without consent after consultation with the Program Vice President or Medical Officer of Health. Note that a record must be subpoenaed for use in a court of law. The subpoena should be directed to the appropriate Program Vice President.

5.8 Documentation of the disclosure of personal health information with or without consent must be dated and maintained with the client's health record.

5.9 The Health Unit retains personal health information only as long deemed necessary to fulfill the purposes identified in section 2.1 or as required by law. The Health Unit has developed retention timelines for health records and also periodically reviews the agency's record retention needs.

5.10 Personal health information no longer necessary or relevant for the identified purposes or no longer required to be retained by law, shall be securely destroyed, erased or made anonymous.

5.11 Personal health information that is subject to a request for access will be retained for as long as it is necessary to allow the individual to exhaust any recourse under PHIPA that they may have with respect to the access request.

Principle 6 – Accuracy

To the extent reasonably possible, Health Unit agents ensure records containing personal health information are as accurate, complete and up-to-date as is necessary for the purposes for which the information is to be used.

6.1 The extent to which personal health information will be accurate, complete and up-to-date will depend on the use to be made of such information, taking into account the interests of the individual and the objective of minimizing the possibility of using inaccurate information to make a decision about the individual.

6.2 Health Unit agents will not routinely update personal health information unless this is necessary to fulfill the purposes for which the information was collected.

6.3 Where personal health information is disclosed by the Health Unit for authorized purposes, any limitation on the accuracy of the information will also be noted.

Principle 7 – Safeguards

The Health Unit protects personal health information in its custody or control with security safeguards that are appropriate to the sensitivity of the information.

7.1 By taking steps that are reasonable in the circumstances, Health Unit agents protect personal health information against a variety of risks, such as, loss, theft, unauthorized access, disclosure, copying, use, modification or destruction of such information, regardless of the format in which it is held.

7.2 Safeguards implemented involve physical, organizational and technical measures including but not limited to:

- Security card access to restricted areas of the Health Unit's premises;
- Restriction of employee access to records as necessary;
- Storing paper records in locked cabinets and ensuring they are not left unattended in plain view;
- Holding in confidence personal health information about individuals and families, of which Health Unit agents become aware in the course of providing services to the public;
- Firewalls, anti-virus, strong passwords, audit logs and encryption of data in transit and at rest;
- Ensuring new systems or processes are accompanied by a privacy impact assessment and threat risk assessment; and
- Regular reviews of privacy compliance initiatives and oversight.

7.3 All Health Unit agents with access to personal health information shall be required, as a condition of employment, to safeguard personal health information viewed or handled by them and to complete a privacy training course.

7.4 If required by and in accordance with PHIPA, the Medical Officer of Health will notify clients and the Office of the Information and Privacy Commissioner of Ontario at the first reasonable opportunity if a breach of personal health information that is in the Health Unit's custody or control is stolen or lost, or if their personal health information is accessed, used or disclosed without authorization.

Principle 8 – Openness

Through this Policy, the Health Unit makes readily available specific information about its practices relating to the management of personal health information.

8.1 Health Unit agents are open and transparent about the Health Unit's policies and procedures with respect to health privacy. Individuals are provided with necessary assistance to learn about the personal health information practices of the Health Unit, without unreasonable effort and in a form that is generally understandable.

8.2 The written public statements made available include:

a) A general description of the information practices of the Health Unit and the type of personal health information held by the Health Unit;

b) The title and address of the contact person who is accountable for the Health Unit's information practices and policies and to whom complaints or inquiries can be forwarded; and

c) The means of obtaining access to personal health information held by the Health Unit.

8.3 The Health Unit makes information about its policies and practices available in a variety of ways including brochures available on the Health Unit's premises, on-line access and via a toll-free telephone number (Health Connection).

Principle 9 – Individual Access

The Health Unit informs individuals of the existence, use and disclosure of their personal health information upon request, and gives the individual access to that information. Individuals are given the opportunity to challenge the accuracy and completeness of their information and have it amended as appropriate.

9.1 PHIPA establishes a right of access for individuals to their personal health information as well as the right to request corrections to their health records. The Municipal Freedom of Information and Protection of Privacy Act, 1991 establishes the rights of access to non-health related personal information that is held by the Health Unit. Visit the Health Unit's Privacy Statement to learn more.

9.2 Health Unit agents will use their discretion in responding to routine verbal access requests. However, in some cases, requests for access under PHIPA must be in writing and submitted on a Personal Health Information Access Form made available by the Health Unit.

9.3 Health Unit agents will take reasonable steps to be satisfied as to the identity of the requestor (being the individual who the personal health information requested is about, or their legal representative).

9.4 The Privacy Officer will respond to an individual's request for access as soon as possible in the circumstances but no later than 30 days after receiving a request for access. However, the time limit may be extended for a further 30 days upon written notice, if responding within 30 days would unreasonably interfere with the Health Unit's operations, or where the time required to undertake consultations makes it unreasonable to provide access within 30 days.

9.5 The requestor must provide sufficient detail to enable the Health Unit to identify and locate the records without unreasonable effort. If the request does not contain sufficient detail, Health Unit agents will offer assistance to the requestor in reformulating the request.

9.6 PHIPA does not prevent Health Unit personnel from informally communicating with clients or their legally authorized representatives about their personal health information, provided such communications remain private and secure.

9.7 In certain situations, the Privacy Officer will not be able to provide access to all the personal health information it holds about an individual, for example, in the context of a legal exception. In such cases, in accordance with PHIPA and in consultation with the Medical Officer of Health, access will be denied or access to certain personal

health information will be severed. The requestor will receive a reason for the refusal and be informed of the right to appeal the Health Unit's decision to the Information and Privacy Commissioner of Ontario.

9.8 Requests for corrections to personal health information records must be in writing. Health Unit agents will make the requested correction if the client provides sufficient evidence to prove that the record is not accurate or complete for the purposes for which the information was collected.

9.9 Corrections are not required if:

- the record was not created by the Health Unit or where there is not sufficient knowledge, expertise and authority to correct the record, including the inability to validate the new information being provided;
- there is reason to believe that the request for correction is frivolous, vexatious or made in bad faith (requests should only be refused for these reasons in the rarest of cases);
- the client has failed to demonstrate that the record is not correct or complete; or
- the client has not provided the information needed to make the correction.

9.10 Health Unit agents are not required to change professional opinions or observation made in good faith about a client.

9.11 Where an individual is unsuccessful at having a record of their personal information corrected, they may prepare a statement of disagreement outlining their objection to its accuracy. This statement will be appended to the record held by the Health Unit.

Principle 10 – Challenging Compliance

An individual may address a challenge concerning the Health Unit's compliance with the principles set out in this Privacy Policy to the Health Unit's Privacy Officer.

10.1 Privacy complaints should be submitted to the Privacy Officer in writing using the Health Unit's Privacy Complaint Form.

10.2 The Health Unit maintains procedures for receiving and responding to all inquiries and complaints about information practices relating to personal health information.

10.3 All complaints concerning compliance with this Policy shall be investigated by the Health Unit in a timely manner. If a complaint is found to be justified, the Health Unit shall take appropriate measures to resolve the complaint including, if necessary, amending its policies and practices.

Privacy Officer Contact Information:

If you have any questions about this Policy, the Health Unit's privacy practices, or need assistance with accessing your personal health information, please contact:

Privacy Officer
Simcoe Muskoka District Health Unit
15 Sperling Drive
Barrie, ON L4N 6K9 Email: PrivacyOfficer @smdhu.org

Procedures

Privacy and Information Management Procedures

Related Policies

IM0108 Information Privacy and Security Incident Management Policy
IM0101 SMDHU Privacy Statement
IM0121 Transporting Records Policy

Related Forms

IM0101 (F1) Confidentiality Agreement

IM0101 (F2) Withdrawal of Consent

IM0101 (F3) Release of Personal Information

IM0101 (F4) MFIPPA Access / Correction Request

IM0101 (F5) PHIPA Access / Correction Request

IM0101 (F6) Privacy Complaint Form

IM0108 (F1) Report of Information Privacy or Security Incident

E-Learning

Information Privacy Security and Access

Final Approval Signature: _____

Review/Revision History:

September 2020

- Policy Revision
- Consolidating of polices IM0102 Accountability, IM0103 Consent, IM0104 Collection and Use, IM0105 Disclosure, IM0106 Access, and IM0107 Correcting Records into *IM0101 Personal Health Information Privacy Policy*
- Creation of Privacy and Information Management Procedures Manual

September 2010 Policy re-numbered, previous number A1.041