# Privacy Policy and Procedures

_____ Health Centre

**As of April, 2015**

## Table of Contents

Background....4

Contributors....4

Definitions....5

Responsibility....7

_____ Health Centre Privacy Contact Person....7

Legislative Framework....8

Health Centre Privacy Policy, Principles and Protocols....9

Procedure 1.0: Privacy Orientation and Training....17

Procedure 2.0: Displaying Privacy Contact Person's Information....21

Procedure 3.0: Communicating the Purpose of Information Gathering....24

Procedure 4.0: Individual Inquiries Regarding Handling of Personal Information....29

Procedure 5.0: Obtaining Consent for Collection, Use and Disclosure of Personal Information....30

Procedure 6.0: Disclosure of Private Information....441

Procedure 7.0: Storage and Disposal of Personal Information....464

Procedure 8.0: Security and Protection of Personal Information....46

Procedure 9.0: Accuracy and Information Correction....599

Procedure 10.0: Openness Regarding Privacy Policy Document....62

Procedure 11.0: Challenging Compliance....63

Procedure 12.0: Breach of Privacy or Security....67

| Forms/Tools | Page |
|---|---|
| Health Centre Privacy Orientation Checklist | 19 |
| Oath of Confidentiality | 20 |
| Privacy Contact Person Position Description | 22 |
| Notice of Purpose | 26 |
| Privacy Statement | 27 |
| Consent for Third Party to Release My Medical Records | 39 |
| Consent to Release My Personal Information to a Third Party | 40 |
| Request for Access to My Personal Information | 43 |
| Retention Schedule Template | 45 |
| Information Security Officer Responsibilities | 55 |
| Acceptable Use Policy | 56 |
| Employee Termination/Reassignment Action Item Checklist | 58 |
| Request to Correct Personal Information | 61 |
| Privacy Complaint Form | 64 |
| Privacy Breach Incident Report | 69 |

## Background

To better support clients and staff of the ___ Health Centre, hereinafter referred to as the Health Centre or Centre, this statement has been developed to outline the Centre's privacy policy and the protocols and procedures surrounding implementation.

## Contributors

This original privacy policy and procedures were developed in 2010 based on a facilitated process involving staff in each of the five Unama'ki health centres. The following individuals participated in the process:

- Stacey Lewis, *Representing the Tui'kn Partnership*
- Anita MacKinnon, *Eskasoni Community Health Centre, Eskasoni, NS*
- Sharon Rudderham, *Eskasoni Community Health Centre, Eskasoni, NS*
- Elaine Alison, *Wagmatcook Health Centre, Wagmatcook, NS*
- Ruth Fraser, *Wagmatcook Health Centre, Wagmatcook, NS*
- Anne MacDonald, *Wagmatcook Health Centre, Wagmatcook, NS*
- Mary Jessome-Pierro, *Wagmatcook Health Centre, Wagmatcook, NS*
- Jennifer MacDonald, Health Director, *Theresa Cremo Memorial Health Centre, Waycobah, NS*
- Mary Jessome-Pierro, *Theresa Cremo Memorial Health Centre, Waycobah, NS*
- Beverly Madill, *Potlotek Health Centre, Chapel Island, NS*
- Tanya Poulette, *Membertou Wellness Home, Sydney, NS*
- Susan Barrett, *Potlotek Health Centre, Chapel Island, NS*
- Angela Paul, *Membertou Wellness Home, Sydney, NS*

Legal input and comments were provided by Krista Yao, Nadjiwan Law Office in Ontario.

The policies and procedures were updated in 2014 in order to ensure that they are compliant with Nova Scotia's Personal Health Information Act (PHIA) which was enacted in June 2013. _____ Band, through its Health Centre, will be designated by the Province of Nova Scotia as a custodian effective _____, 2014.

Some sections of this document were adapted, with permission, from the Nova Scotia Department of Health and Wellness' *PHIA Toolkit*.

## Definitions

- **Aggregate** means a collection of items that are gathered together to form a total quantity.

- **Breach of privacy/confidentiality** means an intentional or inadvertent disclosure of confidential information contrary to applicable privacy policies and/or privacy laws.

- **Confidentiality** reflects the principle and ethics of limiting collection, use and disclosure of personal or sensitive information. Confidential information may relate to patient information, and also to all information not readily available to the public, including information regarding employees and the business affairs of the __Health Centre.

- **Custodian** means an individual or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's power or duties.

- **PHIA** means the Personal Health Information Act.

- **Personal information** means any information, recorded in any form, about an identified individual, or an individual whose identity may be understood or determined from such information.

  The following are examples of Personal information:

  a) An individual's name, address or telephone number;
  b) An individual's race, national or ethnic origin;
  c) An individual's age, sex, sexual orientation, marital status or family status;
  d) An identifying number, symbol or any other particular piece of identifying information assigned to an individual;
  e) Information about the individual's educational, financial, criminal or employment history;
  f) Anyone else's opinions about the individual; and
  g) The individual's personal views or opinions, even if they are about someone else.

- **Personal Health Information** is defined in PHIA as identifying information about an individual, whether living or deceased, and in both recorded and unrecorded forms, if the information:

  (i) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,

(ii) relates to the application, assessment, eligibility and provision of health care to the individual, including the identification of a person as a provider of health care to the individual,
(iii) relates to payments or eligibility for health care in respect of the individual,
(iv) 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,
(v) is the individual's registration information, including the individual's health-card number, or
(vi) identifies an individual's substitute decision-maker.

- **Privacy Contact Person** means the person designated by the ___Health Centre to maintain the confidentiality of all personal information in accordance with that centre's privacy policy.

- **Privacy Statement** means the document, available to clients and the public, which outlines how the Health Centre protects the collection, use and disclosure of an individual's personal information in accordance with ten privacy principles.

- **Privacy Policy** is the collection of Privacy Principles, Privacy Procedures and Privacy Protocols which together reflect how the Health Centre meets its responsibilities for protection of confidential information.

- **Privacy Principle** means an important underlying assumption required to help implement the privacy policy.
- **Privacy Procedure** means the outline of specific actions to be taken by specific individuals in order to implement the privacy policy and protocols.

- **Privacy protocol** means the high level rules of correct and responsible behavior required to implement the privacy policy.
- **Responsibility** means the obligation of the Health Centre to protect information entrusted to it as part of its mandate to serve patients, visitors, and staff who come through its doors.

- **Security** means the measures taken to protect personal information from unauthorized or unintentional loss, theft, access, use, modification or disclosure.
- **Security officer** means the person designated by the Health Centre security officer to manage the Health Centre's security program on a day-to-day basis.

## Responsibility

All Health Centre staff, visiting health team members, volunteers and others who are associated with the Health Centre have a role in maintaining the confidentiality of personal information accessed, handled, or viewed in the course of their work. These individuals are responsible for compliance with the Centre's privacy policy, its protocols and procedures, its ten guiding principles, and applicable privacy laws.

In the event of questions about access to personal information; the Health Centre's collection, use, management or disclosure of personal information; or the Centre's Privacy Policies, the Health Centre Privacy Contact Person, or his or her designate, should be contacted.

Communication of confidential Health Centre business information will be acceptable only in the performance of employee duties and responsibilities.

Obligations to maintain confidentiality of information will continue after employment/contract/association/appointment/volunteer duties/internships with the Health Centre concludes.

## _____ Health Centre Privacy Contact Person

The Health Centre's Privacy Contact Person is ___. (Insert contact information for the respective health director). In her absence, _____ (insert contact information of designate) has been designated to act as the alternate Privacy Contact Person.

*Role of Privacy Contact Person*

- The Privacy Contact Person is accountable for the Health Centre's compliance with the ten privacy principles, and applicable privacy laws.

- It is the responsibility of the Privacy Contact Person to:

    - Facilitate the Centre's compliance with PHIA, as applicable;
    - Ensure that all staff, volunteers and others working at the Centre are informed of their duties in relation to privacy and confidentiality and that each receives appropriate training;
    - Respond to inquiries about the Centre's information practices;
    - Respond to requests for access to an correction of records;

- Receive and process privacy complaints.

- The Privacy Contact Person will designate a delegate to, in his or her absence or by request, support the ongoing implementation of the privacy statement.

## Information Security Officer

The Information Security Officer is responsible for managing the Health Centre's information security program on a day-to-day basis. Specific responsibilities of the Information Security Officer are detailed on page 56. _____ (insert name of security officer) has been designated as the health centre's Information Security Officer.

## Legislative Framework

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to the collection, use, disclosure and destruction of employee information, where the employer is a federally-regulated entity, such as Bands.

The Personal Health Information Protection Act (PHIA) came into effect in Nova Scotia in 2013. PHIA regulates the collection, use, disclosure and destruction of personal health information. PHIA applies to regulated health professionals and to any group practice of health professionals.

Both PIPEDA and PHIA are based upon the same ten privacy principles described herein. However, both statutes, and particularly PHIA, contains more detailed privacy and security requirements for handling personal health information, and details certain situations where the requirements of this privacy policy may not apply.

This privacy policy shall meet or exceed the minimum requirements of applicable laws and regulations, and will be amended from time to time to reflect changes to the law and regulations.

The confidentiality of organizational information (information that is confidential to the Health Centre) is recognized and protected as a term of all employment and service contracts and by an Oath of Confidentiality that shall be taken and signed by those that may have access to information confidential to the Health Centre.

# Health Centre Privacy Policy, Principles and Protocols

The Health Centre will take all reasonable steps to maintain the confidentiality of all personal information in accordance with this privacy policy and applicable laws.

This privacy policy does not cover the collection of aggregate data from which the identity of an individual cannot be determined. This privacy policy outlines the Health Centre protocols and procedures pertaining to the collection of confidential information about an individual.

An individual includes:

1. Clients of the Health Centre – including any individual who may use or has used Health Centre services;
2. Staff – including any person who is or has submitted an application to work at the Health Centre
3. Individuals visiting the Health Centre or who may work or have worked at the Centre. Such individuals will include any person who contributes to the programs and services offered at the Health Centre including, but not limited to, staff, interns, students, chief and council, and volunteers.

## Ten Privacy Principles

The ten principles referenced below define fundamental privacy rights. Adopting these principles and implementing reasonable policies and procedures is the best way to protect personal information. The ten principles, their protocols, and their procedures include the following:

### 1. Accountability

#### Principle

Health Centre is responsible for personal information in its custody and/ to maintain the confidentiality of that information at all times. All Health Centre staff share in this responsibility.

#### Protocols

The Health Centre shall ensure that staff complete annual privacy training and sign an Oath of Confidentiality agreement indicating their knowledge ofand agreement to comply with the ten privacy principles.

The Health Centre shall make readily available specific information about its policy and procedures for the management of personal health information in its custody to members of the public and to clients of the Health Centre.

The Health Centre shall make the contact information of the Privacy Contact Person available on its website and on any promotional material used to inform the public and health centre clients about the policy. This information shall be available upon request.

The Health Centre is responsible for personal information in its custody and/or control, including the transfer or release of information to a third party in accordance with these privacy principles and applicable law.

The Health Centre will not misuse or wrongfully disclose personal information.

The Health Centre staff, including contractors, students, interns and visiting residents, are responsible for ensuring the confidential management of all information regarding an individual with which he/she is dealing, during every encounter and for following the procedures developed to ensure personal information is safeguarded.

## 2. Purpose of Information Gathering

### Principle

The Health Centre will gather personal information from the client, staff or individual for specific purposes.

### Protocols

The Health Centre will inform the individual providing the personal information about the purpose of its collection, use or disclosure at or before the time in which the information is collected

The Health Centre will clearly indicate the specific purpose(s) for which personal information is being collected. This may be done verbally or by using an admission or appointment form, poster or brochure.

The Health Centre will identify a clear process for addressing individual inquiries regarding the purpose(s) for which personal information is being requested or used.

The Health Centre will not collect more information than that which is needed for an identified purpose.

The Health Centre will obtain and record information only for a purpose that serves the needs of the individual from whom the information is being collected.

## 3. Obtaining Consent

### Principle

Knowledge and consent are required to collect, use or disclose personal information unless authorized by applicable privacy laws.

### Protocols

The Health Centre supports informed consent when collecting personal information. Therefore, anyone collecting personal information for use at the Health Centre shall clearly explain, to the individual providing the information, the purpose(s) for which the information is being collected. This will occur either at the time the information is being collected or before.

The Health Centre may seek consent after collection of information, but before use, in cases where the use of the information is for a purpose that was not previously identified.

The Health Centre understands that consent is only valid when it is voluntary. This means that the individual providing the information has the physical and mental capacity to provide consent, and that the client understands how their information will be used.

The Health Centre shall obtain consent prior to or at the time of collection. Consent shall also be obtained when a new use for the personal information is identified.

There are some exceptions where consent may not be required, such as: subpoenas/warrants, child abuse reporting, prevention of imminent harm, communicable diseases, emergency contacts, etc.

## 4. Limiting Collection

### Principle

The Health Centre will limit the amount and type of information collected to what is necessary for the identified purpose and to assure quality service.

### Protocols

The Health Centre will limit the amount and type of personal information collected to what is necessary to meet the identified need and purpose at the time of collection.

## 5. Limiting Use, Disclosure and Retention

### Principle

The Health Centre will not use or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as authorized by applicable law. Personal information will be retained only as long as necessary for the fulfillment of those purposes.

### Protocols

The Health Centre will use or disclose personal information only for the purpose(s) for which it was collected, unless consent is provided or unless use or disclosure is authorized by law.

The Health Centre will only keep personal information as long as necessary to satisfy the purposes of its collection

The Health Centre will document any new purpose for use of an individual's personal information

The Health Centre will retain personal information for 10 years after the last contact with the individual from whom the information was collected or 10 years after that individual's death and/or 10 years past the age of majority.

The Health Centre may identify information that should be retained beyond 10 years, or less than 10 years, for specific purposes. In such a case, that information must be secured and protected from a potential breach.

The Health Centre will adhere to standards used by professional associations and/or regulatory bodies regarding retaining specific information.

The Health Centre will adhere to standards used by external service provider organizations or community partners regarding retaining specific information.

The Health Centre will take the necessary steps to destroy, erase or make anonymous personal information it no longer requires or when the identified purpose for collection has been fulfilled.

The Health Centre will make clients aware that some disclosure between providers is necessary to provide an appropriate level of consultation and/or supervision or for purposes of continuity of care when providers change.

If a client wishes to specify that certain staff members or third parties not have access to his or her file or to part of his or her file, the client will be made aware of the possibility that their request may limit the service provided.

## 6. Accuracy

### Principle

Personal information collected by Health Centre must be as accurate, complete and up to date as its purposes require.

### Protocols

The Health Centre will create and maintain client records which are clear, concise, comprehensive, professional, and which serve to further the care of the client.

The Health Centre will take steps to minimize the possibility of using incorrect information when making a decision about the individual, when disclosing to third parties or when transferring information to another health centre or health care setting.

To ensure accuracy, the Health Centre will develop a process that will be used in situations where personal information needs to be corrected.

The Health Centre will document corrections or amendments to personal information.

## 7. Safeguards

### Principle

Health Centre will ensure that all appropriate steps are taken to protect the personal information in its care with appropriate safeguards.

### Protocols

As the legal owner of the personal information contained in client health records, the Health Centre shall take all reasonable precautions to secure the information against loss, fire, theft, defacement, tampering, access or copying by unauthorized persons.

The Health Centre will adopt appropriate security safeguards to provide necessary protection including physical measures, technological tools, and organizational controls.

The Health Centre will ensure that employees access the computers, files and other recorded information of the Centre only as authorized and required for the effective delivery of programs and services.

The Health Centre will provide all staff, visitors, and volunteers who may be dealing with personal information with appropriate training on the importance of maintaining the privacy and confidentiality of an individual's personal information.

## 8. Openness

### Principle

The Health Centre shall be open and transparent about the policies and procedures used to protect personal information.

### Protocols

The Health Centre will ensure policies and procedures relating to the management of personal information are developed and communicated using plain language principles so that they are easily understood by intended audiences.

The Health Centre will determine and implement strategies for communicating broadly with the community about the Centre's privacy policy in a way that demonstrates its commitment to open and transparent information sharing regarding its privacy policy, principles, protocols, and procedures.

## 9. Individual Access

### Principle

Individuals have a right to know if the Health Centre holds any of their personal information and they have a right to access and to correct that information.

### Protocols

The Health Centre shall establish a process to support the management of an individual's request for accessing, viewing or copying his/her own personal information.

An individual shall be able to challenge the accuracy and completeness of his or her personal information and have requests for corrections added to his or her file. When corrections are added to the file, they are recorded but the original is not altered so as to ensure a complete record.

An individual may not be permitted to access certain records if the record is a mixed record which also contains information personal to another individual, without that other individual's consent.

In some situations, where authorized by law, the Health Centre may limit disclosure of personal information to the individual; for example, where disclosure of a client's health record to the client may result in a risk of serious harm to the treatment or recovery of the individual.

## 10. Challenging Compliance

### Principle

Any individual has the right to challenge the Health Centre's compliance with any of the privacy principles referenced in this statement.

### Protocols

The Health Centre shall establish a process to address challenges to its compliance with the ten privacy principles and corresponding protocols outlined in the privacy policy.

The Health Centre Privacy Contact Person will review all complaints and, if one is found to be justified, the Privacy Contact Person will make appropriate changes to the health centre's policies and procedures.

The Health Centre will investigate all breaches of its privacy policy.

# Procedures, Forms and Tools

# Procedure 1.0: Privacy Orientation and Training

| | |
|---|---|
| **Procedure:** Steps to ensuring comprehensive orientation and training to the Health Centre's privacy policy | |
| **Related Forms/Tools:**<br><br>• Health Centre Privacy Orientation Checklist<br>• Oath of Confidentiality Form | **Approved**<br><br>By:<br><br>Date:<br><br>**Revision Date:** |

**Steps:**

The Health Centre's Privacy Contact Person or designate will coordinate privacy orientation and training.

Initial orientation to the Health Centre's privacy policy will be self-directed.

Anyone, including, but not limited to, staff, volunteers, visiting medical professionals, and students, responsible for recording, viewing, or accessing personal information at the Health Centre shall complete the self-directed privacy orientation.

After completion of the privacy orientation, each participant shall sign and date the Health Centre Privacy Orientation Checklist and the Oath of Confidentiality.

All signed and dated copies of the Privacy Orientation Checklists and the Oaths of Confidentiality must be recorded and filed at the Health Centre.

All participants must be asked, prior to signing the Privacy Orientation Checklist, if they have understood what is expected of them and if they have any questions or concerns regarding their roles and responsibilities with respect to Health Centre's privacy policy.

If concerns are raised, the Health Centre Privacy Contact Person will document those concerns in a file designated for notes and follow up regarding privacy training.

A binder with the Privacy Policy will be kept in a central location in the Health Centre and will be easily accessible for everyone, including members of the public.

In-depth privacy training will be scheduled within one year of approval of the privacy policy and will be repeated annually, as required.

The Health Centre privacy training session will include all elements of the privacy document and will, at a minimum, include the following learning outcomes:

1. Understand the ten privacy principles;
2. Define the key terms contained in the privacy policy;
3. Discuss the importance of complying with the Health Centre's privacy policy and PHIA, and the implications if anyone is found to be in breach of the policy;
4. Clarify what personal information is being collected and why;
5. Review all privacy protocols, procedures and forms/tools associated with the privacy policy, and
6. Know the contact information of the Health Centre's Privacy Contact Person.

Additional training is available through Health Canada's online privacy training modules and is strongly recommended.

# Health Centre Privacy Orientation Checklist

I, _____, of the _____Health Centre, acknowledge and do solemnly swear/affirm that I have completed the required ____Health Centre Privacy Policy Orientation Checklist and understand that I am responsible to comply with the __Health Centre Privacy Policy, its principles and procedures.

I further understand that I am responsible for the safe handling, storage of all private information and in the appropriate conveyance of that information to individuals who come to the __Health Centre to receive care.

| | **Activity** | **Initial Upon Completion** |
|---|---|---|
| 1 | Read the Health Centre Notice of Purpose and the Privacy Statement. | |
| 2 | Read the 10 privacy principles of the *Personal Information Protection and Electronic Documents Act.* (pp. 9-10 of the health centre's Privacy Policy and Procedures) | |
| 3 | Read the definitions contained in the privacy policy document. (pp. 5-6) | |
| 4 | Read the privacy protocols related to each of the 10 privacy principles. (pp. 9-10) | |
| 5 | Read the privacy procedures outlined in the privacy policy document. (pp. 16-71) | |
| 6 | Review the forms/tools associated with the privacy policy document. (pp. 16-71) | |
| 7 | Note and record the contact information of the health centre's Privacy Contact Person. (p. 7) | |
| 8 | Read and sign the Health Centre's "Oath of Confidentiality" form (p. 20) and give the original copy to the health centre's Privacy Contact Person. | |
| 9 | Read and sign the "Health Centre's Acceptable Use" policy (pp. 56-57) and give the original copy to the health centre's Privacy Contact Person. | |
| 10 | Complete and sign this "Privacy Orientation Checklist" and give the original copy to the health centre's Privacy Contact Person. | |

Name _____

Signature _____

Sworn at _____, in the Province of Nova Scotia, this day ____ of

_____, 20____

Witnessed by _____

# Oath of Confidentiality

Anyone, including, but not limited to, staff, volunteers, visiting medical professionals, and students are responsible to protect and care for all ____Health Centre information and property entrusted to them.

I acknowledge and solemnly swear/affirm that I will keep absolutely confidential any and all knowledge and information, of which I have access due to my position/role at the _____Health Centre.

I will not, without due authority, discuss with any other person or persons either by word or letter or other forms of communication any matter directly or indirectly involving the private information of a ____Health Centre patient or involving the ____Health Centre's private affairs.

I understand that my obligations to maintain confidentiality herein shall survive the expiry or termination of my employment, contract or association with the _____ Health Centre, and are binding upon me forever.

Name _____

Signature _____

Sworn at _____, in the Province of Nova Scotia, this day

_____ of _____, 20_____

Witnessed by _____

# Procedure 2.0: Displaying Privacy Contact Person's Information

| **Procedure:** The importance and method of displaying the contact information of the Health Centre Privacy Contact Person | |
|---|---|
| **Related Forms/Tools:**<br><br>• Privacy Contact Person's Duties | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

Health Centre will identify an easily accessible, clearly visible space on its website for its privacy policy information and will add the names and contact information of its Privacy Contact Person and his/her designate to that space.

The Health Centre will make the Privacy Contact Person's contact information public through means appropriate for the Health Centre. This may include a letter to patients, a poster displayed in the Health Centre patient waiting area, or a brief update in Health Centre newsletters.

If the contact information of the Health Centre Privacy Contact Person changes, the Health Centre will make the new contact information public through means appropriate for the Health Centre.

The names and contact information of the Privacy Contact Person and his/her designate will be provided to patients and community members via appropriate outgoing material including, but not limited to, brochures and letters providing updates and news about the Health Centre.

The Health Centre's Privacy Contact Person will be responsible to ensure that his or her contact information, and that of his or her designate, remains accurate and up to date on all Health Centre material highlighting this information.

# Privacy Contact Person's Responsibilities

The Privacy Contact Person will be responsible for the following duties as they relate to the Health Centre's privacy policies and procedures.

The Privacy Contact Person shall appoint a designate, as required, to support adherence to the Health Centre privacy policy.

The Privacy Contact Person or designate will:

- Ensure that the Health Centre is in compliance with its privacy policies, its ten principles, and its procedures.

- Respond to and investigate complaints regarding privacy breaches as well as any challenges made regarding the Health Centre's compliance with any of its privacy principles.

- Make his or her name and contact information available to the public in relation to his or her role as Privacy Contact Person.

- Ensure all persons working for the Health Centre are informed about their roles and responsibilities under the Privacy Policy.

- Respond to an individual's request to access or correct their personal information.

- Respond to questions regarding the Centre's privacy policy, principles, protocols and procedures.

- Monitor and support public awareness campaigns in relation to creating a broad understanding about the Health Centre's privacy policies and its collection of confidential information.

- Update Health Centre staff, volunteers, visiting medical professionals, and students about revisions to the privacy policy, procedures and forms.

- Meet the requirements of PHIA for the designated privacy contact person, which shall include:

    - facilitate the health centre's compliance with PHIA;
    - ensure that all agents of the health centre are appropriately informed of their duties under PHIA;
    - respond to inquiries about the health centre's information practices;
    - respond to requests for access to and correction of records;
    - receive and process complaints under PHIA;

- facilitate the communications to and the training of the health centre’s staff about the health centre’s policies and procedures and about PHIA; and
- develop information to explain the organization's policies and procedures.

# Procedure 3.0: Communicating the Purpose of Information Gathering and Details of Information Management

| | |
|---|---|
| **Procedure:** How to communicate the purposes of gathering personal information | |
| **Related Forms/Tools:**<br><br>Notice of Purpose<br><br>Privacy Statement | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

The Health Centre will develop a Notice of Purposes, as described in PHIA, s.15, which provides enough information to individual clients to understand:

• why their personal health information is being collected;
• how it will be used;
• why it would be disclosed;
• the individual's rights under the Act;
• where the individual can obtain more information about the Act; and
• how the individual can make a complaint or ask for a review under the Act.

The Notice of Purposes will be made accessible to all Health Centre patients and to members of the public who may access the services of the Health Centre.

If a client has limited ability to read or understand the Notice of Purposes, the Health Centre will make reasonable efforts to assist with the individual's understanding of the purpose. This may include verbally explaining the purpose to the individual, or facilitating an explanation – verbally or in writing – in the individual's language.

The Health Centre will also develop a written privacy statement, as described in PHIA s.68, which will explain:

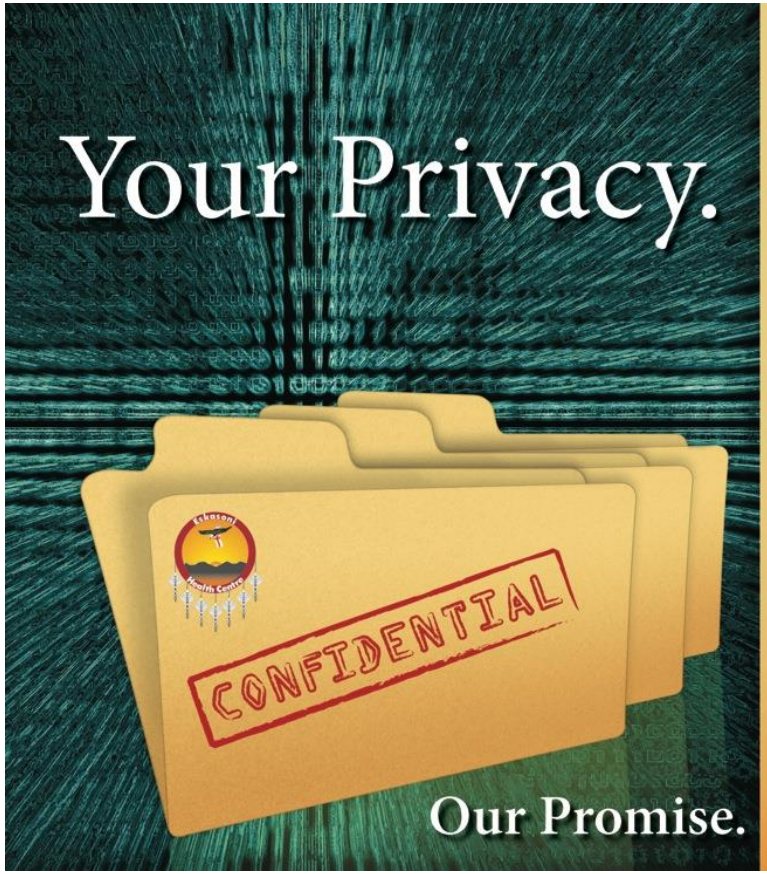
- the health centre's information practices;
- how to contact the health centre's privacy contact person;
- how to obtain access to or request correction of a record;

- and how to make a complaint under PHIA to the health centre and to the Privacy Review Officer.

The written privacy statement will be made available to the public by placing it on the health centre's website. Hard copies of the document will also be made available upon request.

If questions arise and the person collecting the information cannot answer those questions, that person will direct the patient to the Privacy Contact Person or designate.

If a patient refuses to provide personal information, the patient will be directed to the privacy contact person or designate.
The contact information of the privacy contact person or designate will be highlighted for all patients when their personal information is being collected.




## WHAT IS THE PERSONAL HEALTH INFORMATION ACT?

The Personal Health Information Act or PHIA is a new provincial law. It aims to balance your right for your personal health information to be protected, with the need of health professionals to use your information to provide you with proper care and treatment.

## WHAT IS PERSONAL HEALTH INFORMATION?

Personal health information is information about you that is related to your health or health care. It may include:

- your name;
- address;
- date of birth;
- health history;
- provincial health card number;
- other information about tests, procedures and care you received.

As your health services team, we collect personal health information directly from you (or the person acting on your behalf). Sometimes, we ask other health professionals or health care organizations involved in your health care for your personal health information to help us provide you care. We may collect personal health information from other sources, if we have your permission to do so, or if the law allows us to do so even without your permission. Personal health information may be collected and stored in different ways, including electronic files, on paper charts and images like x-rays. We collect personal health information as needed to treat you and assist with your health care.

## WHO CAN SEE OR USE YOUR PERSONAL HEALTH INFORMATION?

- individuals involved in your care and treatment, including health professions students (ex: student doctors and nurses), on a need to know basis or if the law allows us to do so even without your permission (for example, we are required by law to report things like immunizations, child abuse, elder abuse)
- individuals who need the information to get payment for your health care
- anyone who can legally act on your behalf
- specified organizations who have a legal right to see the information in certain situations

## HOW DOES PHIA PROTECT YOUR PERSONAL HEALTH INFORMATION?

As your health services team, we have policies and practices to protect your personal health information. We will:

- properly collect, use, share, keep and destroy your personal health information following the rules in PHIA
- have a privacy contact person who can answer your questions about our handling of your personal health information
- have policies to protect the privacy and security of your personal health information on paper, in electronic form, or unrecorded
- have a complaints policy for you to use if you believe that we are not following the rules in PHIA
- properly respond if the privacy of your personal health information has been breached. This may include telling you or the Privacy Review Officer.

## WHAT ARE YOUR RIGHTS UNDER PHIA?

- to ask for copies of your personal health information (fees may apply);
- to ask for changes to your personal health information if the facts were not recorded correctly;
- to ask for information on who has looked at your personal health information held in electronic form;
- to ask that some or all of your personal health information not be collected by, used by, or shared with specific people or organizations involved in your care;
- to ask for a review by the Privacy Review Officer responsible for PHIA if you do not think the result of your complaint, access request, or correction request properly followed the rules in PHIA.

## WHO TO CONTACT FOR MORE INFORMATION?

This poster is a summary of your rights and our responsibilities under PHIA. There are specific exceptions to these rights and responsibilities.

***If you need more information, please ask our Health Centre's PHIA contact person:***

**Sharon Rudderham**
Eskasoni Community Health Centre
44 Spencer's Lane / P.O. Box 7745
Eskasoni, NS B1W 1B3
(902) 379-3200 (phone)
(902) 379-2421 (fax)
srudderham@eskasonihealth.ca
**www.eskasonihealth.ca**

Notice of Purpose

# Written Privacy Statement



## Your Privacy. Our Promise.

### THE PERSONAL HEALTH INFORMATION ACT

The Personal Health Information Act (PHIA) came into force in June 2013. This new provincial health information privacy and access legislation is intended to ensure that personal health information management rules in the health sector are clear, consistent and relevant to all records of personal health information, including the electronic health information systems being implemented in Nova Scotia.

PHIA balances your right to have your privacy protected with the need of the health sector – including our organization – to collect, use and disclose it to provide appropriate care and service to you.

As a "custodian" of personal health information under PHIA, we have an obligation to protect the privacy of the information we collect, use and disclose about you. This brochure is a summary of the purposes for our management of your personal health information.

### WHAT IS "PERSONAL HEALTH INFORMATION"?

Personal health information is identifying information about you, and includes demographic information (name, address, date of birth), your health card number, information related to your physical and mental health care, and financial information related to your application and eligibility for health care services. Personal health information can be recorded and unrecorded, and continues to be protected after you are deceased.

### DO I NEED TO CONSENT TO THIS DISCLOSURE?

This disclosure is carried out under the principle of "knowledgeable implied consent". This means that we have to provide you sufficient information about the purposes for collecting, using and disclosing your personal health information, and about your right to give or withhold consent. In addition to the information contained in this brochure, you may ask for additional information about the management of your personal health information.

If you continue to seek our services, we can assume your consent to our use and disclosure of your personal health information for your health care.

### CAN I DECIDE WHO CAN AND CAN'T HAVE ACCESS TO MY PERSONAL HEALTH INFORMATION?

You have the right to request that your personal health information not be used or disclosed by a specific health professional or organization. We are required to:

- take reasonable steps to comply with your request
- advise you of any consequences of your request (e.g. one of your health professionals may not be confident that they have sufficient information to provide care to you)
- advise anyone to whom your personal health information is disclosed that the information is not complete
- advise you that we cannot comply with your request where the information is required by law to collect, use or disclose

### HOW DO I REQUEST THAT MY PERSONAL HEALTH INFORMATION NOT BE USED OR DISCLOSED?

A form is available from our PHIA/Privacy contact person.

**Your PHIA/Privacy contact person is the Health Director, Sharon Rudderham**

For more information about our privacy protection practices, or to discuss them, contact us at:
Eskasoni Community Health Centre
44 Spencer's Lane
P.O. Box 7745
Eskasoni, NS B1W 1B3
(902) 379-3200 (phone)
(902) 379-2421 (fax)
srudderham@eskasonihealth.ca

# PROTECTING YOUR PERSONAL HEALTH INFORMATION

### WHY DO YOU COLLECT MY PERSONAL HEALTH INFORMATION?

We collect it for several purposes:

- to inform our decisions related to appropriate health care for you
- to disclose to other providers involved in your health care
- to ensure that all custodians receive appropriate payment for delivering care (e.g. services that are insured for you through the Department of Health and Wellness)
- to conduct research approved under PHIA
- to plan and manage health care services for you and others in Nova Scotia
- for other purposes required or permitted by law

### WHEN DO YOU DISCLOSE MY PERSONAL HEALTH INFORMATION TO OTHERS?

The personal health information we collect from you is used within our organization to provide appropriate care to you. Anyone in our organization who is required to review your personal health information would have access to it.

We may disclose it to health professionals outside of our organization if they are in the "circle of care" for your illness or injury. This information would enable them to provide appropriate care to you.

### CAN I REQUEST A COPY OF MY PERSONAL HEALTH INFORMATION?

Yes. You have the right to request a copy of your personal health information, or request an opportunity to view your personal health information. There are limited exceptions to what you cannot access, including information that was collected during an investigation or information that includes the personal information of another person.

We are permitted to charge you a prescribed fee for providing you with a copy of your record or an opportunity to view your record. We can provide you with the fee schedule.

### CAN I REQUEST THAT SOMETHING IN MY PERSONAL HEALTH INFORMATION BE CORRECTED?

Yes. You may make the request to our PHIA/privacy contact person. There are limited exceptions to your right to a correction of your record, including when the information you request to be corrected is part of a health practitioner's professional opinion.

### WHAT HAPPENS IF YOU LOSE MY PERSONAL HEALTH INFORMATION OR SOMEONE WHO ISN'T AUTHORIZED TO SEE IT GAINS ACCESS TO IT?

If your personal health information is breached and we believe that this breach may cause you harm or embarrassment, we are required to notify you of the breach. If we don't notify you, we are required to notify the Review Officer for PHIA.

### CAN I MAKE A COMPLAINT IF I THINK YOU HAVE NOT FOLLOWED THE RULES IN PHIA?

Yes. Our organization has a PHIA complaints process. Our PHIA/privacy contact person can provide you with the necessary information and form.

### WHAT IF I AM NOT HAPPY WITH THE WAY YOUR ORGANIZATION HAS HANDLED MY COMPLAINT?

You may request a review under PHIA. The Review Officer for PHIA can be reached at:

Review Officer, Personal Health Information Act
P.O. Box 181
Halifax, Nova Scotia B3J 2M4
Phone: 902-424-4684
Toll-free: 1-866-243-1564
Fax: 902-424-8303

# Procedure 4.0: Individual Inquiries Regarding Handling of Personal Information

| | |
|---|---|
| **Procedure:** How to address individual inquiries regarding the handling of personal information | |
| **Related Forms/Tools:**<br><br>N/A | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

Anyone inquiring with the Health Centre about the purposes for which their personal information is being requested, may do so with the person collecting the information. That person representing the Health Centre shall be prepared and able to answer questions regarding the Health Centre privacy policies.

The person making the inquiry is within his or her rights to ask to speak specifically to the Health Centre's privacy contact person or designate. If this happens, the contact information of the privacy contact person/designate will be provided to the person making the inquiry.

A program supervisor may act on behalf of the privacy contact person/designate within the Health Centre to respond to inquiries regarding the handling of personal information. If this happens, the program supervisor will keep the privacy contact person/designate informed about the outcome of the inquiry.

If the person making the inquiry wishes to discuss the details of his or her specific situation, they will need to provide written permission to the privacy contact person/designate/program supervisor to review his or her file and obtain specific answers to the question(s). This may require seeking the help of appropriate medical staff.

# Procedure 5.0: Obtaining Consent for the Collection, Use, and Disclosure of Personal Information [1]

| | |
|---|---|
| **Procedure:** How to handle consent issues related to the collection, disclosure and use of personal information at the Health Centre. | |
| **Related Forms/Tools:**<br><br>• Consent for Third Party to Release My Medical Records<br>• Consent to Release My Personal Information to a Third Party | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

*Note: This procedure deals with consent related to the collection, use and disclosure of personal health information and not consent to treatment. PHIA has not changed the rules around consent to treatment.*

**Consent:**

There are three primary models of consent to the collection, use and disclosure of personal health information:

1. express consent;
2. implied knowledgeable consent; and
3. no consent.

Consent must be obtained from an individual if a custodian is collecting, using or disclosing the individual's personal health information unless the collection, use or disclosure is permitted without consent or required without consent by PHIA.

**General Rules of Consent:**

Under PHIA, consent for the collection, use or disclosure of personal health information, whether express consent or knowledgeable implied consent, must meet the following requirements:

[1]The Health Centre's consent procedures are adapted with permission from the Nova Scotia Department of Health and Wellness' PHIA Toolkit.

- it must be given by the individual;
- it must be knowledgeable;
- it must be related to the specific information at issue; and
- it must be voluntary.

**Knowledgeable Implied Consent**

For the purpose of providing health care or assisting in the provision of health care to an individual, PHIA permits most custodians to rely on knowledgeable implied consent to collect, use and disclose personal health information.

Consent is "knowledgeable" when it is reasonable in the circumstances to believe that:

- the individual knows the purpose of the collection, use or disclosure, as the case may be; and
- the individual knows that s/he may give or withhold consent.

If the individual then proceeds to pursue services, the custodian may infer that the individual is consenting to the collection, use and/or disclosure of the personal health information.

To ensure that consent is "knowledgeable," the Health Centre will post a "Notice of Purpose" describing the purpose of the collection, use and disclosure of personal health information at the Health Centre (as described in Procedure 3). The Notice of Purpose will be posted in waiting areas, exam rooms and other areas where it is visible to clients.

Posting a Notice or Purpose is not sufficient, if there's reason to believe that an individual cannot read or cannot understand the notice. If it is determined that an individual requires assistance understanding the notice, the Health Centre will assist the individual by using an interpreter (if available), or explaining the information in the notice directly to the individual as best as possible.

**Express Consent**

Express consent is "voluntary agreement with what is being done or proposed that is unequivocal and does not require any inference on the part of the organization seeking consent." [2] Express consent can be written or oral. Under PHIA, express consent of an individual is required if their personal health information is to be **collected** and **used** for fund-raising activities as well as for market research and marketing any service for a commercial purpose.

[2] *COACH Guidelines for the Protection of Health Information* (December 15, 2006) at p. 332. COACH is Canada's health informatics association. See www.coachorg.com or the Appendix 4: *Resources* section for information about purchasing the *Guidelines.*

In accordance with PHIA, the Health Centre is required to obtain express consent for the **disclosure** of personal health information in the following situations:

- by a custodian to a non-custodian (unless required or authorized by law);
- by a custodian to another custodian if it is not for the purpose of providing health care (unless required or authorized by law);
- for fund-raising activities;
- for market research or marketing any service for a commercial purpose;
- to the media;
- or to a person or organization for the purpose of research (certain exceptions apply; see Chapter 7 of the PHIA Toolkit).

In these situations, express consent will be obtained by having the client complete either the "Consent for Third Party to Release My Medical Records" form or the "Consent to Release My Personal Information to a Third Party" form, whichever form is appropriate given the specific circumstance.

**Circle of Care**

The term "circle of care" is defined as:

> *"Individuals and activities related to the care and treatment of a patient. Thus, it covers the health care providers who deliver care and services for the primary therapeutic benefit of the patient and it covers related activities such as laboratory work and professional or case consultation with other health care providers."* [3]

The term "circle of care" refers to the health information custodians who provide or support care to an individual in each instance of care provision.

The "circle of care" allows the Health Centre to assume an individual's knowledgeable implied consent to collect, use or disclose personal health information for the purpose of providing health care, unless the Health Centre knows that an individual has expressly withheld or withdrawn consent.

Under the "circle of care," it does not matter whether care and treatment is provided in the private or public sector, or that services are publicly insured or not insured – the personal health information will follow the individual where s/he goes in the health care system.

However, the information may only be disclosed by the Health Centre to another health information custodian (or his/her agent) within the circle of care. If the individual is also receiving care and treatment from a person or organization not

[3] Industry Canada, *PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector, Questions and Answers*, question 12. Available at http://www.ic.gc.ca/eic

designated as a custodian under *PHIA*, express consent must be obtained from the individual.

Finally, it is important to remember that a circle of care is different for each instance of care provision.

**Withdrawal of Consent**

An individual may request to limit or revoke consent for the collection, use or disclosure of their personal health information in the custody or control of the Health Centre by giving notice to the Health Centre. In the context of electronic health records, this limitation or withdrawal of consent is often referred to as a "lockbox"; the terms "consent directives" and "masking" are also used in reference to both paper and electronic records.

An individual may request to limit or withdraw his/her consent at any time, but it is not retroactive. This means that if an individual informs the Health Centre that s/he is withdrawing consent to have information disclosed to one of their health providers, the Health Centre is not required to request that any information previously disclosed to the other provider be returned.

However, the Health Centre must inform the provider named by the individual that the individual's record is not complete, meaning the Health considers that the information disclosed to that provider is not what is "reasonably necessary" for the care of the individual.

The Health Centre must also inform the individual of the consequences of limiting or revoking consent, including the fact that the other provider may decide that s/he is not confident in providing care to the individual without understanding what information has been withheld.

The Health Centre is required to take reasonable steps to comply with an individual's request to limit or withdraw consent. Each individual circumstance will determine what is reasonable.

The withdrawal of consent does not apply to collection, use and disclosure of personal health information that the Health Centre is required by law to collect, use or disclose.

**Capacity to Consent**

For the consent of an individual to be valid, the individual must have the capacity to consent. In the context of PHIA, capacity means:

- the ability to understand information that is relevant to the making of a decision related to the collection, use or disclosure of personal health information and

- the ability to appreciate the reasonably foreseeable consequences of a decision or a lack of a decision.

Any capable individual, regardless of age, may consent or withdraw consent for the collection, use or disclosure of their personal health information. The capacity of an individual must be considered in each instance consent is being sought. An individual may have the capacity at a particular time to consent to the collection, use or disclosure of some parts of personal health information, but may be incapable of consenting at another time.

Where an individual is deemed to have the capacity to consent to the collection, use and disclosure of personal health information, such consent includes disclosure to a parent, guardian or substitute decision-maker where applicable.

**Mature Minors**

Under the provincial *Age of Majority Act*, a person ceases to be a minor when they reach the age of nineteen years. This age is recognized by some provincial legislation, while other provincial legislation provides for benefits and rights when an individual reaches a younger age.

*PHIA* recognizes the common-law principle of "mature minors," which recognizes that the capacity to consent is incremental and situational. The capacity of each individual minor must be considered in the context of each episode of care. A 17-year-old may have the capacity to consent to (or withhold) disclosure of information related to one issue while lacking the capacity to consent to disclosure related to another.

**Substitute Decision-Maker**

Where an individual lacks the capacity to consent or refuses the collection, use and disclosure of personal health information, a substitute decision-maker may make that decision on behalf of the individual. PHIA outlines the following hierarchy of substitute decision-makers:

(a) a person who is authorized by or required by law to act on behalf of the individual;

(b) the individual's guardian appointed by a court of competent jurisdiction;

(c) the spouse of the individual;

(d) an adult child of the individual;

(e) a parent of the individual;

(f) a person who stands in loco parentis to the individual;

(g) an adult sibling of the individual;

(h) a grandparent of the individual;

(i) an adult grandchild of the individual;

(j) an adult aunt or uncle of the individual;
(k) an adult niece or nephew of the individual;
(l) any other adult next of kin of the individual;
(m) the Public Trustee of the Minister of Aboriginal Affairs and Northern Development Canada.

**When Consent Is Not Required**

Under PHIA, there are some circumstances where personal health information may be collected, used or disclosed without consent.

In accordance with PHIA. The Health Centre may **use** an individual's personal health information without consent in the following circumstances (note that "use" does not include "disclosure"):

- for planning or delivering programs or services that the Health Centre provides or that the Health Centre funds in whole or in part, allocating resources to any of them and evaluating or monitoring any of them;
- for detecting, monitoring, or preventing fraud or any unauthorized receipt of services or benefits related to any of them;
- for the purpose of ensuring quality or standards of care within a quality review program of the Health Centre. Note: it cannot be a review initiated by an individual employee of the Health Centre;
- for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual;
- for the purpose of seeking the individual's consent when the personal health information used by the Health Centre for this purpose is limited to the individual's name and contact information;
- for the purpose of a proceeding or a contemplated proceeding in which the custodian or an agent or former agent of the Health Centre is, or is expected to be, a party or witness, if the information relates to or is a matter in issue in the proceeding or contemplated proceeding;
- for the purpose of obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services;
- for research conducted by the Health Centre in accordance with sections 52 to 60 of PHIA (see Chapter 7 of the PHIA Toolkit);
- subject to requirements and restrictions, if any, that are prescribed, if permitted or required by law or by a treaty, agreement or arrangement made under PHIA or another *Act* of the Province or of the Parliament of Canada; or

- for the purpose of risk management or patient safety within the Health Centre.

Under PHIA, the Health Centre may provide personal health information to an agent to use for any of the above purposes. Agents include employees, volunteers, or the custodian's lawyer.

Under PHIA, the Health Centre may **disclose** personal health information without an individual's consent in specific circumstances (for a complete list, see chapter 5, pages 10-19 of the PHIA Toolkit). Below are some examples:

- to another custodian if the custodian disclosing the information has a reasonable expectation that the disclosure will prevent or assist an investigation of fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of a province or the Parliament of Canada;
- to persons acting on behalf of the individual including:
    - a person who is legally entitled to make a health-care decision on behalf of the individual;
    - a legal guardian; or
    - the administrator of an estate, if the use or disclosure is for the purpose of the estate.
- to a regulated health profession body or a prescribed professional body that requires the information for the purpose of carrying out its duties in the Province under an *Act* of the Province or in another province of Canada under an *Act* of that province regulating the profession;
- to any person if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize an imminent and significant danger to the health or safety of any person or class of persons;
- to an official of a correctional facility, as defined in the *Correctional Services Act*, or to an official of a penitentiary, as defined in the *Corrections and Conditional Release Act (Canada)* in which the individual is being lawfully detained if the purpose of the disclosure is to allow the provision of health care to the individual or to assist the correctional facility or penitentiary in making a decision concerning correctional services as defined in the *Correctional Services Act* or services provided under in the *Corrections and Conditional Release Act (Canada);*
- to another custodian for the purpose of ensuring quality or standards of care within a quality review program within the custodian's organization;
- to the Nova Scotia Prescription Monitoring Board for monitoring prescriptions pursuant to the *Prescription Monitoring Act;*
- subject to the requirements and restrictions, if any, that are prescribed, if the disclosure is required or permitted by law or a treaty, agreement or

arrangement made pursuant to PHIA or another *Act* of the Province or the Parliament of Canada. Provincial legislation requiring mandatory disclosure of health information includes the Adult Protection Act, the Health Protection Act, the Gunshot Wounds Mandatory Reporting Act, and the Children and Family Services Act or verifying an individual's eligibility for insured services;

- the disclosure is reasonably necessary for the administration of payments in connection with the provision of health care to the individual or for contractual or legal requirements in that connection;
- for the purpose of risk management or patient safety within the custodian's organization

A disclosure of personal health information without the individual's consent must be documented. The documentation must include:

- a description or copy of the personal health information disclosed;
- the name of the person or organization to whom the personal health information was disclosed;
- the date of the disclosure; and
- the authority for the disclosure.

In circumstances where disclosure without consent is permitted by PHIA, the Health Centre is not obliged to disclose information to a third party unless required to do so under another law or enactment. In addition, the Health Centre may choose to obtain the individual's consent for the disclosure or give notice to the individual of the disclosure.

**Disclosure to Family Members**

Under PHIA, the Health Centre has the discretion to disclose personal health information related to the presence, location and general condition of an individual on the day that the information is requested to:

- family members of the individual; or
- another person if the custodian has a reasonable belief that the person has close personal relationship with the individual.

A custodian may not disclose this information if it is contrary to the express request of the individual.

**Disclosure of Personal Health Information Related to a Deceased Person**

In accordance with PHIA, the Health Centre may release information about an individual who is deceased, or believed to be deceased for the following purposes.

- for the purpose of identifying the individual;
- for the purpose of informing any person whom it is reasonable to inform that the individual is deceased or believed to be deceased;
- to a spouse, parent, sibling, or child of the individual if the recipient of the information reasonably requires the information to make decisions about the recipient's own health care or the recipient's children's health care and it is not contrary to a prior express request of the individual;
- for carrying out the deceased person's wishes for the purpose of tissue or organ donation.

If the information relates to circumstances surrounding the death of the individual or to health care recently received by the individual and the disclosure is not contrary to a prior express request of the individual, the Health Centre may disclose personal health information about a deceased individual to:

- a family member of the individual; or
- another person if the Health Centre has a reasonable belief that the person has a close personal relationship with the individual.

# Consent for Third Party to Release My Medical Records

I, _____hereby authorize the release of my medical

records from _____

to _____Health Centre.

Name _____

Address _____

_____

Health Card # _____

Date of Birth _____

My authorization for release is limited to the following records (please be as specific as possible; include time periods/dates if relevant):

_____

_____

_____

_____

Signature _____

Date _____

Witness _____

Date _____

# Consent to Release My Personal Information to a Third Party

Patient's name: _____

Address: _____

Date of Birth: _____

Health Card: _____

I hereby request and authorize _____

Of _____

To release the following information:

My authorization for release is limited to the following records (please be as specific as possible; include time periods/dates if relevant):

_____

_____

_____

_____

To _____

_____
Witness

_____
Signature of Patient

_____
Date

# Procedure 6.0: Disclosure of Private Information

| **Procedure:** Steps involved in disclosing private information | |
|---|---|
| **Related Forms/Tools:**<br><br>• Request for Access to My Personal Health Information Form<br>• | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

The Health Centre will closely control the release of all confidential information. A properly completed and signed consent form is required for release of any private health information, except in limited circumstances (see procedure 5 in this document as well as chapter 5 of the PHIA Toolkit).

All requests for release of information should be directed to the Health Centre Privacy Contact Person or designate. A nursing staff representative or medical secretary may receive and process requests for release of information if deemed acceptable by the Privacy Contact Person or designate.

The release of information will be carried out in accordance with all applicable legal and regulatory requirements and legislation.

Information released to authorized agencies/individuals shall be limited to that which is required to fulfill the purpose stated on the consent form. Release of information not essential to the stated purpose of the request is strictly prohibited.

Requests for health information received via telephone calls shall be limited to persons or agencies participating in the health care of the patient and shall be supplied only after rigidly applied means of identification to assure that the requesting party is entitled to receive such information.

A record of all requests and disclosures of personal health information shall be kept on each client's file at the Health Centre.

By law, health care providers are required to report cases of child abuse, suspected child abuse, suspected abuse or neglect of adults. Neither the Health

Centre nor its employees shall be held liable for releasing information in good faith, where required by law.

An individual has the right to request the accessing, viewing or copying of his or her personal information. Authorization for release of that information, using the Request for Access to My Personal Health Information Form, shall be signed by the client or a person(s) acting on behalf of the client (see pages 34-35 of this policy for a hierarchy of substitute decision makers).

Individuals become common law after they have lived together for one year. There should be a note on the form confirming the marital status of common-law partners, domestic partners, and married partners.

If a patient is deceased, the administrator of the estate of the deceased may also sign the authorization for release of information, if the use or disclosure is for the purpose of the estate.

# Request for Access to
# My Personal Health Information

I, _____, do hereby request _____Health Centre to release a copy of my personal information to me.

If you wish to have specific components of your personal information released rather than all of it, please describe or list the information you would like released.

_____

_____

_____

_____

_____

Signature _____

Date _____

# Procedure 7.0: Storage and Disposal of Personal Information

| | |
|---|---|
| **Procedure:** How to store and dispose of personal information at the Health Centre | |
| **Related Forms/Tools:**<br><br>• Retention Schedule Template | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

PHIA s.50(1) requires that the health centre have a written retention schedule for all personal health information in its custody or under its control. The Health Centre will retain individual personal information for a minimum of 10 years unless there are special circumstances. Special circumstances may include maintaining a child's chart for 10 years beyond the age of 18. This means that the Health Centre may keep the private information of that person for a period of 28 years.

Private information at the Health Centre will be securely destroyed. Paper and microfiche, CDs, and DVDs will be shredded. Tapes and memory sticks must be permanently erased. Information stored on additional electronic devices, such as personal computers, laptops, photocopiers, FAX machines, laboratory equipment, must be destroyed according to industry standard. Confidential information must not be disposed of via routine waste/garbage.

The Health Centre will comply with the information contained in its retention schedule when determining the appropriate time period for destroying personal information. The Health Centre Retention Schedule will be reviewed on an annual basis by the Centre's Privacy Contact Person and updated appropriately.

Data device serial numbers will be recorded in case the Health Centre must report a loss or theft.

# Retention Schedule Template

| **Item** | **Guidelines for Retention** | **Custodian and Authority for Disposal** | **Minimum Retention Period** | **Retention Mode** (Assume hardcopy unless otherwise stated) |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Procedure 8.0: Security and Protection of Personal Information

| | |
|---|---|
| **Procedure:**<br>How to secure and protect personal information at the Health Centre | |
| **Related Forms/Tools:**<br><br>• Description of Information Security Officer Responsibilities<br>• Acceptable Use Policy<br>• Employee Termination/Reassignment Action Item Checklist | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

The Health Centre will implement administrative, physical and technical safeguards to:

1) ensure personal information is made available or disclosed only to authorized individuals;
2) make certain that personal information is accurate, complete and remains valid over time;
3) ensure information is accessible to authorized individuals when and where required;
4) ensure security and protection of information.

**Administrative Safeguards:**

- The Health Centre will identify and appoint a designated security officer who will have the overall responsibility of managing the Health Centre's security program on a day-to-day basis.
- Personal information (original, copies and electronic) cannot be removed from the Health Centre facilities and program sites. The only exceptions to this provision include:
    - Information needed for the direct provision of patient care; and
    - Information required by law (e.g. to comply with a subpoena or court order)
- Access to personal health information will be on a need-to-know basis. Only those who need to have access to the personal health information for the purpose of carrying out their job functions will have access. The Health Centre will provide only those employees authorized to access personal information with access rights to that information. Access rights

may be granted through file or network passwords, computerized door codes for entry into specific locations, or a list of authorized individuals who may access patient files from a central location. An inventory of all hardware (ex: desktops, laptops, handhelds, tablets, removable media, servers, etc…) and software owned by the Health Centre, and which stores electronic personal health information, will be kept and updated periodically. The inventory will include the location and approximate value of the hardware and software. The inventory will be checked periodically to ensure that computers are where they are supposed to be. A copy of the inventory will be held in a secure place offsite in case of a disaster (such as fire, flood, etc…).

- Security awareness and training will be provided to all Health Centre staff on an on-going basis. All new staff will be oriented to the Health Centre's security policies and procedures upon hire.
- Security reminders will be posted in visible locations.
- The Health Centre will perform periodic reviews of security practices.
- The Health Centre will enter into contractual agreements with security commitments with any third party that may handle personal information.
- The Health Centre's "Information Security Practices" (see below) will be followed by all staff, volunteers and visiting professionals.

**Information Security Practices[4]**

The Health Centre and its staff, volunteers, and visiting health professionals are expected to adhere to the following information security practices:

*Printers, Photocopiers and Fax Machines*

- Printers and fax machines that are used to print, send or receive personal health information will be located in an area that is accessible by authorized persons.
- If you print something, retrieve it from the printer immediately.
- Enable the "Secure Print" feature, if available, on all printers that are used to print personal health information. This feature requires a password to be entered at the printer before it will print.
- If you fax something, confirm the number is still valid and verify that it was dialed correctly.
- Periodically review fax numbers stored in the speed dial and ensure that they are still valid.
- Health Centre staff will use the following notice on fax transmissions: *"This faxed information may contain privileged and/or confidential information and is intended only for the use of the designated recipient(s). If you have*

[4] This section has been adapted from the ***Guide to Information Security for the Health Care Sector: Information and Resources for Small Medical Offices*** developed by eHealth Ontario.

*received this information in error or are not the intended recipient, any review, dissemination, distribution, or copying of this information is prohibited. Destroy the information and notify the sender that you have done so."*

- If you are expecting something by fax, especially if it is sensitive, treat it like a meeting: set a specific time to receive it.
- Do not leave original material in photocopiers or fax machines.

*On the Phone*

- Know to whom you are disclosing information. If uncertain, ask them to provide you with information that would verify their identity.
- Be aware of your surroundings, including cell phone conversations. Be mindful of eavesdropping.

*In Meeting Areas*

- Clean the whiteboard of sensitive information when the meeting is over.
- After a meeting, double check that sensitive information including documents are removed from the meeting room.
- At the beginning of a conference call, ask all participants to identify themselves.
- After a conference call or phone meeting, check that the phone line is closed after the meeting.

*Mobile Computing*

- Ensure your laptop and mobile devices are encrypted and/or password protected.
- Never leave your laptop or mobile devices in your car.
- Never leave your laptop or mobile devices unattended when travelling or in any other public place.
- If your laptop/mobile device uses wireless connections, ensure that all wireless communications are encrypted.
- When using CDs for data backup, store the files only in encrypted format. File encryption tools are provided in Microsoft Office applications.
- When using USB memory devices (USB flash drives) for backup or to move personal health information between computers, use only devices that have built-in encryption and require a password to access information.
- Store USB memory devices, CDs and other media in a secure place (ex: a locked drawer).
- Use power-on passwords – a password that must be entered before the device will start.
- When using a laptop outside of the office environment, ensure that your screen cannot be viewed by anyone other than you.
- When using laptops or mobile devices that contain personal information, never use open or unsecured networks.

*Clear Desk and Environment*

- When away from the office, sensitive information (paper files and computer media) should be locked in secure cabinets. Do not leave materials unattended in open, unsecured areas such as printers, copy machines, fax machines or meeting rooms.
- All sensitive information for disposal should be destroyed or erased in a secure way. Do not place them in a recycling bin or garbage.
- Incoming and outgoing mail and fax should be stored in a secure location.
- Avoid removing sensitive documents and data from business premises, unless necessary.

*Password Guidelines*

- Ensure that your computer has a screen saver that activates after a predefined time and requires a strong password to gain access to the computer.
- Change your passwords frequently, at least every 90 days.
- Passwords must NEVER be disclosed to anyone or written down. A password should not be obvious, easily guessable, or found in a common words dictionary and should not use acronyms, birthdays, sequential numbers, names of family members or pets.
- If you suspect the confidentiality of your password has been compromised, change it immediately and report it to the Security Officer.

*Email*

- Use appropriate signatures and standard disclaimers on email messages, faxes and other documents. Health Centre staff will use the following tagline on outgoing email, for example: *"If you have received this email in error or are not the intended recipient, please do not open any attachments, notify the sender by email or telephone that you have received this message, and after notifying the sender, delete the email from your system."*
- Be aware of techniques used by lawbreakers in attempt to gather personal information from you via email. For example, you may receive an email request to send lab results or provide other health or financial information from a user unknown to you.
- Carefully address emails. Always double-check the name(s) in all the address lines
- Be cautious about communicating sensitive information via email using mobile electronic devices.
- Do not forward sensitive materials from your office email to your personal email address such as Hotmail, Yahoo! and/or Gmail. The security level of these personal email accounts is weak and susceptible to compromise.
- Do not open email messages and attachments from senders you don't recognize and trust.
- If you suspect or know that an email message contains a virus, do not forward the email message.

- Do not reply to spam email, also known as junk email or unsolicited email.
- Do not click on links within spam email.

*Mail/Courier/Internal Mail/Memos*

- Patient information sent by regular mail or courier should be placed in a sealed envelope and clearly identified as confidential.
- When mail is received, it should be held in a secure area until such time as it may be delivered.
- Internal mail/memos containing sensitive information should be sealed and clearly identified as confidential.

*How to Protect Information*

- Understand security as it relates to your role and your obligations.
- Wear your Health Centre ID badge at work. Question anyone without a badge and ensure that visitors in secure or sensitive areas are escorted at all times.
- Select strong passwords and protect them from disclosure.
- Always lock your screen when you are away from your computer.
- Never use another person's user ID or password.
- Scan your computer weekly to ensure that spyware or unauthorized software is not installed.
- Make weekly backups of your data and keep the backups securely offsite.
- Install a privacy screen over your monitor or position your monitor in a way that makes it difficult for casual visitors in your office to read the contents displayed.
- Verify at least twice a year that you can restore data from backup disks or tapes.
- Secure laptops with a physical cable lock when in use in high traffic public areas.
- Request that your computer's hard drive be encrypted.
- Do not install unauthorized software of any kind. This includes games, books, music, etc…
- Never visit websites intended for adult-only audiences, gambling or online games.
- Keep all paper files, backup CDs and/or tapes in a fireproof cabinet.

**Physical Safeguards**

- The Health Centre's building alarm system will be functioning, monitored and used at all times.
- Offices will be secured at all times and accessed only by authorized personnel.
- Appropriate security mechanisms will be used at any unattended entrance to a secure area (ex: locks on doors, card access control, monitored surveillance cameras).
- The data room door will be secured at all times and only accessed by authorized personnel.

- The Health Centre will develop and implement a checklist of action items when an employee is terminated (whether voluntary or for cause) or whose duties have changed. The checklist will include such things as immediately deactivating access (ex: alarm pass codes), return keys, return software and hardware, notify IS vendor of change, etc…
- Data on hard drives and file servers will be securely destroyed before disposing of, or re-purposing, hardware.
- Printer, photocopier and fax machine memories will be wiped clean before disposing of, or re-purposing, the equipment.

**Technical Safeguards**

*Measures to Protect Network Infrastructure*

The Health Centre will review its network's protection against unauthorized access to protect network infrastructure from external (e.g. malware and hackers) and internal threats (e.g. network operational centres should be kept locked).

- An adequate firewall appliance will be in place and configured correctly at all times.
- Wireless network/internet access will be password protected and encrypted.
- Intrusion detection and internal network traffic will be actively monitored.
- Internet access will be through a firewall implemented through hardware (e.g. on a network router) or software residing on the user machine.
- Updates to software and security patches will be applied and managed.

*Measures to Protect Operating System, Program Software, and Data*

The Health Centre will utilize various measures to protect operating system software, program software and data.

- Back-up information will be stored in a secure, locked environment off-site.
- Information intended for long-term storage on electronic media will be reviewed on a regular basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.
- Up-to-date backups of all data (from both servers and personal computers) will be securely stored in a location off site.
- Encryption and authentication will be used to minimize the risk of access by unauthorized individuals.
- Antivirus/antimalware software will be used on servers and personal computers to protect against unauthorized modification, loss, access, or disclosure. As viruses and malware threats are constantly changing and advancing, the Health Centre will ensure that antivirus/antimalware software is up-to-date to protect from such threats.
- Data will be protected data during transport or on a mobile device.
    - Devices such as laptops, memory sticks and smart phones may facilitate mobility; however these devices should only be utilized for

personal health information if the appropriate security measures are in place.
    - Encryption will help to mitigate the risk of transporting data and it is required that, when taking data from a secure office location and putting it onto a mobile device or transporting it otherwise, data must be encrypted.
- Each staff member will be assigned a unique user ID.
- User IDs and passwords will be not be shared either directly or indirectly, through careless storage of user IDs and passwords.
- Network operating systems will be applied and managed.
- Computers will be set to automatically log-off after a specific period of inactivity.

**Security Breach**

*What Is a Security Breach?*
A security breach is an unwanted or unexpected situation that results in:

- The unauthorized disclosure, destruction, modification or withholding of information.
- A failure to comply with the Health Centre's security requirements.
- Unauthorized access, use or probing of information resources.
- An attempted, suspected or actual security compromise.
- Waste, fraud, abuse, theft, loss of or damage to resources.

*Why Might They Happen?*

- Failure to comply with approved policies and practices.
- Indifference to or being unaware of responsibilities.
- Inadequate, or lack of, safeguards.
- Inadequate training or supervision.

*What Are Possible Consequences?*

- Damage to reputation, loss of trust, financial losses, theft of computing resources, loss of employment or legal consequences.

*What to Do if You Witness a Breach?*

- Security breaches must be reported to the Health Centre's Privacy Contact Person.
- In accordance with PHIA regulations, security breaches that pose a risk to personal health information should be thoroughly documented and analyzed to determine the root cause or causes of the breach. Once the root cause has been identified, corrective action is required to minimize the risk of the event happening again in the future.
- The Privacy Contact Person must take appropriate action to contain actual or potential breaches, investigate, and report the finding(s).

- If you experience a breach, report it to the Privacy Contact Person. All incidents relating to the information you are responsible for should be appropriately identified, responded to, escalated and investigated.
- Information regarding privacy breaches can be found in Procedure 12 of this document as well as Chapter 3 of the PHIA Toolkit.

**Record of User Activity**

*PHIA* defines a record of user activity as a report produced at the request of an individual for a list of users who accessed the individual's personal health information on an electronic information system for a time period specified by the individual.

Section 63 of PHIA gives individuals the right to request a record of user activity for any electronic information system that a custodian uses to maintain the individual's personal health information. The record of user activity may be generated manually or electronically. It is important to note that the record of user activity must be made available within 30 days and at no charge.

The PHIA regulation section 11 (2) provides that the record of user activity must include at least all of the following information:

(a) the name of the individual whose personal health information was accessed;
(b) a unique identification number for the individual whose personal health information was accessed, including their health-card number or a number assigned by the custodian to uniquely identify the individual;
(c) the name of the person who accessed the personal health information;
(d) any additional identification of the person who accessed the personal health information, including an electronic information system user identification name or number;
(e) a description of the personal health information accessed or, if the specific personal health information accessed cannot be determined, all possible personal health information that could have been accessed;
(f) the date and time the personal health information was accessed or, if specific dates and times cannot be determined, a range of dates when the information could have been accessed by the person.

Given that not all custodians have (or should have) an elaborate electronic information system with robust audit functionality, the regulation allows for a broad response to the specific type of personal health information accessed along with ranges for the dates and times.

Therefore, custodians unable to extract this information electronically from their electronic information system are still able to comply with the regulation by providing a more general description. This information may be captured through

the custodians scheduling system (date and time) along with a detailed list of the personal health information captured by the applicable system.

**Audit Log Versus Record Of User Activity**

It is important to distinguish between an “audit log” and a “record of user activity”.

A record of user activity “means a report produced at the request of an individual for a list of users who access the individual’s personal health information on an electronic information system for a time period specified by the individual” (PHIA regulation section 11 (1)).

An audit log, if one exists, is an electronic file or record which details, during a given period of time, who has accessed patient information in an electronic information system. The audit log may or may not contain more fields than those required by regulation to produce a record of user activity.

A record of user activity may be generated by taking specific fields from a system’s audit log and forming a report that could be provided to an individual. As per PHIA regulations, the audit logs used to generate a record of user activity, must be kept by the Health Centre for at least one year from the date they were used to create a record of user activity.

# Information Security Officer Responsibilities

The Information Security Officer is responsible for managing the Health Centre's security program on a day-to-day basis. Specific responsibilities include the following:

- Ensuring all Health Centre staff, volunteers, and visiting professionals are aware of the Health Centres Information Security Practices and receive the training and support required to implement them.
- Ensure disposal of personal and personal health information meets security standards
- Ensure staff have access to a shredding machine to securely dispose of personal health information no longer required.
- Instruct staff how to create strong passwords, one that is easy to remember but difficult to guess, and never to share their passwords.
- Ensure staff understand that they are not to install unauthorized software, connect unauthorized devices to their computers, or use their computers for unauthorized purposes.
- Make certain that all staff members make weekly backups of their data. If possible, keep the backups offsite.
- Revoke or suitably adjust (physical, network, system and application) access and change shared passwords as soon as employees leave or change responsibilities.
- Direct the IT service provider to set up security safeguards on all office computers including strong encryption, security patches and antivirus solutions.
- Ensure the IT service provider provides a written description of the service provided.
- Report all security incidents to the Health Centre's Privacy Contact Person. Arrange assistance in leading the investigation, if necessary, and ensure required remediation is completed.
- Monitor and perform spot checks on a regular basis to ensure all staff are following the Information Security Practices. Take appropriate action if not followed.

# XXX Health Centre's Acceptable Use Policy

This Acceptable Use Policy applies to all employees, visiting health professionals, and volunteers who have access to computers and the Internet through the XXX Health Centre. Use of the Internet by employees and volunteers of the Health Centre is permitted and encouraged where such use supports the goals and objectives of the organization. However, access to the Internet through the Health Centre is a privilege and all employees, volunteers, and visiting health professionals must adhere to the policies concerning computer, e-mail and Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Individuals may also be held personally liable for damages caused by any violations of this policy. All employees, volunteers, and visiting professionals are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

Computer, email and internet usage

- Company employees, volunteers and visiting professionals are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role
- All Internet data that is composed, transmitted and/or received by the Health Centre's computer systems is considered to belong to the Health Centre and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties
- The equipment, services and technology used to access the Internet are the property of the Health Centre and the organization reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails sent via the Health Centre's email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by the Health Centre if they are deemed to be harmful and/or not productive to business

Unacceptable use of the internet and associated technology by employees includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via the Health Centre's email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy

- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the health centre
- Hacking into unauthorized websites
- Sending or posting information that is defamatory to the Health Centre, its products/services, colleagues and/or customers
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Online shopping
- Playing games
- Passing off personal views as representing those of the organization

If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification

All terms and conditions as stated in this document are applicable to all users of the Health Centre's network, Internet connection and associated technology. This acceptable use policy applies during work hours and also extends to use of health centre network, Internet and technology after work hours. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by the Health Centre.

User compliance
I understand and will abide by this Internet Usage Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

_____ _____

Employee signature Date

# Employee Termination/Reassignment Action Item Checklist

Employee Name: _____

Date of Termination or Reassignment: _____

When an employee is terminated (whether voluntary or for cause) or when an employee's duties have changed, the following actions will be taken:

- ☐ access to building de-activated (ex: deactivate alarm pass codes and return keys)
- ☐ software and hardware returned
- ☐ IS vendor notified of change
- ☐ e-mail de-activated
- ☐ Dymaxion notified to deactivate Practimax access
- ☐ employee identification card and name badge returned

Actions Completed by:

_____

Signature

_____

Date

# Procedure 9.0: Accuracy and Information Correction

| | |
|---|---|
| **Procedure:** How to ensure the accuracy of personal information and correct errors or omissions | |
| **Related Forms/Tools:**<br><br>• Request to Correct Personal Information | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

Health Centre staff collecting personal information will take all necessary steps to ensure that the information is accurate. Such steps may include:

- repeating the spelling of names;
- reviewing personal information with the patient at the time of collection;
- repeating the name of next-of-kin, family physician, and home address to the patient at check in and
- noting corrections on patient charts using provider initials.

A patient who believes there is an error or omission in his or her personal information may make a request to the Health Centre to change their information. Such errors or omissions may include address updates, changes in the status of next-of-kin, and/or incorrect dates or incorrect information about that person's health status.

Requests for changes in personal information must be made in person or in writing, using the Request to Correct Personal Information form. The Health Centre will receive a signed copy, which it will keep on file, of the individual's request.

Any amended information will be forwarded to third parties by the Health Centre if those third parties have been involved in the patient's care.

Under PHIA, ss. 85-90, the Health Centre is not required to correct the information if:

a) it consists of a record that was not originally created by the Health Centre and the Health Centre does not have sufficient knowledge, expertise and authority to correct the record;

b) it consists of a professional opinion or observation that a health professional or Health Centre staff has made in good faith about an individual;

c) the Health Centre believes on reasonable grounds that a request for a correction is frivolous or vexatious; or is part of a pattern of conduct that amounts to an abuse of the right of correction,

If the Health Centre does not correct the information for the reason(s) listed above, it shall provide written notice to the client.

# Request to Correct
# Personal Information

Personal information on this form is collected under the _____Health Centre's Privacy Policy and will be used to respond to your request to correct your personal and private information.

About you

Last Name _____
First Name _____
Middle Name _____

Address _____
(including street, city/town/village, province, and postal code)

Telephone Number _____
Health Card Number _____

What personal information needs to be corrected? Please provide as much detail as possible. Be sure to give the complete name listed in the Health Centre records if it is different from the name above. If you need more space, please use the back of this form and/or attach a separate sheet of paper.

_____
_____
_____

What correction do you want to make and why? Please attach any documents that support this request.

_____
_____
_____

Signature of Applicant _____

Date _____

# Procedure 10.0: Openness Regarding Privacy Policy Document

| | |
|---|---|
| **Procedure:** The Health Centre's procedures for ensuring openness and transparency involving its privacy policy, principles, and protocols, and procedures. | |
| **Related Forms/Tools:** | **Approved**<br>By:<br>Date:<br>**Revised Date:** |

**Steps:**

The Health Centre will adhere to plain language principles in the development of all privacy information that will be made available to the public.

The Health Centre will prepare, laminate and post "Notice of Purpose" posters throughout the building(s) identifying where to find a copy of the the Health Centre's written privacy statement, privacy policy and procedures, and the contact information for the Health Centre's Privacy Contact Person.

The Health Centre will make the following information easily available to all staff, volunteers, students, and visitors as well as health centre patients.

- The policies and procedures used to support the management of personal information;
- Names and contact information of the privacy contact person and his or her designate;
- The process by which an individual can gain access to his or her personal information;
- The process by which an individual can lodge a complaint in regard to a breach of privacy or make a challenge to the Health Centre's compliance with the ten principles;
- General information about the Health Centre's privacy policies, the reason information is collected and the Centre's commitment to ensuring that confidential information is safeguarded.

# Procedure 11.0: Challenging Compliance

| | |
|---|---|
| **Procedure:** How to address challenges to the Health Centre's compliance with its privacy principles. | |
| **Related Forms/Tools:**<br><br>• Privacy Complaint Form | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

In situations where an individual challenges the Health Centre's compliance with its Privacy Policies, Procedures, or PHIA, the complaint must be made either in writing by letter or email or verbally to the Centre's Privacy Contact Person or designate.

If the complaint is made verbally, the Health Centre's privacy contact person/designate shall paraphrase on the Privacy Complaint form and both the person making the complaint as well as the Privacy Contact Person/designate shall sign and date the form.

The privacy contact person/designate shall document the specific principle(s), protocol(s) and/or procedure(s) that may be relevant to the complaint.

The privacy contact person shall review the complaint and, if necessary, seek assistance from a lawyer or privacy policy expert regarding the basis of the complaint.

The investigation results and, if applicable, suggested remedies will be reported back to the individual, in writing, within a period of no more than 30 days by the privacy contact person/designate.

In order to ensure that an individual's complaint does not negatively impact their care and treatment, all documents related to the complaint should be kept in a record separate from the individual's personal health information record.

# Privacy Complaint Form

This form is provided to you to allow you to provide all information related to your complaint. You may also send a letter outlining your complaint to the Privacy Contact Person for our organization (see below for contact information).

1. **PATIENT/CLIENT NAME AND CONTACT INFORMATION** (please print clearly)

Last Name First Name Middle initial

Mailing address

Daytime telephone number

E-mail address (only required if you wish to be contacted by e-mail)

How do you wish to be contacted? Please check one:
□ phone □ regular mail □ e-mail

**If you are making the complaint on behalf of someone else, please provide your name and contact information:**

Last Name First Name Middle initial

Relationship to patient/client/resident

Mailing address

Daytime telephone number

E-mail address (only required if you wish to be contacted by e-mail)

How do you wish to be contacted? Please check one □ Phone Regular mail E-mail

**You must attach a copy of the document authorizing you to make the complaint.**
Example: written consent of the individual, guardianship documents.

## 2. DETAILS OF THE COMPLAINT

**Please provide as much information as you can about the complaint you are making**. Please include details of the incident(s) leading to your complaint, the name of any individuals who are involved in the incident(s), the date when the incident(s) occurred, and any information about your efforts to attempt to resolve this complaint outside of this complaint process (e.g. informal discussions with someone involved in the incident).

**Please attach any documents relevant to the complaint**

## 3. RESOLVING THE COMPLAINT

What do you think should happen to resolve your complaint?

## 4. CONSENT AND SIGNATURE

**In order to fully investigate your complaint, we will need to review your personal health information relevant to your complaint. Please check and initial your response.**

___ I consent to the _____ reviewing my personal health information in order to fully investigate my complaint

___ I **do not** consent to the _____ reviewing my personal health information in order to fully investigate my complaint

We may also need to discuss the facts presented on this form and any other information related to the complaint with individuals in our organization**. We would only disclose information relevant to the complaint.**

___ I consent to the _____ discussing the facts presented on this form and any other information related to the complaint with individuals in _____. I understand that _____ will only disclose information relevant to my complaint.

___ I **do not** consent to the _____ discussing the facts presented on this form and any other information related to the complaint with individuals in _____.

Please note that we may not be able to fully investigate your complaint if we do not have access to all the relevant information related to your complaint.

_____

**Signature** **Date**

**Please deliver or mail your original form to:**

**Name of privacy contact person**
**Name of health centre**
**Address of health centre**
**Phone:**
**Fax:**

If you have any questions about this form or the process for making a complaint, please contact the [name of privacy contact person] at the Health Centre.

# Procedure 12.0: Breach of Privacy or Security

| **Procedure:** Steps for addressing breaches | |
|---|---|
| **Related Forms/Tools:**<br><br>• Privacy/Security Breach Incident Report | **Approved**<br><br>By:<br><br>Date:<br><br>**Revised Date:** |

**Steps:**

If a privacy or security breach has occurred or is suspected, the staff member(s) responsible for, or who has discovered the breach, is required to immediately identify the scope of the breach to their manager, if they have one, and to the Health Centre Privacy Contact Person/designate. This person(s) must also take steps to prevent further loss or unauthorized disclosure of personal and/or sensitive information.

The staff member(s) responsible for, or who has discovered the breach, and their manager, if applicable, must document the event and the extent of the breach.

The Health Centre Privacy Contact Person/designate is responsible for coordinating the investigation of the breach and in reporting the results of the investigation, including steps for disciplinary action if warranted, to the staff member(s) responsible and their manager(s).

The investigation and any follow-up action shall be documented using the Privacy/Security Breach Incident Report.

Subject to applicable laws, the Health Centre Privacy Contact Person/designate must notify any affected client(s) at the first reasonable opportunity if the Privacy Contact Person/designate believes on a reasonable basis that the client's information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification, AND that as a result, there is a potential for harm or embarrassment to the client.

The Privacy Contact Person/designate may decide not to notify the client if it is unlikely that a breach occurred, or if there is no potential for harm or embarrassment to the client as a result.

If a decision is made not to notify the client, PHIA s.70(2) requires the Privacy Contact Person notify the Nova Scotia Privacy Review Officer as soon as possible: http://foipop.ns.ca/contact-us

If the Health Centre Privacy Contact Person is the person responsible for the breach, the coordination of the investigation will be assigned to an individual who is NOT a staff person at the Health Centre (ie: medical staff head within the Centre or the privacy officer at the Cape Breton District Health Authority).

Coordination of a privacy breach investigation may include steps to mitigate concerns among Health Centre staff and patients, volunteers, visitors, and others involved in the activities of the Centre as well as members of the public. Such steps may include:

- Preparing a briefing note for appropriate staff (e.g. senior administrative staff, public affairs staff, information systems staff);
- Introducing immediate changes to security codes such as passwords, door codes etc and informing those impacted by this change;
- If the breach has been made public, a statement that the Health Centre is investigating the breach and will address any and all issues related to the breach.

The decision to inform the Health Centre staff and volunteers, visitors and members of the public about the breach will be made by the Privacy Contact Person/designate in consultation with the offending staff person's manager, legal counsel, and public affairs counsel.

If the breach does not involve a staff member but an individual associated with the Health Centre in another way such as a visitor, patient, volunteer or student, the above steps will be taken as appropriate.

# Privacy Breach Incident Report

**Timing:**

If a privacy breach is suspected or known to have occurred within the Health Centre, it shall be reported immediately. Prompt reporting will allow the Health Centre to prepare to respond to potential public inquiries and any complaints that may be received. Such notification may enhance the public's understanding of the incident and increase confidence in the Health Centre.

**Reporting:**

All privacy breaches must be reported to the Privacy Contact Person or designate. The Health Centre Privacy Contact Personr/designate is _____ and may be contacted using the following information.

Email: _____

Telephone: _____

Mailing Address: _____

**Form:**

Date: _____

Name of person reporting the incident (if applicable)

_____

Contact information of person reporting the incident

_____

_____

**Incident Description** (Please include date and time breach occurred, date and time breach was reported, details of breach including names and contact information for all individuals whose information was allegedly breached, and the name of the person(s) responsible for the breach. Use separate form if needed)

**Describe steps taken to contain the breach.** This may include recovering copies of information in all media and remiving access privileges to person allegedly involved in the breach. Include the names and positions of all persons involved in containing the breach. Attach all relevant documents.

**Investigation description.** Include all information related to the investigation of the breach as well as ncluding decisions follow up, and changes to procedures and or protocols. To be completed, dated and signed by the Health Centre Privacy Contact Person/designate). Attach all relevant documents.

**Notification**

Were all affected individuals notified? Yes _____ No _____

Who should be notified?
1. Individuals (whether patients or staff) whose personal information is involved in the breach and
2. Other organizations that are or may be affected by the breach.

If YES:

Who was responsible for notification?

---

How was notification provided?

---

When was notification provided?

---

If NO, why not?

If the decision was made not to notify the individual(s), was the NS Privacy

Review Officer notified of this decision? If so, attach a copy of the notice.

Signed: _____ Date: _____