

**Sample Privacy and Security**

**Policy Manual**

*Version 1.0*

**Disclaimer**

The information in these resources does not constitute legal advice. It is general information intended to assist physicians in understanding their obligations and general duties under the Newfoundland and Labrador *Personal Health Information Act*. *The information is provided as guidance for clinics in Newfoundland and Labrador for developing their privacy program and may be updated from time to time. Any updates to the Sample Privacy and Security Policy Manual will be posted on edocsnl.ca. In the case of a discrepancy between PHIA and the document, PHIA shall be taken as correct.*

The eDOCSNL Privacy and Security Resource materials have been developed to align with applicable legislation and best practices. The eDOCSNL Privacy and Security Resources are based on original work completed by the Saskatchewan Medical Association, EMR Program.

**Table of Contents**

[Responsibilities of the Contact Person (Privacy Officer) 4](#_Toc465947897)

[Obligations of Employees and Health Professionals 5](#_Toc465947898)

[Privacy and Security Awareness, Education and Training 6](#_Toc465947899)

[Accuracy and Integrity 7](#_Toc465947900)

[Identified Purpose and Openness 9](#_Toc465947901)

[Challenging Compliance 10](#_Toc465947902)

[Closing the Medical Practice 11](#_Toc465947903)

[Patient Access to Own Record 12](#_Toc465947904)

[Correcting a Patient Record upon Request 15](#_Toc465947905)

[Individual’s Representative 17](#_Toc465947906)

[Collection 19](#_Toc465947907)

[Use 20](#_Toc465947908)

[Disclosure 23](#_Toc465947909)

[Disclosure of Personal Health Information to Relatives 27](#_Toc465947910)

[Disclosure of Personal Health Information to a Successor 28](#_Toc465947911)

[Disclosure of Personal Health Information for Health and Safety Purposes 29](#_Toc465947912)

[Disclosure of Personal Health Information for Legal Proceedings 30](#_Toc465947913)

[Managing Patient Consent and Masking in the EMR 31](#_Toc465947914)

[Agreements 33](#_Toc465947915)

[Management of Breaches 34](#_Toc465947916)

[Business Continuity Plan 38](#_Toc465947917)

[Storage, Retention, and Destruction of Paper Records 39](#_Toc465947918)

[Scanning and Destruction of Paper Records 41](#_Toc465947919)

[Backups and Storage 42](#_Toc465947920)

[User Account Management 43](#_Toc465947921)

[Auditing 45](#_Toc465947922)

[Destruction of Office Equipment and Medical Devices 47](#_Toc465947923)

[Retaining Personal Health Information 47](#_Toc465947924)

[General Security Software 48](#_Toc465947925)

[Security of the Office 49](#_Toc465947926)

[Use of Cameras for Patient Care 50](#_Toc465947927)

|  |  |
| --- | --- |
| Responsibilities of the Contact Person (Privacy Officer) | |
| **Legislative Reference:** PHIA s. 18 | **CPSNL Reference: n/a** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Associated eDOCS NL Documents and Templates:** Privacy and Security Notice Poster | |

**Policy**

[Physician name] will appoint one or more contact persons to perform the following functions:

1. facilitate compliance with the Personal Health Information Act;
2. Ensure that all employees, contractors, agents and volunteers are informed of their duties under the Personal Health Information Act;
3. Respond to privacy inquiries from the public; and
4. Respond to requests for access to or correction of personal health information that is in the custody or control of [Physician name].

[Physician name] will make a written statement that sets out the name and contact information for the contact person and make it available within the clinic.

Examples of a written statement include:

* Publication of the information on a website;
* Posting a notice at the clinic in a highly-visible area; and / or
* Providing pamphlet or other hand-out containing the information to individuals.

If [Physician name] has not identified a contact person, [Physician name] will make their own contact information available in the written statement.

**Procedure**

**Note:** This policy does not require procedures. There does need to be a clear understanding of who in the clinic has the responsibilities listed in“Responsibilities of the Contact Person”. These may be listed here or with the relevant policies and procedures as has been done in this sample manual.

|  |  |
| --- | --- |
| Obligations of Employees and Health Professionals | |
| **Legislative Reference:** PHIA s. 14 | **CPSNL Reference:** Advisory - Privacy, Confidentiality, and Disclosure of Patient Information |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Associated eDOCS NL Documents and Templates:** Oath/Affirmation of Confidentiality | |

**Policy**

All employees, agents, contractors and volunteers, as well as health professionals with the right to treat individuals at [Clinic Name] are obligated to protect personal health information in accordance with the Personal Health Information Act and this Policy Manual which includes signing an Oath/Affirmation of Confidentiality annually.

**Procedures**

1. All employees, agents, contractors and volunteers, as well as health professionals will:
   1. Receive an electronic copy of this Policy Manual to read and use.
   2. Ensure they understand all policies and procedures and ask for clarification when they do not understand.
   3. Participate in all education and training offered by [Physician Name].
   4. Are responsible and accountable for ensuring the protection and security of personal health information they collect, use, and disclose and assist others to do the same.
   5. Are responsible and accountable for assisting patients in any request for their personal health information, requests for corrections to their personal health information, and inquires on the privacy practices of [Physician Name].
   6. Take an Oath or Affirmation of Confidentiality that will be held in each employee’s personnel file or with correspondence related to the person’s engagement.
   7. As a condition of engagement with [Physician Name] all health professionals who are not custodians under the *Personal Health Information Act* shall sign an oath/affirmation of confidentiality.
      1. The signed oath or affirmation will be held in each employee’s personnel file or with correspondence related to the person’s engagement with [Clinic Name].
2. Those who do not comply with these procedures will be considered to have breached the Personal Health Information Act as well as the policies and procedures of [Clinic Name] and will be subject to disciplinary action by [Physician Name], the health professional’s regulatory body, or the courts as authorized by the *Personal Health Information Act*.

|  |  |
| --- | --- |
| Privacy and Security Awareness, Education and Training | |
| **Legislative Reference:** PHIA s. 13 | **CPSNL Reference: N/A** |
| **Policy Author:** | **Effective and Revision Date:** |
| **Associated eDOCS NL Documents and Templates:** Oath/Affirmation of Confidentiality; Acceptable Use Agreement; Privacy and Security Awareness and Training for New Employees Checklist | |

**Policy**

[Clinic Name] creates a culture of privacy through awareness activities, educational opportunities, and privacy and security training to ensure all employees, agents, contractors and volunteers, as well as health professionals are aware of their obligations under the Personal Health Information Act.

**Procedures**

1. The Privacy and Security Statements will be posted in a place visible to all employees, agents, contractors and volunteers, as well as health professionals working at [Clinic Name].
2. The “Privacy Officer” is responsible for developing and maintaining an educational program about these policies and procedures.
3. Role specific training is provided to all employees, agents, contractors and volunteers, as well as health professionals who require training on privacy and security procedures such as faxing, emailing, scanning, storage, backups, destruction and other activities as identified.
4. The “Privacy Officer” provides orientation to new employees on their first day. This orientation includes a thorough discussion of the privacy and security policies and procedures and is documented using the “Privacy and Security Awareness, Education and Training for New Employees Check List”.
   1. New employees, agents, contractors and volunteers, as well as health professionals are given a copy of the Policy Manual.
   2. New employees, agents, contractors and volunteers, as well as health professionals sign an Oath or Affirmation of Confidentiality before they are provided with access to personal health information.
   3. New employees, agents, contractors and volunteers, aI have sis well as health professionals sign the acceptable use agreement before they are given a username and password for the EMR.

|  |  |
| --- | --- |
| Accuracy and Integrity | |
| **Legislative Reference:** PHIA s. 16 | **CPSNL Reference:** Bylaw 6 |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Associated eDOCS NL Documents and Templates:** N/A | |

**Policy**

Upon collection, [Physician Name(s)] and all employees, agents, contractors and volunteers, as well as health professionals at [Clinic Name] will include the date the information was collected and the name of the individual providing the information. Before either using or disclosing personal health information that is in its custody or under its control, a [Physician Name] will:

1. take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purpose for which the information is used or disclosed;
2. clearly set out for the recipient of the information the limitations, if any, on the accuracy, completeness or up-to-date character of the information; and
3. take reasonable steps to ensure that the recipient is the person intended and authorized to receive the information.

**Procedures**

1. Records are updated during the patient’s appointment or as soon as possible afterwards.
2. The patient’s EMR record includes:
   1. The date that [Physician Name] or other health provider at the clinic sees the patient.
   2. A record of the assessment of the patient which includes the history obtained, particulars of the physical examination, the investigations ordered and where possible, the diagnosis; and a record of the disposition of the patient including the treatment provided or prescriptions written by [Physician Name], professional advice given and particulars of any referral that may have been made. Prescribing information includes the name of medication, strength, dosage and any other directions for use.
3. The patient record should include every report received respecting a patient from another custodian or other health professional.

1. The records are to be kept in a systematic manner.
2. [Physician Name] takes steps to improve the accuracy of the information the clinic collects, which includes
   1. That it be written in clear language with only common abbreviations used.
   2. The EMR records the date, time, and the name of the author.
   3. Additions and corrections are made in a manner that allows the original information to still be read.
   4. Ensuring scanned documents and photocopies are complete and readable.
   5. Staff is trained on how to keep accurate records.
3. [Physician Name] takes steps to protect the integrity of the personal health information which include:
   1. Accurate recording of the personal health information.
      1. Updating records when notified of corrections
      2. Notifying other custodians when a correction or notation is made in the record
   2. Accurate scanning and photocopier of personal health information.
   3. Perform daily backups.
   4. Ensure secure and environmentally safe storage.
   5. Audit of accesses to personal health information.
   6. Use up-to-date security software.
   7. Limit access to those who need to know the information.

|  |  |
| --- | --- |
| Identified Purpose and Openness | |
| **Legislative Reference:** PHIA ss. 19, 20 | **CPSNL Reference:** N/A |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Associated eDOCS NL Documents and Templates:** Poster | |

**Policy**

[Clinic name] provides patients with information on the purpose for the collection, use and disclosure of their personal health information and is open with patients about the clinic’s privacy and information practices.

**Procedures**

1. The Privacy Officer ensures that **information is posted about the clinic’s privacy practices** within the clinic.
2. The poster will contain at a minimum
   1. The name and contact information for the Privacy Officer.
   2. Information about [Physician Name]’s information handling practices.
   3. The anticipated uses and disclosures of personal health information.
   4. How patients can manage their consent directives.
   5. Information about how patients can ask for access to their personal health information and how to request a correction to errors and omissions.
   6. Information about how patients can make a complaint to the Office of the Information and Privacy Commissioner of Newfoundland and Labrador.
3. Copies of the Department of Health pamphlet about PHIA will be available in the waiting room.
4. Anyone authorized to collect personal health information at the clinic will answer all questions about the anticipated collection, uses and disclosures of the personal health information.

|  |  |
| --- | --- |
| Challenging Compliance | |
| **Legislative Reference:** PHIA ss. 13, 18 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Associated eDOCS NL Documents and Templates: n/a** | |

**Policy:**

[Clinic Name] provides a confidential process for patients to lodge a complaint regarding the clinic’s adherence to its policies and procedures, or to notify the clinic of a potential or suspected breach of personal health information.

**Procedures**:

1. A patient may submit a complaint to [Physician Name] or an employee at [Clinic Name] in writing or verbally.
2. A complaint should be confidential but may not be anonymous.
3. [Physician Name] will be notified of the complaint as soon as possible, or at least before the end of the clinic office hours.
   1. If the complaint is a suspected privacy or security breach, [Physician Name] will activate the breach management plan.
   2. All discussions and actions related to the complaint will be documented.
4. The response to the patient may be provided verbally.
5. A periodic analysis is made of all complaints to determine if there are systemic issues that should be addressed through updates in policies, changes in education, awareness, training or other action.
6. A patient dissatisfied with the response to a complaint will be provided with information on how to contact the Office of the Information and Privacy Commissioner of Newfoundland and Labrador.

|  |  |
| --- | --- |
| Closing the Medical Practice | |
| **Legislative Reference:** PHIA s. 39 | **CPSNL Reference:** Bylaw 6; Policy - A Physician's Responsibility when Permanently Closing a Medical Practice |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Associated eDOCS NL Documents and Templates:** N/A | |

**Policy**

[Physician Name] will ensure the proper transfer or storage of patient records upon closing the medical practice.

**Procedures**

1. [Physician Name] will make reasonable efforts to notify all patients at least 90 days prior to when he/she ceases operation, to indicate the storage or transfer arrangement for the records.
2. [Physician Name] will follow the guidelines of the College of Physicians and Surgeons of Newfoundland and Labrador Medical Records Bylaw 6 and Policy - A Physician's Responsibility when Permanently Closing a Medical Practice. In preparation to close the practice [Physician Name] will:

(i)  give prior written notification to the College of where their medical records will be retained or;

(ii) transfer the records to:

* + 1. the patient or to the patient’s authorized representative,
    2. to another medical practitioner, or
    3. to a regional health authority

1. [Physician Name] will notify patients of practice closure through three published notices in the daily newspaper, including one weekend publication over a period of two weeks, in addition to one or more of the following:
   1. By a letter to the patient;
   2. Directly at the time of an office visit;
   3. By a notice in the physician’s office; and
   4. By a telephone answering service.
2. If [Physician Name] does not transfer the records he/she will:
   1. retain the records within their EMR instance; or
   2. have the records extracted from the EMR instance and maintain the records in a secure manner.

until such a time that the retention periods have expired.

|  |  |
| --- | --- |
| Patient Access to Own Record | |
| **Legislative Reference:** PHIA s. 52 | **CPSNL Reference**: Bylaw 6; Guideline - Patient Access to Office Medical Recordsand the Personal Health Information Act |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Associated eDOCS NL Documents and Templates:** Access to Personal Health Information Form, Letter of Refusal or Partial Refusal of Access or Referring an Access Request, Letter of Extension. | |

**Policy**

[Clinic Name] provides patients with access to their own personal health information upon request. Requests may be made in writing unless otherwise agreed upon.

**Procedures**

CPSNL Bylaw 6 states:

1. The records required to be made and retained by a medical practitioner must be:
   1. Legibly written, typewritten, or electronically recorded;
   2. Kept in a systematic manner;
   3. Where it is necessary to revise an existing medical record entry, the revision shall be made in such manner as to not remove, delete, erase, or render illegible each previously existing unrevised record or entry, and the date of the revision shall be clearly noted in the vicinity of each such revision; and
   4. Kept in a secure manner, and accessible only to
      1. the medical practitioner;
      2. to such persons employed or associated with the medical practitioner’s practice who are specifically authorized by the medical practitioner to access a patient record and who are made aware by the medical practitioner of the need to maintain the confidentiality of patient records;
      3. patients and other authorized persons in accordance with the Medical Act, PHIA and any other applicable law or regulation, or by-law, policy or guideline of the College, as may be corrected from time to time, including without limiting the foregoing those policies and guidelines.

**Informal Requests**

[Physician Name] will provide patients, at the time of their appointment, with copies of information discussed at the appointment, upon request.

**Formal Requests**

1. Patient requests for access to their own medical records may be madeto the Office Manager.
   1. Patients wishing to make written requests are encouraged to use the clinic’s application form.
   2. The Office Manager will document a verbal request using the clinic form when the request cannot be completed immediately.
   3. The Office Manager will help patients complete the request when necessary.
   4. The Office Manager will confirm the identity of the requestor.
2. A patient may view his or her own original chart in the presence of [Physician Name] or the Office Manager.
3. Should the patient want a copy of the chart, the clinic charges fees in alignment with the Newfoundland and Labrador Medical Association’s, “Physician’s Guide to Billing Noninsured Services”, published in 2009.
   1. The Office Manager will provide the patient with an estimate of the cost for a copy of the record before preparing the copy
4. At the patient’s request all terms, codes, and abbreviations will be explained. If [Physician Name] is unable to provide an explanation the patient will be referred to someone who can.
5. If [Physician Name] does not have the information requested and is aware of another custodian who has the information, the patient’s request will be sent to the other custodian.
   1. When [Physician Name] transfers a request, the patient will be notified as soon as reasonably possible.
6. Patients are provided with access to, or a copy of, their own personal health information as quickly as possible within 60 calendar days after the completed request has been received by the Office Manager.
7. [Physician Name] may take up to an additional 30 calendar days to provide access when
   1. meeting the time limit set out would unreasonably interfere with the operations of the clinic; or
   2. the information consists of numerous records or locating the information that is the subject of the request cannot be completed within the time limit set out.
8. When the clinic exceeds the original 30 calendar days [Physician Name] will send a letter to the patient, prior to the 30th day, explaining the delay.
9. [Physician Name] will refuse access to the personal health information when:
   1. Granting access would reveal personal health information about an individual who has not consented to disclosure (PHIA s. 58(1)(b)).
   2. The personal health information was collected and used for one of the following reasons the patient will be referred to the custodians who provided the information

* review by a standards or quality of care committee studying or evaluating health care practices (PHIA s 58(1)(c)(i))
* a body with the responsibility of discipline of health care professionals or the quality or standards of professional services provided by health care professionals (PHIA s58(1)(c)(iii)).

1. [Physician Name] may refuse access to the personal health information when access could result in a risk of serious harm to the mental or physical health or safety of the individual (PHIA s 58(2)(d)(i)).
2. When the record contains information that should not be given to the patient, that information should be severed from the record and the remaining information provided to the patient.
   1. Information is severed by printing the page with the information to be provided to the patient. The information to be severed is struck out with a black marker. In the margin write the section of PHIA that authorizes the severing of the information. The marked page is photocopied to ensure the severed information is not visible through the mark.
3. The Office Manager prepares all letters to patients explaining the refusal of access or the severed information and the relevant section of PHIA. All letters to patients explain the correction or notation and advises the patient that he/she can ask the Information and Privacy Commissioner to review the decision of the medical practice. The letter is signed by [Physician Name].
4. A copy of the particular package sent to a patient must be retained for Clinic records. In the event a complaint to the OIPC is made, a copy of the package may be requested for review.

|  |  |
| --- | --- |
| Correcting a Patient Record upon Request | |
| **Legislative Reference:** PHIA ss. 60, 61, 62, 63, 64 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Templates:** Request for Correction Form, Letter confirming Correction, Letter notifying of Notation, Letter regarding Correction or notation to another Custodian | |

**Policy**

[Physician Name] responds to all requests from patients to correct their personal health information. Factual personal health information that is incorrect will be corrected when reasonably possible. Professional opinions will be corrected at the clinic’s discretion. If a correction is not made a notation must be added to the record.

**Procedures**

1. Requests may be accepted verbally or in writing.
2. The Office Manager will assist the patient in completing the application form.
3. Corrections are made where accuracy can be confirmed.
4. A patient request to correct a professional opinion or diagnostic test is made at the clinic’s discretion. If the correction is not made a notation must be made in the record**.**

**Receiving the Request**

1. All applications from a patient for correction are dated and signed by the Office Manager the day the completed application is received by the practice.
   1. Corrections or notations are made as soon as possible and in any event not more than 30 calendar days after receiving the completed request.
   2. The time may be extended for an additional 30 days where meeting the time limit would unreasonably interfere with the operations of the clinic or the information is located in numerous records.
   3. The Office Manager must be satisfied of the identity of the person making the application. For most patients this will have occurred at the time the patient requested the chart or they are known to the clinic.
2. Corrections are made by recording the correct or omitted information in the record and if incorrect information must be struck out this will be in a manner that still allows the incorrect information to be read.
   1. When it is not possible to record the corrected information in the record a note will be added to the record that directs anyone accessing the record to the location of the correct information.
3. [Physician Name] will not make a correction but will make a notation where:
   1. The record was not originally created by [Physician Name] and [Physician Name] does not have sufficient knowledge, expertise, or authority to correct the record.
   2. The information the patient is requesting be changed consists of professional opinion or diagnosis that [Physician Name] made in good faith about the patient.
4. [Physician Name] provides written notification to the patient making the request that the correction was made or not made, in which case a notation was added to the record.
   1. The letter explains when and how the correction or notation was made.
5. Where practical, written notice is also sent to any other custodian or person, who was sent the information in the previous 12 months before the request for correction or notation was received.
   1. Where the physician believes that the correction will not have an impact on the patient’s ongoing health care or other benefits, such notice is not required
6. When [Physician Name] does not make the correction, the Office Manager will provide the patient with information on how an appeal can be made to the Office of the Information and Privacy Commissioner of Newfoundland and Labrador.

|  |  |
| --- | --- |
| Individual’s Representative | |
| **Legislative Reference:** PHIA s. 7 | **CPSNL Reference:** Bylaw 6 |
| **Policy Author:** | **Effective and Revision Dates:** |

**Policy**

In certain circumstances, [Physician Name] is authorized to take instructions regarding the management of an individual’s personal health information from persons other than the individual to whom the personal health information pertains.

**Procedures**

1. It is recommended that patients wanting to designate someone to make decisions about their personal health information on behalf of them do so in writing.
   1. All written appointments of a designate are scanned and stored in the patient’s record.

**People and Organizations Authorized to Exercise the Rights of Patients**

Any person or organization who seeks personal health information about a patient without consent will be requested to show [Physician Name] the authorization to receive the personal health information. PHIA gives this authority to the following individuals and organizations.

1. a person with written authorization from the individual who is the subject of the information to act on the individual’s behalf;
2. a substitute decision maker appointed by the individual in accordance with the Advance Health Care Directives Act, where the individual lacks the competency to exercise the right or power or is unable to communicate, and where the collection, use or disclosure of his or her personal health information is necessary for or ancillary to a "health care decision", as defined in the Advance Health Care Directives Act, or, where a substitute decision maker has not been appointed, a substitute decision maker determined in accordance with section 10 of the Advance Health Care Directives Act;
3. a court appointed guardian of a mentally disabled person, where the exercise of the right or power relates to the powers and duties of the guardian;
4. the parent or guardian of a minor where, in the opinion of the custodian, the minor does not understand the nature of the right or power and the consequences of exercising the right or power;
5. by the individual’s personal representative, where the individual is deceased, or, where there is no personal representative, by the deceased's Government of Newfoundland and Labrador Department of Health and Community Services 38 nearest relative, and for this purpose, the identity of the nearest relative may be determined by reference to section 10 of the Advance Health Care Directives Act;
6. where the individual is a neglected adult within the meaning of the Neglected Adults Welfare Act, by the Director of Neglected Adults appointed under that Act; or
7. where an individual has been certified as an involuntary patient under the Mental Health Care and Treatment Act, by a representative as defined in that Act, except as otherwise provided in this Act.

|  |  |
| --- | --- |
| Collection | |
| **Legislative Reference:** PHIA ss. 24, 29, 30, 31, 32 | **CPSNL Reference:** Bylaw 23.2(c)(vii) |
| **Policy Author:** | **Effective and Revision Dates:** |

**Policy**

[Physician Name] collects only the personal health information that is reasonably necessary to provide care and treatment to benefit patients.

**Procedures**

[Physician Name] must not collect personal health information about an individual unless:

* The individual who is the subject of the information has consented to its collection and the collection is necessary for a lawful purpose; or
* The collection is permitted or required by the Personal Health Information Act.

Consent to collect, use or disclose his or her personal health information may be express or implied. Within the circle of care, implied consent is relied on.

As is permitted under the Personal Health Information Act, [Physician Name] may collect personal health information about an individual without that individual's consent where the individual is incapable of providing consent and the collection is necessary for the provision of health care to the individual when:

* There is no authorized representative who can provide consent on behalf of the individual or, consent cannot be obtained in a timely manner; or
* The individual has been certified as an involuntary patient or is the subject of a community treatment order under the Mental Health Care and Treatment Act.

[Physician Name] must not collect personal health information if other information will serve the purpose of the collection, unless otherwise required by law.

Except as directed in PHIA, a [Physician Name] must collect personal health information directly from the individual who is the subject of the information.

[Physician Name] must not collect more personal health information than is reasonably necessary to meet the purpose of the collection unless there is a legal requirement to collect that information.

Consent directives limiting or withdrawing consent do not have the effect of restricting the recording of personal health information required by standards of professional or institutional practice.

|  |  |
| --- | --- |
| Use | |
| **Legislative Reference:** PHIA s.33 | **CPSNL Reference**: Advisory - Privacy, Confidentiality, and Disclosure of Patient Information |
| **Policy Author:** | **Effective and Revision Dates:** |

Note: The policies and procedures on Use and Disclosure may be combined.

**Policy**

[Physician Name] uses the minimum amount of personal health information necessary for the care and treatment of patients.

**Procedures**

1. [Physician Name] uses personal health information for
   1. The care and treatment of patients.
   2. The purpose the information was collected.
   3. A purpose consistent with patient care including arranging, assessing the need, providing, continuing to support health or services for the patient.
   4. Discussing with the patient’s next of kin, or someone the patient has a close personal relationship, the current health services being provided to the patient and the patient has not expressed a contrary intention to a disclosure of this type.
2. The clinic uses the least amount of personal health information necessary for the purpose.

3. All uses are consistent with the ethical practices of the medical profession.

1. Personal health information may be used without consent only as allowed in PHIA.
2. A patient may withdraw his or her consent for the use of personal health information and the medical practice will take reasonable steps to comply with the withdrawal promptly.
   1. A withdrawal of consent is not retroactive
3. Authorization to use personal health information is restricted to those who need it to meet the requirements of their role.
   1. Full access is provided all health providers at the clinic unless a patient restricts access to only [Physician Name].
   2. All employees and health professionals have access restricted through job descriptions, letters of engagement, and through technical features available in the EMR, including role-based access and masking.
4. Personal health information collected from patients is used by [Physician Name] for

Provision and continuity of care

* identify and contact patients
* historical record
* health promotion and prevention
* referral to specialists or other treating physicians
* requesting laboratory investigations
* requesting diagnostic tests
* generating prescriptions
* referral to other health care providers
* referral to home care agencies
* home care supervision

Billing

* billing provincial health plan
* billing third parties

1. Other uses authorized by PHIA

[Note: Include the uses that are most likely to happen in the clinic and include a reference to PHIA and the Reference Manual for other uses.]

**Health Care Delivery and Planning**

* For seeking the consent of the individual or his or her representative, where the personal health information used by the custodian for this purpose is limited to the name and contact information of the individual or the individual's representative;
* For the delivery of health care programs or services that are provided or funded by the custodian including planning, delivering, evaluating, monitoring or preventing fraud or unauthorized receipt of services or benefits;
* Where the custodian is a minister or a department, for the purpose of obtaining health care cost recovery;
* For obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health care or related goods and services;
* Where the custodian is a rights advisor under the Mental Health Care and Treatment Act for the performance of functions referred to in the Mental Health Care and Treatment Act, or;
* Where the custodian is an authority; a board, council, committee, commission, corporation or agency established by an authority, a department created under the Executive Council Act, or a branch of the executive government of the province, engaged in the delivery or administration of health care in the province; the minister, or the Centre for Health Information the following functions are permitted within the geographic area in which the custodian has jurisdiction:
  + planning and resource allocation,
  + health system management,
  + public health surveillance, and
  + health policy development.

**Quality and Risk Management Quality and Risk Management**

* Risk management or error management;
* Activities to improve or maintain the quality of care or activities to improve or maintain the quality of related programs or services, or;
* To prevent or reduce a risk of serious harm to:
  + the mental or physical health or safety of the individual the information is about or another individual; or
  + public health or public safety

**Proceedings or Legal Requirements**

* A proceeding or contemplated proceeding in which the custodian is or is expected to be a party or witness and the information relates to the proceeding, or;
* As permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada

**Research and/or Transforming into De- Identified Information**

* For research projects that are approved by a research ethics board or research ethics body under the Health Research Ethics Authority Act;
* Disposing information in compliance with the Act; or modifying it to conceal the identity of the individual who is the subject of the personal health information; or
* To produce information that does not, either by itself or in combination with other information in the custody of or under the control of the custodian, permit an individual to be identified.

1. [Physician Name] will not use or obtain access to personal health information about one of the clinic employees for any purpose related to that person’s employment without consent of the employee.

|  |  |
| --- | --- |
| Disclosure | |
| **Legislative Reference:** PHIA ss. 25, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, | **CPSNL Reference:** Bylaw 23.2 (c)(ix) |
| **Policy Author:** | **Effective and Revision Dates** |

**Policy**

[Physician Name] discloses personal health information as part of providing care to patients. If personal health information is disclosed for other purposes it will be with the consent of the patient or the disclosure is authorized without consent by law.

**Procedures**

1. Whenever possible, disclosures are noted in the patient charts. Sometimes this note is inferred by the completion of a prescription, requisition or other action.
2. A patient may withdraw his or her consent for the disclosure of personal health information and the medical practice will take reasonable steps to comply with the withdrawal promptly.
   1. A withdrawal of consent is not retroactive.
3. [Physician Name] discloses personal health information to other custodians who are health professionals in accordance with the ethical practices of the custodian’s profession.
4. [Physician Name] will ask any person or organization requesting personal health information the authority for the request to collect the personal health information, including with the patient’s consent.
5. When [Physician Name] is aware, or should reasonably be aware, that the personal health information was collected or disclosed in contravention of PHIA, [Physician Name] will not further disclose the personal health information without the consent of the patient.

**Express Consent**

1. Express consent is used for disclosures to non-custodians, such as schools, employers and insurance companies as required by PHIA.

**Implied Consent**

1. When personal health information is disclosed as part of the patient’s care to a health professional or another custodian, [Physician Name] relies on implied consent from the patient. Disclosures with implied consent may be for
   1. The care and treatment of the patient.
   2. Arranging, assessing the need, providing, and continuing to support a service requested or required by the patient.

**Disclosure without Consent**

1. **[**Physician Name] may disclose personal health information without the consent of the patient for:

**Health related purposes**

1. for the purpose of determining or verifying the eligibility of the individual to receive health care or related goods, services or benefits provided under an Act of the province or of Canada and funded in whole or part by the government of the province or of Canada;
2. for the purpose of determining or providing payment to the custodian for the provision of health care or for processing, monitoring, verifying or reimbursing claims for payment for the provision of health care;
3. to a department or the government of another jurisdiction or to an agency of that government to the extent necessary to obtain payment for health care provided to the individual who is the subject of the personal health information;
4. for the purpose of delivering, evaluating or monitoring a program of the custodian that relates to the provision of health care or payment for health care;
5. for the purpose of review and planning that relates to the provision of health care by the custodian;
6. to an information manager;
7. to a person who requires the personal health information to carry out an audit for, or provide legal services, error management services or risk management services to, the custodian;
8. to the Canadian Institute for Health Information or other entity prescribed in the regulations for the purpose of compiling and analyzing statistical information to assist in the management, evaluation and monitoring of the allocation of resources, health system planning and delivery of health care services in accordance with the terms of an agreement between the Canadian Institute for Health Information or other entity and the province;
9. to a potential successor of the custodian for the purpose of allowing the potential successor to assess and evaluate the operations of the custodian, on condition that the potential successor first enters into an agreement with the custodian to keep the information confidential and secure and not to retain the information any longer than is necessary for the purpose of the assessment or evaluation; and
10. to its successor where the custodian transfers records to the successor as a result of the custodian ceasing to be a custodian or ceasing to provide health care within the geographic area in which the successor provides health care and the successor is a custodian

**Law Enforcement**

There are situations in which [Physician Name] is required to disclose personal health information to law enforcement and others in which they may use their discretion:

*Mandatory disclosures*

[Physician Name] must disclose any personal health information required without the consent of that individual in the following situations:

* The disclosure is required by a provincial Act, federal Act or by a treaty, agreement or arrangement made under these Acts, to authorized recipients under those Acts or instruments.
* The disclosure is required to carry out or facilitate an inspection, investigation or similar procedure for the purpose that is authorized by or under:
* The Personal Health Information Act;
* The Child, Youth and Family Services Act;
* Another provincial Act; or
* An Act of Canada to authorized recipients under those Acts, where the disclosure is for the purpose of facilitating an inspection, investigation or similar procedure.

*Discretionary disclosures*

[Physician Name] is permitted to disclose personal health information without the consent of the individual to another custodian where [Physician Name] has a reasonable expectation that disclosure will:

* Detect or prevent fraud;
* Limit abuse in the use of health care; or
* Prevent the commission of an offence under an Act of the province or of Canada.

**Research and Secondary Uses**

[Physician Name] is permitted to disclose personal health information without the consent of the individual who is the subject of the information for the purposes of research where a research project has been approved by a research ethics board or research ethics body under the Health Research Ethics Authority Act.

[Physician Name] will not disclose personal health information if other information will serve the purpose of the disclosure.

**Registry**

[Physician Name] must disclose personal health information, without the consent of the individuals, to a custodian designated in the regulations under the Personal Health Information Act who maintains a registry for:

* Facilitating or improving the provision of health care; or
* Relating to the storage or donation of body parts or bodily functions.

**Outside the Province**

[Physician Name] is permitted to disclose personal health information to entities outside of the province of Newfoundland and Labrador under any of the following circumstances:

* The individual who is the subject of the information consents to the disclosure;
* The disclosure is permitted by the Personal Health Information Act or the regulations enacted under the Personal Health Information Act;
* The person receiving the information performs functions similar to the functions performed by the superintendent of a correctional facility or the administrator of a psychiatric unit in the province of Newfoundland and Labrador;
* The disclosure meets all the following conditions:
* The purpose of the disclosure is health planning or health administration;
* The information relates to health care provided in the province to a person who is a resident of another province or territory of Canada, and
* The disclosure is made to the government of that province or territory of Canada;
* The disclosure is reasonably necessary for the provision of health care to the individual; or
* The disclosure is reasonably necessary for the administration of payment or for contractual or legal requirements in connection with the provision of health care to the individual. If the custodian discloses personal health information about an individual with a limited consent directive in place and the personal health information is limited to less than the disclosing custodian considers reasonably necessary for the provision of health care to the individual, the custodian must notify the receiving entity of that fact.

|  |  |
| --- | --- |
| Disclosure of Personal Health Information to Relatives | |
| **Legislative Reference:** PHIA s. 37 and 38 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Templates:** N/A | |

**Policy**

Unless the disclosure is contrary to an express request of the individual, without the consent of the individual who is the subject matter of the information, [Physician Name] may disclose personal health information to a person other than a custodian for the purpose of contacting a relative, friend or potential substitute decision-maker of the individual, where the individual is injured, incapacitated or ill and unable to give consent personally. In such cases, the disclosure should be limited to the minimum amount of personal health information necessary.

**Procedures**

[Physician Name] is permitted to disclose personal health information about an individual who is a patient or resident in a health care facility operated by the custodian to a person that the custodian reasonably believes is a member of the individual's immediate family, a relative or a person with whom the individual has a close personal relationship where:

1. the custodian offers the individual the option, at the first reasonable opportunity after admission to the facility, to object to that disclosure and the individual does not do so; and,
2. the disclosure is made in accordance with accepted professional practice.

**Deceased Patients**

[Physician Name] may also disclose personal health information to relatives in the following situations where the individual is deceased or presumed to be deceased:

1. To identify an individual who is deceased or presumed to be deceased;
2. To inform a person that the individual is deceased or presumed to be deceased and the circumstances of the death, where appropriate;
3. To the personal representative of the deceased for a purpose related to administration of the estate of the deceased individual;
4. To allow the spouse, partner, siblings or descendants of a deceased individual to make decisions about his or her own health care or the health care of his or her child or where the disclosure is necessary to provide health care to the recipient.

|  |  |
| --- | --- |
| Disclosure of Personal Health Information to a Successor | |
| **Legislative Reference:** PHIA s. 39 | **CPSNL Reference: Policy – A Physician’s Responsibility when Permanently Closing a Medical Practice** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Templates:** N/A | |

**Policy**

[Physician Name] may disclose personal health information to a successor or potential successor in the event of closing or moving their practice.

**Procedures**

[Physician Name] may disclose personal health information to a successor or potential successor without the consent of individuals for the following purposes and under the following circumstances:

1. To provide a potential successor the opportunity to assess and evaluate the operations of [Physician Name] on condition that the potential successor first enters into an agreement with [Physician Name] to keep the information confidential and secure and not to retain the information any longer than is necessary for the purpose of the assessment or evaluation; or
2. [Physician Name] may transfer records to the successor as a result of [Physician Name] ceasing to be a custodian or ceasing to provide health care within the geographic area in which the successor provides health care and the successor is a custodian.

When transferring personal health information to another custodian, [Physician Name] will make reasonable efforts to inform individuals whose information is to be transferred, ninety days prior to the transfer taking place. Notice may include:

* By a letter to the patient;
* Directly at the time of an office visit;
* By a notice in the physician’s office; and
* By a telephone answering service.

When prior notice of the transfer is not possible, information regarding the transfer will be made available by way of public notice of the transfer.

The public notice will contain the following information:

1. That [Physician Name] has ceased or will cease to be a custodian within the jurisdiction;
2. The identity and contact information of the successor; and
3. How a patient may access his or her record after the transfer.

|  |  |
| --- | --- |
| Disclosure of Personal Health Information for Health and Safety Purposes | |
| **Legislative Reference:** PHIA s. 40 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Templates:** N/A | |

**Policy**

[Physician Name] may disclose personal health information without the consent of an individual where [Physician Name] reasonably believes that disclosure is required:

1. To prevent or reduce a risk of serious harm to the mental or physical health or safety of the individual the information is about;
2. To prevent or reduce a risk of serious harm to the mental or physical health or safety of another individual; or
3. For public health or safety.

[Physician Name] is permitted to disclose personal health information without the consent of that individual to the superintendent of a correctional facility in which the individual is lawfully detained or to the administrator of a psychiatric unit in which the individual is detained to assist the facility or unit in making a decision respecting the following:

* Making arrangements for the provision of health care to the individual; or
* Placing the individual into custody, detention, release, conditional release, discharge or conditional discharge under the following:
  + - Mental Health Care and Treatment Act;
    - Prisons Act;
    - Young Persons Offences Act and regulations under that Act;
    - Part XX.1 of the Criminal Code;
    - Prisons and Reformatories Act (Canada); and
    - Youth Criminal Justice Act (Canada).

|  |  |
| --- | --- |
| Disclosure of Personal Health Information for Legal Proceedings | |
| **Legislative Reference:** PHIA s. 41 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Templates:** N/A | |

**Policy**

There are situations in which [Physician Name] is required to disclose personal health information for legal proceedings and others in which they may use their discretion:

*Mandatory disclosures*

[Physician Name] is obligated to disclose personal health information without the consent of that individual, in the following situations:

* To a body responsible for the discipline of a health care professional or for the quality or standards of professional services provided by a health care professional, including an investigation by that body; or
* For the purpose of complying with a summons, subpoena, warrant, demand, order or similar requirement issued by a court, person or entity, including the commissioner, with jurisdiction to compel the production of personal health information or with a rule of court concerning the production of personal health information in a proceeding.

*Discretionary disclosures*

[Physician Name] may decide to disclose personal health information without the consent of the individual for the following purposes:

* A proceeding or contemplated proceeding in which the custodian is or is expected to be a party or a witness where the information relates to or is a matter in issue;
* A committee as referred to in subsection 8.1(2) of the Evidence Act;
* To a proposed guardian or legal representative for the purpose of the appointment of a person as a guardian or representative for an individual;
* To a guardian authorized under an Act of the province or the Rules of the Supreme Court, 1986, to commence, defend or continue a proceeding on behalf of the individual or to represent the individual in a proceeding; or
* For the purpose of laying an information, order or making an application for an order where the personal health information relates to or is a matter in issue in the information or application.

|  |  |
| --- | --- |
| Managing Patient Consent and Masking in the EMR | |
| **Legislative Reference:** PHIA s. 27, 28 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Templates:** Consent Directive and Masking Request Form, Access to Personal Health Information Request Form | |

**Policy**

[Physician Name] will take all reasonable steps to comply with a patient’s request to limit the collection, use and disclosure of their personal health information in the EMR.

**Procedure**

**Accepting Consent Directives**

1. When personal health information is collected, used or disclosed solely for health care purposes [Physician Name] relies on implied consent from the patient.
2. A request to limit, restrict, or withdraw consent will be accepted at any time.
   1. The clinic privacy poster will include information on a patient’s right to limit access to their personal health information, including masking it.
3. [Physician Name] will use the masking functionality in the EMR to restrict the use and disclosure of the patient’s personal health information in accordance with the patient’s consent directive.

**Explaining Collection, Uses and Disclosures Mandated by Law**

1. Anyone collecting, using, or disclosing personal health information will explain the authority for the action if a patient wants to limit consent for that activity.

**Explaining the Benefits and Risks of Masking and Limiting Disclosure and Use**

1. When the authority for the collection, use or disclosure allows for the patient to limit, restrict, or withdraw consent the consent directive is met to the best of the clinic’s ability.
2. Anyone collecting the personal health information will explain the benefits and risks of the consent directive if there are any. This may include
   1. Essential information is not available in a timely manner.
   2. Not all members of the care team will have access to the needed information to provide appropriate care.
   3. Staff will be unable to check whether the patient’s results, specialist reports, etc. are available before booking an appointment for the patient with [Physician Name]. Staff will not be able to assist the physician in making specialist referrals, sending requisitions for diagnostic services, procedures, or prepare billing work for the physician.
   4. In extreme cases, when a patient refuses to allow an override of the mask, care may be denied because of lack of information and the patient will have to wait until [Physician Name] is available.

**Alternatives to Masking**

1. [Physician Name] will advise the patient of alternatives to masking.
   1. The Office Manager can provide printed audit reports to the patient.
   2. [Physician Name] will also consider alternative solutions suggested by the patient that will not be in contravention of any law or ethical practice by a physician.

**Process for a Patient to Give a Consent Directive**

1. When the patient informs [Physician Name] that they wish to limit the access, collection, use or disclosure of their personal health information.
   1. A Consent Directive and Masking Request Form is completed, scanned and held as part of the EMR record.
   2. A simple restriction on a use or disclosure is noted in the patient’s record and the record is flagged.
   3. Patients wanting an audit of their record should complete the Access to Personal Health Information Request Form.

**Unmasking a Record/Overriding a Consent Directive**

1. Only [Physician Name] and the Office Manager have the authority to unmask a record in the EMR or in any other way override a patient’s consent.
   1. When a record is unmasked the reason must be indicated. The reasons include:

* Patient Consent
* Provider Consent because of safety concerns related to the patient
* Access is required to complete, verify or document a previously provided health service requested or required by the patient
* Access is required for billing
* Access for use or disclosure is required by law
  1. The person authorized to unmask the record in the EMR should also indicate the time period the record is to remain unmasked. The users should select the minimum time necessary to fulfill the identified purpose for the unmasking.
  2. All masked records should be audited and reviewed at regular intervals.

|  |  |
| --- | --- |
| Agreements | |
| **Legislative Reference:** PHIA s. 22 | **CPSNL Reference:** Bylaw 6 |
| **Policy Author:** | **Effective and Revision Dates:** |

**Policy**

[Physician Name] uses written agreements to establish responsibilities and mitigate risk when third parties have or may have access to personal health information on behalf of the practice.

**Procedures**

[Physician Name] must ensure that all agreements between custodians and information managers:

* Be in writing;
* Provide for the protection of personal health information against unauthorized access, use, disclosure, disposition, loss or modification in compliance with the Act;
* Specify the purposes for which the information manager may use and disclose personal health information, and must set out all applicable restrictions to such use(s) and / or disclosure(s);
* Contain a meaningful description of all of the personal health information maintained by the information manager;
* Document the security measures used by the information manager to protect the personal health information in its custody or control;
* Identify the situations under which the information manager may disclose personal health information to another person or entity;
* Identify all stakeholders involved in the management of the personal health information including contractors or subcontractors and define the relationships with the identified individuals or groups;
* Reference any other related Service Level Agreements pertaining to the custodian / information manager relationship;
* Permit the custodian to review the policies and procedures of the information manager related to the protection and management of personal health information to verify they are consistent with those of the custodian; and
* Define notification and other change management processes as they relate to the provision of services by the information manager.

The information manager must agree to:

* Comply with the Personal Health Information Act and with the provisions of the agreement, and must acknowledge both obligations in the agreement;
* Report any breaches of the personal health information;
* Upon termination return information in a mutually acceptable format; and
* Adhere to the policies and procedures of the custodian.

|  |  |
| --- | --- |
| Management of Breaches | |
| **Legislative Reference:** PHIA ss. 20, 44 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Templates:** Privacy and Security Breach Reporting Form, Breach notification letter | |

**Policy**

[Physician Name] considers a privacy breach as a collection, use or disclosure of personal health information in contravention of the *Personal Health Information Act* and these policies. [Physician Name] responds promptly to potential, suspected and confirmed privacy and security breaches and will engage the necessary expertise in managing breaches.

**Procedures**

1. The first person aware of the suspected breach will take actions to stop or contain, the breach if it is ongoing,
   1. Anyone aware of a suspected breach shall notify the Office Manager or [Physician Name].
2. [Physician Name] and the Office Manager will work to ensure
   1. Unauthorized copies of the personal health information are retrieved, or notification of the destruction of the information is received. The notification of destruction includes the type of information that was involved in the suspected breach and how it was destroyed.
   2. Disconnection of the EMR, and other information systems, from the Internet and the Network if they have been compromised. Oak Computing Services is contacted to assist in containing the suspected breach and investigation.
   3. Until an investigation of the unauthorized access can be completed, the user account of the individual in question should be deactivated. Note: As it should be a requirement of the individual’s duties to have access to the system, the investigation should be conducted immediately.

**Investigation and Analysis**

1. [Physician Name] leads an internal investigation into the suspected breach which includes
   1. Establishing an investigation team with the necessary expertise which may include experts in information technology, NLCHI, and other custodians who may have their own accountability for the information.
   2. Understanding the circumstances of the breach and determining if it was a breach of personal health information.
   3. Examining physical and technical security and business process for a role in the breach.
   4. Identifying anyone who may have had unauthorized access to the personal health information through the examination of the audit logs of the EMR.
   5. The Office Manager thoroughly documents the breach using the form developed by eDOCS NL.
   6. Determine if an actual breach occurred.

**Notification of Others**

1. Key stakeholders are contacted as appropriate for the breach
   1. If the breach involves information from the EHR it should be reported to the NLCHI Service Desk at 1-877-752-6006.
   2. If the breach involves information received from another custodian, that custodian is contacted.
   3. If the breach involves information from a person who is not a custodian, that person is contacted.
   4. The Office of the Information and Privacy Commissioner of Newfoundland and Labrador may be contacted for assistance and advice on managing the breach or on the notification of patients.

Telephone:  (709) 729-6309

Toll Free in Newfoundland and Labrador: 1-877-729-6309

* 1. The Office of the Information and Privacy Commissioner of Newfoundland and Labrador must be notified of a material breach. Such a breach may cause significant harm to the patients whose information was breached, involves a large number of patients, or is systemic in nature.
  2. Contact the police if there is possible criminal activity.
  3. The EMR vendor is contacted if the breach is related to the EMR.
  4. Contact the Health Ethics Board (HREB) if the breach involves personal health information used in a clinical trial or other research approved by the HREB.
  5. Contact legal counsel and insurers if deemed appropriate.

**Notification of Patients**

1. Patients are notified as soon as possible after the breach and the potential harm to the patient is understood.
   1. Patients are notified when there is a real risk of significant harm to
      * the provision of health care or other benefits to the patient and/or
        + the mental, physical, economic or social well-being of the patient.
   2. Notification of patients is made by telephone, mail or at the next appointment, depending on the seriousness of the breach.
   3. A notification to a patient about a breach includes

* the date of breach,
* details of the extent of the breach and the type of personal health, information involved,
* the potential risks to the patient,
* the steps that have been taken to address the breach both in the immediate and long term,
* how the patient can contact the Office of the Information and Privacy Commissioner of Newfoundland and Labrador.

1. [Physician Name] may contact the Office of the Information and Privacy Commissioner of Newfoundland and Labrador to assist in determining the most appropriate method of notifying patients.

**Prevention**

1. Document recommendations and develop strategies to minimize future risks at the medical practice.
2. The Office Manager ensures that the containment and notification recommendations of this policy have been met.
3. [Physician Name] ensures the disciplinary policy is followed if an employee is involved in an intentional breach.
   1. If a health professional is involved in an intentional breach, [Physician Name] will contact the appropriate regulatory body.
4. If the breach occurred at an Information Manager the contract will be reviewed.
5. The Office Manager reviews these policies and procedures after the completion of the investigation and makes any necessary changes based on the lessons learned.
6. The Office Manager arranges for additional training based on lessons learned.
7. [Physician Name] cooperates with any and all investigations by the Office of the Information and Privacy Commissioner of Newfoundland and Labrador into a breach of privacy at the clinic.
8. [Physician Name] cooperates with any and all investigations by eDOCS NL into a breach of privacy involving the EHR.

**Penalties**

1. When accesses are deemed inappropriate, the Privacy Officer determines if it was willful or unintentional.
   1. Users who unintentionally access personal health information inappropriately are subject to all or any of the following:

* further privacy training
* loss of privileges to use the EMR
* suspension without pay for one day
  1. Users who willfully access personal health information inappropriately are subject to all or any of the following
* further privacy training
* loss of privileges to use the EMR
* suspension without pay for up to five days
* possibility of charges under PHIA
* dismissal

|  |  |
| --- | --- |
| Business Continuity Plan | |
| **Legislative Reference: PHIA** s 15 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |

**Policy**

[Physician Name] maintains up-to-date business continuity plan that provide guidance on how to manage an interruption in business due to unplanned events.

**Procedures**

1. The business continuity plan includes
   1. Emergency contact numbers
   2. Employees contact numbers
   3. Vendor and other third party contact numbers with account numbers for the medical practice
   4. Recommended alternative sites for patients to receive care
   5. A plan on how to notify patients if their appointment is cancelled or they should go to an alternate location.
2. The business continuity plan will be reviewed annually and updated as necessary.

|  |  |
| --- | --- |
| Storage, Retention, and Destruction of Paper Records | |
| **Legislative Reference:** PHIA s. 13 | **CPSNL Reference:** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Template:** Record of Destruction | |

**Policy**

[Physician Name] retains paper records, which have not been scanned into the EMR, for 10 years after the last entry into the patient record, whether it is the paper record or the EMR. In the case of a patient who at the date of last provision of service was under the age of nineteen (19) years, until that patient attains the age of twenty-one (21) years or for ten (10) years following the date of last provision of service to that patient, whichever is the longer period. [Physician Name] stores and destroys all records securely.

**Procedures**

1. Once a year the Office Manager removes the records of patients who have been inactive for five years. Paper records are placed in banker boxes.
   1. The Office Manager prepares a list of all records selected for archiving; the number of the banker box the record is stored and signs the list.
   2. The list contains
      * + patient name and health services number
        + physician name
        + last year an entry was made in the record.
   3. The list is confirmed for accuracy by one other person who also signs the list.
   4. [Physician Name] reviews the list of records for archiving and signs the list.
   5. The banker boxes are sealed and initialed by the Office Manager.
2. The Office Manager arranges for [Information Manager] to pick up the banker boxes and place them in storage.
3. Annually, the Office Manager prepares a list of paper records that can be destroyed according to the Policy.
   1. The Office Manager ensures that the patient has not returned to the practice under a different name or health services number.
   2. The Office Manager reviews the list of records that belong to patients that have not been active in the clinic in over six years with [Physician Name].
   3. The list of records to be destroyed is signed by [Physician Name].
4. The Office Manager contacts [Information Manager] to confirm the records that are to be destroyed. A copy of the signed list of records is sent by bonded courier or encrypted email to the company.
   1. After the company has confirmed by email they have the records on the list they proceed with destroying the records by shredding.
   2. After the shredding of the records [Information Manager] sends a letter signed by the manager of the shredding operation and at least one other employee involved in the shredding of the records confirming the destruction.
5. A record of destruction is kept by the Office Manager with

* description of information destroyed
* date the information was destroyed
* how the information was destroyed
* why the information was destroyed
* who destroyed the information.

**Information Management Agreement**

1. [Physician Name] has signed an IM agreement for secure storage and destruction of paper and electronic records with

* [List IM Companies]

1. The IM agreement includes
   1. All IM employees are bonded and sign an oath or affirmation of confidentiality with the supplier.
   2. The IM premises are monitored 24 hours a day, seven days a week.
   3. There are environmental controls against damage to the records from water, fire and insects.
   4. [Physician Name] or a representative may visit the premises annually to review security practices.
   5. The IM is knowledgeable of PHIA and adheres to its requirements.

|  |  |
| --- | --- |
| Scanning and Destruction of Paper Records | |
| **Legislative Reference:** | **CPSNL Reference:** CMPA Duties and Responsibilities when Transitioning to Electronic Medical Records |
| **Policy Author:** | **Effective and Revision Date:** |

**Policy**

The accuracy of scanned records is confirmed before the paper document(s) are destroyed.

**Procedures**

1. The Office Manager will train the office assistant on the procedure for scanning documents of personal health information.
2. All scanned documents are saved as PDF, a read only format.
3. The person scanning the document shall review the scanned document to ensure it is readable and copied completely.
4. The scanned document is named and filed according to clinic procedures.
5. The paper documents are placed in the designated secure receptacle which is locked by the Office Manager.
6. Once a month the Office Manager will randomly select documents from the receptacle and perform a complete quality assurance test to ensure the scanned document is accurate, complete, retrievable, readable and useable.
7. When the quality assurance procedure has been completed all documents in the secure receptacle are securely shredded.

|  |  |
| --- | --- |
| Backups and Storage | |
| **Legislative Reference:** PHIA s. 13, 15 | **CPSNL Reference:** Bylaw 6 |
| **Policy Author:** | **Effective and Revision Dates:** |

**Policy**:

[Physician Name] will ensure that Telus Health maintains a secure backup of all EMR records. Other electronic administrative records will securely backed up by the Clinic.

**Procedures**

1. The Office Manager carries out the duties related to backups.

**Vendor Backups**

1. The Telus Health will manage all backups.

**Offsite Backups**

1. [Physician Name] has contracted [Information Manager] to perform daily remote backups of other records.
2. The Office Manager ensures there is a successful backup each day.

**Administrative Records**

1. Electronic administrative records that are inactive for five years are copied onto an encrypted hard drive storage device by the Office Manager.
   1. Each year when new files are added the Office Manager confirms that previously stored records are accessible and readable.
   2. Administrative records that remain inactive for an additional two years are deleted from the storage device.

**Recovering Information from Backup Devices**

1. If the information on the EMR becomes corrupt, the hard drive crashes or the server is stolen; Telus Health is contacted to recover the information on the backup and to transfer it to an operating server.

|  |  |
| --- | --- |
| User Account Management | |
| **Legislative Reference:** PHIA s. 48 | **CPSNL Reference:** Bylaw 6 |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Templates:** Acceptable Use Agreement | |

**Policy**

Each person with access to the EMR and the office computers will have their own user name and password.

**Procedures**

1. The Office Manager manages the creation and deletion of user accounts and has the administrative rights to change the privileges for each user.
2. Before each user is assigned access to the EMR or other information system they are required to sign an Acceptable Use Agreement.
3. A user name and password is the equivalent of a signature for ensuring users only access the personal health information they need to know to perform their role.
4. Each user will be authorized to view, use, collect, disclose, create, correct and mask the personal health information according to the requirements of that person’s position.
5. A user’s account is suspended should any concerns arise about the use of the account. If the issue is resolved, the account will be re-activated.

**Passwords**

1. Users select their own passwords which are a minimum of eight characters and are a combination of numbers, letters, symbols, and upper and lower case.
2. [Physician Name] will update the “Password Expiry Interval” to remind users to change passwords every three months. A 5 day warning should be given.
3. Passwords should never be shared with anyone else.

**Penalties**

1. When accesses are deemed inappropriate the Privacy Officer determines if it was willful or unintentional.
   1. Users who unintentionally access personal health information inappropriately are subject to all or any of the following:

* further privacy training
* loss of privileges to use the EMR
* suspension without pay for one day
  1. Users who willfully access personal health information inappropriately are subject to all or any of the following
* further privacy training
* loss of privileges to use the EMR
* suspension without pay for up to five days
* possibility of charges under PHIA
* dismissal

|  |  |
| --- | --- |
| Auditing | |
| **Legislative Reference:** PHIA s. 48 | **CPSNL Reference:** Bylaw 6 |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Template:** Access to Personal Health Information Form | |

**Policy**

[Physician Name] monitors all activity in the EMR by employees and health professionals. Audit reports regarding patient records are made available to patients upon request.

**Procedures**

1. [Physician Name] maintains an EMR that has the ability to audit users of the system.
   1. All employees and health professionals are aware of the auditing of all of their activities in the EMR.
   2. All employees are aware that [Physician Name] is notified automatically on all accesses and attempted accesses to masked information, all overrides of masking, and all accesses to flagged patient records.
   3. The Office Manager is authorized to run regular audit reports to be reviewed by the [Physician Name].
2. Audit reports will be created if there is a suspected breach, for random reviews of user activities or at the request of a patient.

**Information Captured in Audit Logs**

1. The audit logs capture information required by CPSNL, information useful to patients and information necessary to monitor user activity of the EMR. The information captured in the audit logs

* name of the patient
* name of user
* date and time of access
* information that was accessed
* action performed related to personal health information – create, add, modify, delete, view, or disclose
* who the information was disclosed to
* preserves the original content of the recorded information when changed or updated
* accesses to masked information
* overrides of masked information
* failed attempts to access masked information
* changes in consent directives
* successful and failed login attempts.

**Patient Requests and Complaints**

1. Patients requesting an audit report of users should complete the Access to Record Request Form.
2. The Office Manager prepares all audit reports requested by patients and [Physician Name] reviews and signs the report before it is given to the patient.
3. Audit Reports provided to patients must include a letter detailing the reason for access to their record.

**Monitoring Program**

1. [Physician Name] reviews a random selection of audit reports once per week.
   1. At least one report reviewed is by user for a minimum one week period.
   2. At least one report reviewed is by patient over a minimum one week period.
2. [Physician Name] receives all alerts sent automatically by the EMR and reviews for inappropriate access.
3. When accesses are deemed inappropriate [Physician Name] determines if it was willful or unintentional.
   1. Users who unintentionally access personal health information inappropriately are subject to all or any of

* further privacy training
* loss of privileges to use the EMR
* suspension without pay for one day
  1. Users who willfully access personal health information inappropriately are subject to all or any of
* further privacy training
* loss of privileges to use the EMR
* suspension without pay for up to five days
* possibility of charges under PHIA
* dismissal

1. Patients are notified of the breach in accordance with the Management of Breaches Policy.

|  |  |
| --- | --- |
| Destruction of Office Equipment and Medical DevicesRetaining Personal Health Information | |
| **Legislative Reference:** N/A | **CPSNL Reference:** N/A |
| **Policy Author:** | **Effective and Revision Dates:** |

**Policy**

[Physician Name] ensures that all personal health information is removed from the office equipment and medical devices before the devices are recycled or destroyed.

**Procedures**

1. Neither the office equipment nor medical devices will be disposed of in the regular garbage or recycling.
2. The Office Manager maintains a list of office equipment and medical devices that could possibly retain personal health information. The list of such devices as of [date] is:

* [List of devices]

1. A record of destruction is kept by the Office Manager with the following information

* description of information potentially on the device
* when the device was destroyed
* how the device was destroyed
* why the device was destroyed
* who destroyed or recycled the device

1. Any device retaining the primary source of the personal health information is examined by the Office Manager to ensure the information has been properly transferred to the replacement device. The old device is not destroyed until the Office Manager has confirmed the accuracy and integrity of the transferred information.
   1. This procedure applies to:
      * client server

* laptop computers
* desktop computers

1. [Information Manager] is contracted to destroy all devices securely.

|  |  |
| --- | --- |
| General Security Software | |
| **Legislative Reference:** PHIA s. 15 | **CPSNL Reference:** N/A |
| **Policy Author:** | **Effective and Revision Dates:** |

**Policy**

[Physician Name] maintains security software licenses that provide regular updates to the firewall, anti-virus, malware and the virtual private network software.

**Procedures**

1. The Office Manager maintains a license for security services which includes firewall protection, encryption for emails, and scanning emails for viruses.
2. All servers, computers, USB keys and mobile devices purchased by the clinic will include encryption capabilities.
3. The Office Manager maintains other security software update licenses as appropriate.
4. The Office Manager reviews the security updates from the EMR vendor monthly to ensure updates have been received and installed.

|  |  |
| --- | --- |
| Security of the Office | |
| **Legislative Reference:** PHIA s. 15 | **CPSNL Reference:** N/A |
| **Policy Author:** | **Effective and Revision Dates:** |

**Policy**

[Physician Name] ensures that the medical practice’s physical office space is secure.

**Procedures**

1. [Physician Name] has signed a lease with the landlord that stipulates the hours the exterior doors are locked.
   1. Access to the building after hours is monitored by a swipe card entry system that records the ID number of the person entering the premises and records the time the person enters and leaves the building.
   2. The landlord has provided an alarm system for the office.
   3. [Physician Name] has a contract with [Security Company Name] to monitor the alarm system.
2. The Office Manager manages the office keys and the opening and closing of the office each day.
   1. All physicians are provided with a key to the office door and to their own office and examination rooms.
3. Monitors, printers, and fax machines are placed where patients, unauthorized staff and others cannot see the personal health information on them.
   1. The server is in an environmentally safe area and secured to the floor or wall, or place in a locked cupboard.
4. Portable equipment such as laptops, external hard drives, USB keys, CDs should be stored in a secure location and use a lockable box to store and transport small storage media devices.
   1. Portable equipment is never left unattended when taken outside the office, such as in cars or the hospital cafeteria.
   2. All portable equipment has strong encryption capabilities and all personal health information on portable equipment is encrypted.
   3. Physicians, employees and third parties are required to lock screen or log off whenever they leave their workstation unattended. Use CTRL, ATL, DELETE.
5. All computers are password protected.

|  |  |
| --- | --- |
| Use of Cameras for Patient Care | |
| **Legislative Reference:** PHIA s. 15 | **CPSNL Reference: n/a** |
| **Policy Author:** | **Effective and Revision Dates:** |
| **Associated eDOCS NL Documents and Templates:** N/A | |

**Policy**

[Physician Name] ensures that photographs taken during the provision of care will be protected in accordance with the clinic’s policies and procedures.

**Procedures**

1. [Physician Name] will only use the Med Access Mobile Application to collect pictures take during the provision of care.
   1. Photographs captured via the Med Access Mobile App are not stored on the device, but are uploaded via 256 bit HTTPS/SSL encrypted connection and deleted from the device after upload.