NORMAN RECOLLET HEALTH CENTRE PRIVACY POLICY

Policy Type:	Health	**Initially Approved:**	01/26/2026 BCM WFN 25/26-01-285
Policy Sponsor:	Health Department	**Last Revised:**	01/26/2026
Primary Contact:	Health Director	**Review Scheduled:**	01/2027
Approver:	Chief and Council BCM WFN 25/26-01-285		

TABLE OF CONTENTS

GENERAL PRIVACY POLICY

PURPOSE

This policy outlines what the Norman Recollet Health Centre ("the Health Centre") and its agents must comply with under the Personal Health Information Protection Act (PHIPA).

POLICY STATEMENT

The Health Centre is committed to protecting client privacy. PHIPA sets out rules that Health Information Custodians must follow when collecting, using, disclosing, retaining and disposing of Personal Health Information (PHI). These rules apply to all Health Information Custodians operating within the province of Ontario, including the Health Centre.

This policy applies to every person who works with or has access to PHI at the Health Centre, including, but not limited to employees, volunteers, students, health professionals (physicians, nurses, dieticians, physiotherapists, etc.), researchers, contractors, sub-contractors and other agents. All of these individuals are referred to as Agents of the Health Centre.

DEFINITIONS (from PHIPA)

"Agent" means a person authorized by the Health Centre to handle PHI for the Health Centre.

"Health Information Custodian" or "HIC" means persons or organizations described in PHIPA who have custody or control of PHI as a result of their work. The Health Centre is a HIC.

"Identifying information" is information that identifies an individual, alone or with other information.

"Information practices" means the policy of the Health Centre for actions in relation to PHI, including:

- when, how and the purposes for which the Health Centre collects, uses, modifies, discloses, retains or disposes of PHI, and
- the administrative, technical and physical safeguards and practices that the Health Centre maintains with respect to PHI.

"Personal Health Information" or "PHI" means identifying information about an individual (living or deceased) in oral or recorded form as it relates to:

- Physical or mental health, including health histories of the person and their family
- Provision of health care
- A home and community care plan of services
- Payment or eligibility for health care
- Donation of body parts or bodily substances
- Health card number

- Identity of the person's substitute decision maker
- Identifying information that is not described above but that is contained in a client's PHI record.

"Privacy Breach" is when PHI is stolen, lost or inappropriately accessed, used or disclosed without client consent.

"Substitute decision maker" is a person legally authorized to give or refuse consent to a treatment on behalf of a person who is incapable with respect to treatment.

PROCEDURE

1. Accountability

The Health Centre is a Health Information Custodian responsible for collecting, using and disclosing PHI in its custody or control. The Health Centre is required to have information practices in place that comply with PHIPA. The Health Centre has designated a Privacy Contact Person who is accountable for the Health Centre's compliance with this Policy.

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

1.2. Responsibilities: The Contact Person is an agent of the Health Centre and is authorized on behalf of the Health Centre to:

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

1.3. Public Record of Contact Person: The identity of the Contact Person will be publicly available as detailed below. The Contact Person can be contacted via telephone at 705-858-7700, via email at nursepractitioner@wahnapitaefn.com], or by writing to Attention Privacy Contact Person, 190 Loonway Rd, Capreol ON, P0M 1H0.

1.4. Openness: the Health Centre will be open about its information practices concerning the management of PHI. Individuals can acquire information about the Health Centre

policies and procedures without unreasonable effort. This information will be made available in a generally understandable form.

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

a. provides a general description of the Health Centre'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 the Health Centre and the Information Privacy Commissioner.

1.6. Third Party Contracts: The Health Centre 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 Health Centre.

2. Identifying Purposes for the Collection of Personal Information

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 clients, both inside and outside of the Health Centre;
- To communicate or consult client's health care with their doctor(s) and other health care providers;
- To receive payment/funding for clients' health care and Health Centre services, including from Canada, the province and/or private insurers;
- 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 client surveys;
- To notify clients of an appointment or change an appointment;
- To report as required or permitted by law;
- 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 PHI is collected 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, Health Centre agents will be able to explain to individuals the purposes for which the information is being collected.

3. 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.

3.1 Capacity: A client 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. The Health Centre 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 withdraw consent. A substitute decision maker or another authorized individual may provide consent on behalf of the client, as permitted by law.

3.2 Consent may be express or implied. When a custodian disclosed PHI to another custodian *for the purpose of providing health care*, the consent of the individual may be implied, unless the individual has specifically withheld or withdrawn the consent. If the purpose of the disclosure is not to provide health care, consent must be express. Also, consent for disclosures to third parties that are not custodians must be express.

3.3 Knowledgeable Consent: 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.

The Health Centre 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.

3.4 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 the Health Centre's Privacy Office. The withdrawal of consent will not have a retroactive effect.

3.5 Limited Consent and Conditional Consent:

Limited Consent: When disclosing PHI with a consent that has been limited by an express instruction from the individual, the Health Centre 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 the Health Centre's collection, use or disclosure shall not prohibit or restrict the Health Centre from recording PHI as required by law or established standards of practice.

3.6 Persons Who May Consent: the Health Centre will follow applicable laws when determining whether an individual may consent.

4. Limiting Collection of Personal Information

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. The Health Centre will not collect PHI if other information serves the purpose.

5. 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 the Health Centre will be granted based on a need-to-know basis.

5.2 Authorized Disclosure: Disclosure of PHI is only permissible with client consent or as permitted or required by applicable laws.

5.3 Retention and Storage of PHI: The Health Centre will develop and implement a policy on Retention, Storage and secure Destruction of PHI.

5.4 Disclosures for Shared Electronic Health Record Systems: The Health Centre may participate in a shared electronic health records (EHR) program which permits the

secure sharing of clients' PHI with other health care providers involved in their care through an EHR. Clients have the right to know what PHI has been sent to an EHR and which care providers may have accessed this information.

5.5 Handling and Destruction: The Health Centre's record retention and disposal policies will be established in accordance with applicable legislation and guidelines for the health sector.

6. 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. Ensuring Security of Personal Information

Personal information will be secured with measures appropriate to the nature and format of the information being stored.

7.1 Scope of Security Measures: Security measures will be used to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, modification or disposal. The Health Centre will protect personal information regardless of the format in which it is held.

7.2 Measures: The methods of protection will include, for example:

a. Physical measures, such as lockable filing cabinets and restricting access to offices;
b. Organizational measures, such as limiting access to PHI on a "need-to-know" basis;
c. Technological measures, such as 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 Health Centre requirements governing access to PHI.

8. Education and Awareness

The Health Centre will provide programs to educate and inform Health Centre staff of the importance of maintaining the confidentiality of PHI and their respective responsibilities. Prior to the start of employment, the granting of Health Centre privileges or entering into any direct affiliation with the Health Centre, and on a regular basis thereafter, Health Centre staff are required to:

a. Review the Health Centre's privacy policy and procedures,
b. Sign the Health Centre's Confidentiality Agreement,
c. Participate in mandatory privacy training.

On a regular basis, Health Centre management will be provided with a list of staff who are non-compliant with privacy requirements (policy review, confidentiality agreement and privacy training) for follow up.

9. Individual Access to Personal Information

Except as restricted by law, a client will be informed of the existence, use and disclosure of their personal information and will be given access to that information. A client will be able to challenge the accuracy and completeness of the information and may request to have it amended.

9.1 Upon written request of the person to whom the PHI pertains or of their Substitute Decision Maker, the Health Centre 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, the Health Centre may withhold the information and give written notice to the individual stating that the Health Centre is refusing the request, giving the reason, and stating that the individual is entitled to make a complaint about the refusal to the Commissioner.

9.2 Correction/Amending: When a client to whom the Health Centre 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 client may request in writing that a correction be made to the record.

10. Privacy Incident Management

It is prohibited and against the law to access client data unless such access is required to perform duties assigned or sanctioned by the Health Centre. Anyone found accessing client data outside these parameters has committed a serious breach of privacy and will be subject to disciplinary action.

The Privacy Contact Person will reference legislation and privacy auditing best practices to conduct regular audits of Health Centre records and systems.

The Health Centre promotes transparency and requires staff to report privacy and data protection concerns, including suspected breaches of PHI and privacy policies and procedures to the Privacy Contact Person, in confidence.

All suspected privacy incidents will be managed according to the Health Centre's Privacy Breach Protocol. If none exists, the Health Centre will follow the steps set out in the Information and Privacy Commissioner's publication "Responding to a Health Privacy Breach: Guidelines for the Health Sector".

11. 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 Health Centre privileges and a report to their respective regulatory college, if applicable.

12. Challenging Compliance with the Health Centre's Privacy Policies and Practices

The Health Centre's Contact Person is the initial point of contact for complaints and inquiries related to compliance with PHIPA at the Health Centre. If any individual has a question, concern or complaint about the Health Centre's compliance with privacy obligations under PHIPA, they can contact the Health Centre's Privacy Contact Person at: Nurse Practitioner, 190 Loonway, Capreol, ON, P0M 1H0, 705-858-7700, nursepractitioner@wahnapitaefn.com.

When a complaint is received, the Privacy Contact Person will:

- Acknowledge that the complaint has been received
- Investigate the complaint
- Determine what action will be taken, if any
- Provide a response to the complainant
- Advise the complainant of their right to complain to the Information and Privacy Commissioner of Ontario

At any time, 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

REQUESTS FOR CLIENT RECORD ACCESS, CORRECTION AND COMPLAINT BACKGROUNDER
Norman Recollet Health Centre

ACCESS, CORRECTION AND COMPLAINT BACKGROUNDER

POLICY

The Health Centre's policy regarding client access, correction and complaints is in the General Privacy Policy, paragraphs 8 and 11.

BACKGROUNDER AND KEY CONCEPTS

Access (PHIPA ss. 51-54)

With some exceptions, the Act provides individuals with a right of access to records of their own personal health information. The right of access applies to a record that is dedicated primarily to the individual. If the record is not primarily about the individual, the right of access extends only to that portion of the record that is about the individual. However, a person does not have a right of access to personal health information in a record that is dedicated primarily to the personal health information of another person. The right of access does not apply to records that contain quality of care information, information required for quality assurance programs, raw data from psychological tests or assessments, and other specified types of information (i.e., information that is used solely for research purposes and laboratory test results).

Custodians must provide individuals with access to records containing their own personal health information unless:

- a legal privilege restricting disclosure applies;
- another law prohibits the disclosure;
- the information was collected or created for a proceeding;
- the information was collected or created during an inspection, investigation or similar
- procedure; or
- access could result in serious harm to any person or the identification of a person who was required to provide information or who has provided the information in confidence.

If one of the above exceptions applies to the record, the custodian should sever the record and provide access to that part of the record to which the exception does not apply.

Requests for access should be in writing and must provide enough information to allow the custodian to identify and locate the record. Where the individual has not provided sufficient detail, the custodian is required to offer assistance. It is important to note that nothing in the

Act prevents a custodian from granting access to a record in response to an oral request or communicating with an individual about his or her record of personal health information. Custodians are encouraged to provide access to records in the absence of formal written requests.

Correction (PHIPA, s.55)

If an individual believes that a record of personal health information is not as accurate or complete as necessary for its purpose, the individual may make a written request to the custodian to correct the record. The custodian has 30 days to respond to the request. A 30-day extension is permitted if responding to the request within 30 days would unreasonably interfere with the activities of the custodian or more than 30 days is needed to undertake consultations to respond to the request.

The custodian is obligated to correct a record that is not accurate or complete, unless the custodian did not create the record or the record consists of a professional opinion made in good faith. Corrections can be made by recording the correct information in the record. This can be done by striking out incorrect information in a way that does not obliterate the information or by labelling the information as incorrect, severing it from the record, and storing in separately but linked to the record. If it is not possible to record the correct information in the record, the custodian must ensure that there is a system in place to inform anyone who accesses the record that the information is not correct and to direct the person to the correct information.

Once a correction has been made, the individual may require the custodian, to the extent reasonably possible, to inform anyone to whom the information has been disclosed. One exception is if the correction cannot reasonably be expected to affect the provision of health care or other benefits to the individual.

If the custodian refuses the correction request, the individual may prepare a statement of disagreement and require the custodian to attach it to the record. The individual may also require the custodian to make all reasonable efforts to disclose the statement of disagreement to anyone who would have been notified had a correction been made.

An individual who is not satisfied with a decision of the custodian with regard to the correction of a record is entitled to complain to the Commissioner.

Complaints System (PHIPA, section 56-65)

A person who believes another person has contravened or is about to contravene the Act may complain, in writing, to the Commissioner.

Upon receiving a complaint, the Commissioner may ask about other means the complainant

is using or has used to try to resolve the matter; require the complainant to try to settle the matter with the person who is the subject of the complaint; or authorize a mediator to try to settle the matter.

If the issues in a complaint cannot be settled informally, the Commissioner may conduct a review of the complaint. It is the Commissioner's decision whether or not to conduct a review. In the absence of a complaint, the Commissioner also has the power to conduct a self-initiated review.

Adapted from: A Guide to the Personal Health Information Protection Act, Information and Privacy Commissioner/Ontario, December 2004.

ACCESSING HEALTH RECORDS
Norman Recollet Health Centre

Procedural Guide

The Rule

Except under special circumstances, clients have the right to access their personal health records.

Clients may request access to their personal health records orally or in writing. Oral requests are routine when the client is still receiving care, and the Act does not prohibit you from responding to oral requests. The request must be in writing, however, to invoke the rights and procedural requirements set out in the Act. A substitute decision-maker can request access on a client's behalf because the right of access exists whether or not a client has capacity. Substitute decision-makers will follow the same process to obtain access to the personal health record as the client.

What you need to do if you are asked for access to a personal health record:

- Verify the client's identity or substitute decision-maker's authority.
- Determine if the request contains enough detail to let you reasonably find the record. If you need more information to find the record, work with your client to obtain the information you require. If you cannot find the record after a reasonable search, tell the requestor so in writing.
- Determine if one of the legal exceptions applies to providing access. See the tables below for a description of where you may refuse access.
- If a legal exception applies:
    - tell the requestor in writing that you are refusing access, in whole or in part, and why you are doing so,
    - where possible, sever the record and provide access to the part of the record where no legal exception applies,
    - tell the requestor about your complaints procedure, and that if the requestor is not satisfied with your resolution of the complaint, the requestor can complain to the Commissioner, and
    - in some circumstances, you cannot even tell the requestor that a personal health record exists.
- If no legal exception applies and you can find the record, arrange to provide access. You can provide access by showing the requestor the original record. If you choose to show the requestor the original record, you should arrange for the requestor to be monitored while viewing the record to ensure that it is not altered in any way. You can also provide access by giving the requestor a copy of the record. You must provide a copy if the requestor asks for a copy.

- If reasonably practical, answer any questions about any medical terms or abbreviations used in the record.

Fees for Providing Access

You may charge a fee to provide access to a personal health record if you first give the requestor an estimate of the fee. The fee you charge cannot exceed either a prescribed amount or, if no amount is prescribed, a reasonable cost recovery charge. You may waive payment of all or any part of the fee if it is fair to do so.

Timeframe to Respond to a Request for Access

Respond to requests for access as soon as possible. If you need more than 30 days to respond to a request for access, provide the requestor with written notice of an extension.

An extension is only permitted if:

- replying to the request within 30 days would reasonably interfere with your activities because locating the personal health record requires a complex search, or
- the time required to undertake the necessary consultations would make it reasonably impractical to reply within 30 days.

The written notice of an extension should explain when you will respond, and why an extension is needed. An extension cannot exceed an additional 30 days. If you do not provide access within the stated time period, the requestor can assume that you have refused the request.

Urgent Requests for Access

If a requestor can satisfy you that the request is urgent, you must provide access within the requested time period, if it is reasonable to do so.

Refusing a Request for Access

The table below lists circumstances where you may refuse access to personal health records. Even when a restriction to access exists, a requestor has a right to access personal health information not related to the restriction. You must sever the restricted information from the rest of the record, and give the requestor access to the remaining information.

You should tell requestors that their request has been refused and, where appropriate, give reasons for the refusal. There may be situations where access is refused and you do not confirm or deny the existence of a record. This is context specific and you may need to confer with a psychologist, legal counsel or the Commissioner about how reasons for your refusal should be communicated.

You should tell requestors that they can complain about your refusal to the Commissioner. You should also provide information on how to contact the Commissioner.

Guidelines for Refusal of Access

In each of the following situations, you should provide access to the part of the record that is not impacted by the reason for refusal and that can reasonably be severed from the record.

Reason for Refusal of Access	**Follow-Up Notification to Requestor**	
	State you are refusing the request (in whole or in part) and reason for the refusal	**State you are refusing to confirm or deny the existence of any record**
The record contains quality of care information	×	
The record contains information collected/created to comply with the requirements of a quality assurance program under the *Health Professions Procedural Code* that is Schedule 2 to the *Regulated Health Professions Act*	×	
The record contains raw data from standardized psychological tests or assessments	×	
The record (or information in the record) is subject to a legal privilege that restricts disclosure to the requestor	×	
Other legislation or court order prohibits disclosure to the requestor	×	
The information in the record was collected/created in anticipation of or use in a proceeding that has not concluded		×
The information in the record was collected/created for an inspection/investigation/similar procedure authorized by law that has not concluded		×
Granting access could reasonably be expected to result in a risk of serious harm to the patient or to others (Where this is suspected you may consult a physician or psychologist before deciding to refuse access)		×

Reason for Refusal of Access	Follow-Up Notification to Requestor	
	State you are refusing the request (in whole or in part) and reason for the refusal	State you are refusing to confirm or deny the existence of any record
Granting access could lead to the identification of a person who was required by law to provide the information in the record		×
Granting access could lead to the identification of a person who provided the information in the record in confidence (either explicitly or implicitly) and it is considered appropriate to keep the name of this person confidential		×
The request for access is frivolous, vexatious or made in bad faith	×	
The identity or authority of the requestor cannot be proven by the requestor	×	

Source: Hospital Privacy Toolkit: Guide to the Ontario Personal Health Information Protection Act, Ontario Hospital Association, Ontario Hospital eHealth Council, Ontario Medical Association, Office of the Information and Privacy Commissioner/Ontario, September 2004.

INDIVIDUAL REQUEST TO ACCESS PERSONAL HEALTH INFORMATION
Norman Recollet Health Centre

Instructions: We will provide you with access to your personal health record unless a legal exception applies. We will review all health record access requests and will make every effort to respond to your request in a timely manner. Please complete Parts A and B of this form. Part C is for the Health Centre's internal use.

PART A: CLIENT INFORMATION

Last Name _____ First Name _____ Initials _____

Home Address _____

Phone Number _____ Date of Birth _____

If you are a parent/guardian/substitute decision-maker, your contact information

Last Name _____ First Name _____ Initials _____

Home Address _____

Phone Number _____

Note: Include copies of documents that provide your authority as a substitute decision-maker.

PART B: ACCESS REQUEST

1. Describe what you need and include details that will help us locate the record (e.g. dates, name of healthcare provider, etc.)

_____

_____

_____

_____

2. How would you prefer to access this information?
    - Receive hard copies of originals (note that there may be a fee)
    - Receive electronic copies (if available)
    - Examine originals in the Health Centre

Signature

Name (print)

Date

PART C: (INTERNAL USE ONLY) RESPONSE TO ACCESS REQUEST	
1. Date Request Received	
2. Date Response Issued	
	○ Access request granted ○ Access request not granted ○ Access request granted in part If complete access request not granted, reason:
3. Reasons and dates regarding any extensions:	
4. Processed by:	

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS
Norman Recollet Health Centre

Personal Health Information

Identify the administrative, technical and physical safeguards that your organization has in place to protect the security of personal health information and consider whether any additional safeguards are required. It is not necessary to employ every safeguard listed below. Examples of safeguards are offered but not all are appropriate for every case. In addition to the generic safeguards described below, special safeguards may be required for extremely sensitive information.

PHYSICAL SAFEGUARDS

Office area restricted to staff:

- no staff permitted without continuous supervision
- for larger organizations, use security badges or sign-in sheets
- all files with personal health information locked away after hours
- all files with personal health information locked away before non-staff permitted entry (e.g. cleaners)
- all non-staff who require entry (e.g. cleaners) must sign confidentiality agreement
- other: _____

Office area open to non-staff:

- area must be supervised at all times
- all files with personal health information must be locked away when staff not present (e.g., after hours)
- all files with personal health information must be locked away or supervised when staff person leaves their desk
- other: _____

Home office:

- files with personal health information must be locked away in a desk, filing cabinet or separate room when unattended
- other: _____

Transfer of physical files:

- in a sealed envelope, marked private and confidential, sent by Canada Post or reputable courier with a strong privacy policy (if appropriate)

- in a sealed envelope, marked private and confidential, delivered by staff
- in a sealed envelope to be picked up by recipient or person authorized by recipient (identity to be confirmed)
- other: _____

General:

- office equipped with alarm/security system
- other: _____

TECHNICAL SAFEGUARDS

Office area restricted to staff:

- no non-staff permitted without continuous supervision
- for larger organizations, use security badges or sign-in sheets
- all non-staff who require entry (e.g. cleaners) must sign confidentiality agreement
- a strong login password is required on each terminal/device
- other: _____

Office area open to non-staff:

- area must be supervised at all times
- no personal health information can be left on a screen when person leaves workstation (log off, shut down or lock computer)
- a strong login password is required on each terminal/device
- other: _____

Mobile devices (e.g. smart phones, laptops, USB keys) and remote access:

- must have strong encryption
- must have strong login password
- identifying information should not be used in cell phone conversations, text messages or email messages
- remote access available only through secure remote network or virtual private network
- other: _____

Transfer of electronic information:

- by using an encrypted USB drive or other encrypted storage device
- by using a secure web portal
- by email if:
  - consent is obtained;

- the message is anonymized; or
- the information is encrypted.

- by fax if:
  - a cover sheet identifies the recipient and includes a privacy clause;
  - the fax number has been approved by the recipient;
  - the recipient is expecting the fax;
  - the recipient has advised that the fax machine is securely located; and
  - the recipient confirms that all pages have been received.
- other: _____

General:

- networks/computers must be protected by up-to-date virus scanners and firewalls
- appropriate file back-up systems must be in place
- for more sophisticated networks, unique user identifiers, audit trails, and intrusion detection systems
- for wireless networks, up-to-date transmission encryption should be used
- other: _____

ADMINISTRATIVE SAFEGUARDS

- staff (including temporary staff) is trained in the following:
  - the importance of protecting the privacy of personal health information
  - access to personal health information within the organization is on a need-to-know basis
  - the organization's Privacy Policy
  - the appropriate use of social media
  - sensitivity in collecting or using personal health information verbally where others might hear
  - sensitivity in handling personal health information on mobile devices where others might be able read ("shoulder-surfing")
  - when providing copies of personal health information internally or externally, to remove or redact unnecessary personal health information
  - to recognize and avoid being "pumped" for information
  - to ensure that any personal information is not accidentally discarded in the regular garbage or blue box disposal system, but rather is cross-cut shredded
  - to ensure that when electronic data is deleted or hardware is discarded, the data cannot be recovered
  - to avoid discussing personal information in public places (e.g., elevators, restaurants, washrooms, public transit)
  - the fact that the organization needs to be notified about any breaches, who must be notified and that notification must be made at the first reasonable opportunity
  - that breach of the organization's policies will result in discipline up to and including dismissal, as well as a report to the relevant regulatory College and may result in a complaint to the Information and Privacy Commissioner or a provincial prosecution

- regular (at least annual) review and updating of staff through a continuing education program

- privacy and security agreements with the following consultants and outsourced providers:
  - temporary workers
  - cleaners
  - information technology providers
  - marketers
  - legal
  - bookkeeping and accounting

- file storage
- credit card companies
- website manager
- office security
- building maintenance
- landlord
- other: _____

- regular and systematic monitoring of compliance with the organization's policies by the Contact Person or his or her delegate (which should be documented)

- regular reminders to staff to change their passwords and to have strong passwords

- regular and systematic auditing of the electronic safeguards by an external company (which should be documented)

- review physical layout and procedures appropriate to the context (e.g., use rooms rather than cubicles or curtains for sensitive interviews, keep people in the waiting room for as short a time as possible)

- other: _____

Adapted from: The Personal Health Information Protection Act, 2004: A Guide for Regulated Health Professionals, June 28, 2016. Original Work Copyright 2016 by Steinecke Maciura Leblanc.

CONFIDENTIALITY AGREEMENT
Norman Recollet Health Centre

1. I understand that during my association with Norman Recollet Health Centre, I may have access to confidential information relating to clients, other Health Centre staff, the Health Centre and the First Nation. 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, client, organizational and First Nation) is collected, used and disclosed only in the circumstances necessary by law and authorized for client care or as specifically authorized by the Health Centre for Health Centre business and compliance with the *Personal Health Information Protection Act*, 2004, where applicable.

3. I shall not remove confidential information from the Health Centre premises except when I must do so for a legitimate purpose related to my association with the Health Centre. I shall not remove client records or other personal health information from the Health Centre unless authorized by the Health Centre's Privacy Contact Person or their delegate. If I am required to remove information from the Health Centre's premises, I will take all necessary measures to safeguard this information.

4. I will take all reasonable steps necessary to safeguard any system or electronic passwords provided to me and I shall not disclose them 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 arrange for assignment of a new password.

5. I understand that my access to the Health Centre's records, including personal health information of clients, will be strictly limited to accessing the information on a need-to-know basis for direct client care or performance of my 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 that the Health Centre will conduct regular detailed audits of my access and use of electronic records systems. I understand and agree that I will be accountable for access to any records where I do not have a need to know.

7. I understand that the aggregate or anonymous health reports about Health Centre clients in general or about the First Nation are also sensitive and confidential and that they must be accessed or created only on a need to know basis and the confidentiality of them must be maintained in the same manner as if they contained personal health information.

8. 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 the Health Centres privacy policies or procedures, I agree to notify the Privacy Contact Person at: 705-858-7700, 190 Loonway Rd,

Capreol, ON, P0M 1H0, email: nursepractitioner@wahnapitaefn.com and my supervisor at my first reasonable opportunity.

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

   - Deactivation of my access to electronic health systems and records;
   - Discipline including termination of employment or contractual with the Health Centre;
   - A report to my regulatory college where applicable;
   - A report to the Information and Privacy Commissioner, where applicable.

10. 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.

11. 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 the Health Centre.

12. I further understand that my association (employment or contract) with the Health Centre is conditional upon my agreement herein and that my refusal to agree to these terms will disqualify me from working at the Health Centre.

13. 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 Contact Person.

I, _____, agree that I have read and will observe and comply with the Health Centre's privacy policy, procedures and this Confidentiality Agreement.

_____ _____

Signature Date

CONSENT BACKGROUNDER
Norman Recollet Health Centre

POLICY

The Health Centre's policy regarding consent for the collection, use and disclosure of personal information is in the General Privacy Policy, paragraph 3.

BACKGROUNDER AND KEY CONCEPTS

Principles of Identifying Purposes and Obtaining Consent

PHIPA generally requires consent for the collection, use and disclosure of personal health information (s. 29). PHIPA provides specific guidance as to what constitutes a valid consent for the collection, use and disclosure of such information.

For example, implied consent is generally permitted where it is reasonable to assume that the individual knows the purpose of the collection, use or disclose and their right to give or withhold consent. If the purposes are stated in a poster or brochure readily available and likely to be seen by the individual (for an example, the Health Centre's written Privacy Statement), one can assume the individual knows the purpose.

Importantly, custodians can assume that they have an individual's implied consent to collect, use or disclose personal health information for the provision of health care if the following conditions are met:

- the information was received from the individual, the individual's substitute decision-maker or another health information custodian;
- the information was received for the purpose of providing health care to the individual;
- the information is collected, used or disclosed for the purpose of providing health care to the individual;
- if information is being disclosed, it must only be disclosed to another health information custodian; and
- the individual has not withheld or withdrawn consent.

While this term is not defined in PHIPA, this is commonly referred to as sharing personal health information within the *"circle of care"* (s. 18-20).

Express consent (verbal or written) is needed, however, to disclose personal health information to a non-custodian and to disclose PHI to another custodian for purposes other than the provision of health care. In addition, express consent is required for certain fundraising and marketing activities (s. 18-20, 32-33).

Practitioners can assume that a written consent is valid unless provided with grounds to the contrary (s. 20).

A direction from a client not to record pertinent information is invalid (ss. 19(2)). However, a client may direct that part of his or her file not be given to another custodian. This is commonly referred to as placing that information in a *"lock-box"*. If the custodian believes that the other custodian needs the "locked" information, the disclosing custodian must advise the receiving custodian that some relevant information has been withheld at the direction of the client (but not what that withheld information is) (ss. 20(2) and 20(3)). [See Information and Privacy Commissioner of Ontario – Lock-box Fact Sheet]

PHIPA provides detailed rules for obtaining substituted consent where the individual is not capable of understanding the information issue or appreciating its reasonably foreseeable consequences. The rules for substituted consent are very similar to those for treatment of incapable persons. One can presume an individual is capable until it becomes apparent that he or she is not capable (s. 21). The substituted decision maker for handling of treatment information issues is generally the same as the substituted decision maker for treatment decisions (s. 5). If the information issue is not related directly to treatment, the list of substituted decision makers is very similar to that under the Health Care Consent Act, 1996 (s. 23). One minor difference is that a capable person can authorize someone in writing to act on his or her behalf. Another difference is that a custodial parent can authorize decisions affecting the personal health information of their child 15 years or younger unless the child disagrees, the child consented to the original treatment on his or her own or for some family counselling situations (s. 23). A third difference is that a guardian or attorney for property can act as a substitute (ss. 26(1)).

Principles of Use and Disclosure

PHIPA provides some flexibility for the use of personal health information without consent. For example, personal health information can be used without consent for a purpose of planning or delivering programs, risk management, educating practitioners and some research situations (ss. 37(1)).

Similarly, PHIPA provides for the disclosure of personal health information without consent, including disclosure in the following circumstances:

- to other practitioners or facilities for the provision of health care, if it is not reasonably possible to obtain consent in a timely manner so long as the client has not objected to such disclosure;
- to address a significant risk of serious bodily harm to a person or group;
- to potential and actual successors of the custodian (although potential successors must provide a written confidentiality assurance and affected individuals must be notified of any actual transfer of records to a successor);

- to assess capacity under the Health Care Consent Act, 1996 and the Substitute Decisions Act, 1992;
- to a health regulatory College;
- in legal proceedings where the custodian or agent is or is expected to be a party or witness;
- to the Public Guardian and Trustee, the Children's Lawyer, a children's aid society, so that they can carry out their statutory functions;
- in some research situations (subject to approval by a research ethics board);
- in some health planning and management purposes;
- to a health data institute under various rules and restrictions; and
- in other situations where permitted or required by law (ss.38-47).

Adapted from: The Personal Health Information Protection Act, 2004: A Guide for Regulated Health Professionals, June 28, 2016 (Original Work Copyright 2016 by Steinecke Maciura Leblanc)

CLIENT CONSENT FORM FOR THE COLLECTION, USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION
Norman Recollet Health Centre

Note to client: We want your informed consent. We want you to understand what we do with the personal health information we collect about you. Please ensure that you have read and understood our written statement, "Our Privacy Statement". If you have any questions, please ask.

1. I, _____, understand that to provide me with required health services, the Norman Recollet Health Centre ("Health Centre")will collect personal information about me (e.g., birth date, home contact information, health history, etc.).

2. I have reviewed the Health Centre's written statement ("Our Privacy Statement") on the collection, use and disclosure of personal health information. I understand how the written statement applies to me. I have been given a chance to ask questions about the Health Centre's privacy policies and they have been answered to my satisfaction.

3. I understand that the Health Centre will only collect, use or disclose my personal health information with my express or implied consent, unless a collection, use or disclosure without consent is permitted or required by law.

4. I authorize the Health Centre to collect, use and disclose my personal health information for the following purposes *(indicate your consent by checking the applicable box(es)):*

   - ○ to notify me of new programs or services available through the Health Centre;
   - ○ to notify me of special events and opportunities at the Health Centre (e.g. a seminar or conference);
   - ○ *[add any other purposes that require express consent].*

I understand that I can withdraw my consent at any time by contacting the Health Centre's Privacy Contact Person.

I agree to the Health Centre collecting, using and disclosing personal health information about me as set out above and in the written statement.

_____
Print Name

_____
Date

_____
Signature

WRITTEN PRIVACY STATEMENT
For the Information of Clients of the Norman Recollet Health Centre

The Norman Recollet Health Centre is a community health clinic and is a "health information custodian" for the purposes of Ontario's *Personal Health Information Protection Act* (PHIPA).

What Do We Collect?

In accordance with PHIPA, we collect Personal Health Information (PHI) about you directly from you or from the person acting on your behalf. The PHI that we collect may be in various forms and may include, for example, your contact information, date of birth, health history, family health history, records of your visits, lab results, and diagnostic imaging results. Occasionally, we collect PHI about you from other sources, if we have your consent to do so or if the law permits.

Our Privacy Commitment to You

The Health Centre is committed to protecting your privacy and ensuring the confidentiality of your Personal Health Information. We may collect, use and disclose Personal Health Information for the following purposes:

- To provide you with health care and assistance, both within and outside our health centre;
- To communicate or consult about your health care with your doctor(s) and other health care providers;
- To make arrangements for required medical transport;
- To plan, administer and manage the health centre's internal operations;
- To conduct quality improvement and risk management activities;
- To compile statistics;
- To fulfill other purposes permitted or required by law;
- To locate you or your family only in urgent/emergency situations.

The health centre uses a secure electronic system to share your health information with other health services providers that care for you so they have the most up-to-date and complete record of your health history and needs.

We will collect, use and disclose only as much PHI as is needed to achieve these purposes. You can withhold or withdraw your consent to the collection, use or disclosure of your PHI by contacting the Health Centre's Privacy Contact Person.

Your Rights and Choices:

You have the right:

- to see and receive a copy of your personal health information;
- to request a correction of your records if you believe there are errors;
- to receive more information about the health centre's Privacy Program by contacting the Privacy Contact Person; and
- to file a complaint with the Information Privacy Commissioner of Ontario if you believe that the health centre is non-compliant with PHIPA.

How to Reach Us

If you have questions or concerns about our privacy practices, or if you wish to access or correct your record, please speak to our Privacy Contact Person at:

Nurse Practitioner
190 Loonway Rd.
Capreol, ON, P0M 1H0

Privacy Commissioner of Ontario

You have the right to contact the Information and Privacy Commissioner of Ontario if you think the health centre has violated your rights. The Commissioner can be reached as follows:

Information and Privacy Commissioner/Ontario
Bloor Street East, Suite 1400
Toronto, Ontario, M4W 1A8
T: 416-326-3333 or 1-800-387-0073
www.ipc.on.ca

Reference: PHIPA, section 16.

PRIVACY CONTACT RESPONSIBILITIES:
Norman Recollet Health Centre

KNOWLEDGE

The privacy contact must be familiar with and remain current in:

- The duties and obligations of the health centre and the privacy contact under the *Personal Health Information Protection Act* (PHIPA);
- The health centre's policies and procedures;
- First Nation privacy laws, if applicable;
- General privacy principles and guidelines; and
- How to protect individual and community privacy in aggregate formats, such as community reports.

KEY RESPONSIBILITIES

The privacy contact should be actively handling the following responsibilities:

- Promotes staff compliance with PHIPA, including:
    - Identifying privacy compliance issues for the health centre,
    - Recommending when a privacy impact assessment is required,
    - Conducting an annual review to make sure current administrative, physical and technical safeguards protect the privacy of client records,
    - Assisting in developing and maintaining privacy, security and operational policies and procedures,
    - Making sure agents are aware of the responsibilities and duties under PHIPA and that they sign confidentiality agreements that are regularly updated,
    - Providing advice to staff and agents regarding privacy-related issues and PHIPA,
    - Identifying privacy training, assessment tools, and awareness opportunities for self and staff,
- Facilitates the health centre's compliance with PHIPA;
- Assists in ensuring the overall security and protection of information held by the health centre;
- Ensures that the health centre enters into appropriate agreements related to health information sharing, where required;
- Investigates and reports privacy breaches;
- Receives inquiries and complaints about possible PHIPA violations;
- Responds to questions from leadership and management regarding how PHI is managed, protected and disclosed;

- Together with senior management, reviews all privacy policies and procedures on a regular basis (e.g. every 2 to 3 years) to confirm they remain current and complete and revises as necessary to address identified gaps;
- Maintains a high-level view of the PHI that is collected, used and disclosed by staff delivering services on behalf of the health centre and ensures appropriate authorization for access are in place;
- Regularly monitors user access and activity to practices and clinical data by regular audits (e.g. at least annually) to ensure access is appropriate and initiates training and/or corrective actions when necessary;
- Responds to requests of an individual for access to or correction of a record of PHI about the individual;
- Assists to develop procedures and responds to client questions, complaints, access, and correction requests related to information practices;
- Establishes procedures to publish changes to existing privacy policies and procedures and new ones; and
- Champions the health centre's information practices to ensure alignment with other policies that might already be in place as a result of existing community activities such as Emergency Preparedness Planning.

Because of the management, supervisory and investigative role of the Contact Person, the Contact Person should be a management-level employee in the health-centre.

Reference: PHIPA, section 15.

POLICY FOR RETENTION, STORAGE AND DESTRUCTION OF PERSONAL HEALTH INFORMATION:
Norman Recollet Health Centre

RECORDS RETENTION

The Health Centre will ensure that client health records are retained for the minimum time required by the applicable professional standards in the health industry.

10 years after discharge if the clients is above 18 years old
If it is a child, it is 10 years after the age of 18 years old

DESTRUCTION OF RECORDS

The Health Centre will only destroy Personal Health Information (PHI) once its professional and legal obligations to retain the record has come to an end.

Health Centre Staff must obtain authorization from the Privacy Contact Person prior to the destruction of PHI.

Destruction of PHI must be conducted in a secure and confidential manner and in such a way that it cannot be reconstructed or retrieved. As such, the Health Centre must, where applicable:

- cross-shred all paper medical records;
- permanently delete electronic records by physically destroying the storage media or overwriting the information stored on the media; and
- destroy any back-up copies of records.

The Health Centre will document the secure destruction of PHI to assist in creating an audit trail for monitoring compliance. The document will include the following information:

- date of destruction;
- name, title, contact information, and department of the person submitting the authorization;
- description of the information or media being destroyed;
- quantity being destroyed;
- origination or acquisition year (can be a range);
- location of the records;
- reason for destruction;
- method of destruction;
- whether destruction is to be performed in-house;
- identity and contact information of the person conducting destruction, if relevant
- destruction method;

- witness to the destruction.

If a contractor is retained to conduct the secure destruction, the Health Centre must obtain a Certificate of Secure Destruction from the contractor indicating:
company name

- a unique serialized transaction number;
- the transfer of custody;
- a reference to the terms and conditions;
- the acceptance of fiduciary responsibility;
- the date and time the information ceased to exist;
- the location of the destruction;
- the witness to the destruction;
- the method of destruction;
- a reference to compliance with the contract (if employing a secure destruction service provider);
- signature.

STORAGE

The Health Centre must ensure PHI in its custody or control is stored in a safe and secure environment and in a way that ensures its integrity and confidentiality. Procedures will be implemented to address physical security (such as locked filing cabinets, restricted office access, alarm systems), technological security (passwords, encryption and firewalls),and administrative controls (security clearances, access restrictions, staff training and confidentiality agreements).

The Health Centre must ensure medical records are readily available and producible when access is required.

Additional Policies, Procedures and Best Practices (IPC)

Additional documentation is available through The Office of the Information and Privacy Commissioner (IPC).

The following is a list of documentation that may be of specific benefit to supporting PHIPA compliance:

IPC Documents
Best Practices for Secure Destruction of PHI (IPC)
Breach Notification Guidelines (IPC)
Fact Sheet on Communicating PHI by email (IPC)
Fact Sheet on Lock-Box (IPC)
Fact Sheet on Secure Disposal of Electronic Media (IPC)
Information Security Best Practices (IPC)
Privacy and Security Considerations for Virtual Health Care Visits (IPC)
Responding to a Health Privacy Breach (IPC)

REVISION HISTORY

Date (mm/dd/yyyy)	Motions