Privacy and Security Reference 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. 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

Acronyms

CPSNL – College of Physicians and Surgeons of Newfoundland and Labrador

EHR – Electronic Health Record

EMR – Electronic Medical Record

PHIA – the *Personal Health Information Act*

OIPC – Office of the Information and Privacy Commissioner of Newfoundland and Labrador

PIPEDA – *Personal Information Protection and Electronic Documents Act*

REB – Research Ethics Board

Glossary

Access means to obtain, view or retrieve information

- Access may be used in relation to the patient's right to review and/or obtain a copy of his or her medical record
- Access may be used in relation to the act of viewing information in the EMR

Agent *in relation to a custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian,* PHIA 2(1)(a).

Circle of Care in the context of consent as outlined in PHIA section 24(2); means *the persons participating in and activities related to the provision of health care to the individual who is the subject of the personal health information and includes necessarily incidental activities such as laboratory work and professional consultation, PHIA 24(3).*

Collect, *in relation to personal health information, means to gather, acquire, receive or obtain the information by any means from any source and "collection" has a corresponding meaning, PHIA 2(1)(d).*

Commissioner *means the Information and Privacy Commissioner appointed under the Access to Information and Protection of Privacy Act, 2015,* PHIA 2(1)(e).

Contact Person is a person designated by a Custodian to perform the functions outlined in PHIA. This person may also be referred to as a Privacy Officer.

Consent means to provide permission

Custodian means a person who has custody or control of personal health information. Section 4 of PHIA outlines the following as custodians*:*

a) an authority;
b) a board, council, committee, commission, corporation or agency established by an authority;
c) a department created under the Executive Council Act , or a branch of the executive government of the province, when engaged in a function related to the delivery or administration of health care in the province;
d) the minister, where the context so requires;
e) a health care professional, when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;
f) a health care provider;
g) a person who operates
    a. a health care facility,
    b. a licensed pharmacy as defined in the Pharmacy Act, 2012 ,
    c. an ambulance service, or
    d. a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health

care provider;

h) *the Provincial Public Health Laboratory;*
i) *the Centre for Health Information;*
j) *with respect to Memorial University of Newfoundland, the Faculty of Medicine, the School of Nursing, the School of Pharmacy and the School of Human Kinetics and Recreation;*
k) *the Centre for Nursing Studies;*
l) *the Western Regional School of Nursing;*
m) *a person who, as a result of the bankruptcy or insolvency of a custodian, obtains complete custody or control of a record of personal health information, held by the custodian;*
n) *a rights advisor under the Mental Health Care and Treatment Act;*
o) *the Workplace Health, Safety and Compensation Commission; and*
p) *a person designated as a custodian in the PHIA regulations.*

Custody means the physical and legal responsibility for information.

Disclose *in relation to personal health information in the custody or control of a custodian or other person, means to make the information available or to release it but does not include a use of the information and "disclosure" has a corresponding meaning,* PHIA 2(1)(g).

Electronic Health Record (EHR) means a secure and private lifetime record of an individual's key health history and care within the health system. The record is available electronically to authorize healthcare providers and the individual in support of high quality care.

Electronic Medical Record (EMR) means a computer-based patient record system. It is sometimes extended to include other functions, such as order entry for medications and tests. For the purposes of this document, EMR is the system used in physicians' offices.

Health Care Provider *means a person, other than a health care professional, who is paid by MCP, another insurer or person, whether directly or indirectly or in whole or in part, to provide health care services to an individual,* PHIA 2(1)(k).

Information Manager *means a person or body, other than an employee of a custodian acting in the course of his or her employment, that*

- *processes, retrieves, stores or disposes of personal health information for a custodian, or*
- *provides information management or information technology services to a custodian,* PHIA 2(1)(l).

Personal health information is outlined in section 5 of PHIA and means identifying information in oral or recorded form about an individual that relates to:

a) *the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family;*
b) *the provision of health care to the individual, including information respecting the person providing the health care;*
c) *the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;*

d) *registration information;*
e) *payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;*
f) *an individual's entitlement to benefits under or participation in a health care program or service;*
g) *information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;*
h) *a drug as defined in the Pharmacy Act, 2012 , a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or*
i) *the identity of a person identified as a representative in relation to care*

Privacy breach means any unauthorized collection, use or disclosure of personal health information. In essence, a privacy breach occurs whenever a person has contravened or is about to contravene a provision of PHIA, or of the regulations passed under PHIA. Furthermore, if the criteria of a material breach is met, it must be reported to OIPC.

Primary purpose means the purpose for which personal health information was originally collected, and includes any purpose that is consistent with that purpose.

Privacy is a broad concept which involves the right of the individual to exercise a measure of control over his or her personal health information. It involves the decision of the individual about what personal health information will be disclosed to a custodian and for what purposes. It captures both security and confidentiality which are subsets of privacy.

Privacy Officer see contact person.

Record *means a record of personal health information in any form, and includes personal health information that is written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produces records on a storage medium, PHIA (2)(1)(s).*

Registration information *means information about an individual that is collected for the purpose of registering the individual for the provision of health care, and includes a health care number and other identifier assigned to an individual, PHIA 2(1)(t).*

Research *means a systematic investigation designed to develop or establish principles or facts or to generate knowledge, or any combination of principles, facts and knowledge, and includes the development, testing and evaluation of research, PHIA (2)(1)(v)*

Secondary uses means the use or disclosure of information for a purpose other than that for which it was originally collected, which is a program activity or service related to patient care. An example is the collection, use, and disclosure of personal health information for billing purposes.

Security means the procedures and systems used to restrict access, and to protect and maintain the integrity of the personal health information.

Third Parties means individuals and organizations who provide a service to a clinic that will, or may, require them to come in contact with personal health information but who are not custodians, employees, health professionals, medical students, residents.

Use*, in relation to personal health information in the custody or control of a custodian, means to handle or deal with the information or to apply the information for a purpose and includes reproducing the information, but does not include disclosing the information,* PHIA (2)(1)(aa)*.*

Purpose of the Personal Health Information Act
(PHIA s. 4)

The purposes of the *Personal Health Information Act are:*

- *to establish rules for the collection, use and disclosure of personal health information that protect the confidentiality of that information and the privacy of individuals with respect to that information;*

- *to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in PHIA;*

- *to provide individuals with a right to require the correction of personal health information about themselves, subject to limited and specific exceptions set out in PHIA;*

- *to establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control;*

- *to provide for an independent review of decisions and resolution of complaints with respect to personal health information in the custody or control of custodians; and*

- *to establish measures to promote the compliance with PHIA by persons having the custody or control of personal health information.*

Instructions

Using the Privacy and Security Reference Manual

As part of eDOCSNL implementation it is recommended that anyone creating a privacy and security policy manual for a clinic read **Steps in Creating a Privacy and Security Policy Manual** first.

Throughout the **Reference Manual** the term "custodian" is used. This term is a reminder that physicians who are custodians under PHIA have a different legal accountability than physicians who are employees, medical students or residents, of another custodian, such as a regional health authority. This **Reference Manual** provides guidelines for physicians to use in interpreting PHIA. These guidelines do not constitute legal advice. It is divided into sections of related policy topics.

- There are several general responsibilities that a custodian must meet and these are covered in the Accountability section. This section discusses the roles and responsibilities of a privacy officer and the obligations of employees, medical students and residents, and others who are subject to the policies and procedures and other requirements of PHIA.
- PHIA is very specific about patients' rights to have access to their own personal health information and to ask for corrections when a record is inaccurate or incomplete. This section also includes information about representatives and substitute decision makers.
- The third section is about the consent related to the collection, use and disclosure of a patient's personal health information. This does not include consent for treatment or service. There are several restrictions and authorizations in PHIA on the collection, use, and disclosure of personal health information.
- The Safeguards section contains overviews of some of the tools that physicians can use to mitigate risks, such as agreements, and breach. While these are not explicitly outlined in PHIA, they will help physicians meet some of their general duties to protect personal health information.
- This is followed by guidelines on other safeguards, including retention, storage, and destruction of records. This section provides advice only to electronically stored information.

When the word "shall" or "must" is used in the **Privacy Resource Materials** it means it is a requirement under PHIA. "May" is used, as it is in PHIA, when a physician has discretion in how the PHIA requirement is met. "Should" and "recommended" generally refers to the expectations of the College of Physicians and Surgeons and the industry best practice.

To assist your clinic in carrying out its privacy and security program, you may want to develop additional checklists to supplement these materials; ensuring all required activities are completed.

For additional information, useful reference materials include:

- the NLMA's, CPSNL's, and CMPA's[1] websites,
- relevant policies from any RHA with which personal health information is shared,
- The Newfoundland and Labrador Department of Health website[2]
- the Office of the Information and Privacy Commissioner website[3]

[1] https://www.cmpa-acpm.ca/en
[2] http://www.health.gov.nl.ca/health/
[3] http://www.oipc.nl.ca/

Accountability

Custodians

(PHIA s. 4)

PHIA establishes the rules and responsibilities for custodians in the protection of patient privacy and the security of their personal health information. All physicians implementing an EMR need to understand the concept of a custodian under PHIA, and how to determine if they are one.

Determining if a Physician is a Custodian under the *Personal Health Information Act*

For physicians to determine if they are a custodian, they should consider the following questions, 1) are they an employee, and 2.) do they have custody or control of the personal health information they collect?

Is the physician an employee of a Custodian? (see the definition of custodian in the Glossary) If so, the physician is not a custodian. If the physician is an employee of a non-custodian such as a private company the physician should consider whether he/she has custody or control of the personal health information. i.e. could the physician take the information to a newly established private practice.

If the physician is an employee of a custodian, the physician does not need to put in place a privacy program in accordance with PHIA. Instead they would need to participate in the privacy program of the custodian i.e. they still need to be aware of and meet the obligations contained within PHIA but under the procedures established by the custodian.

Does the physician have custody of personal health information? Custody refers to the responsibility for or care of the personal health information beyond the period of providing care. If the physician were to leave the current location of practice could he/she take the records or a copy of them to a new practice location? If a physician enters into an agreement with another custodian to leave the records at the original practice it does not minimize the responsibilities of the physician as a custodian while still practicing at that location.

- If the physician has custody or control of the personal health information then the physician is a custodian and must meet the requirements of PHIA.
- If the physician does not have custody or control of the personal health information then the responsibility to ensure the privacy and security of the personal health information belongs to the custodian with custody or control, such as a regional health authority. This does not negate however the physician's obligations under PHIA with respect to personal health information.

Does the physician have responsibility for, or control of, the personal health information that has been placed under the guardianship of someone who is not a custodian, such as a storage facility?

- If yes, then the physician is a custodian and must meet the requirements of PHIA.
- If the physician does not have control of the personal health information, or custody of it, then the physician is not a custodian. Such would be the case when a physician transfers records to

another custodian.

Determining Accountability in a Group Clinic

It is very common for a group of physicians to establish a group practice, whether it is a legal entity or a group of physicians in a shared space using some common services. In a group practice each physician is a custodian. In many of these practices all resources of the practice are shared, including employees and management of the EMR and, in some practices, the actual EMR records are shared.

Custodians must determine if they have sole custody or control of their patients' records or if this responsibility is shared with the other physician- custodians in the practice. Two questions to consider are:

1. Does each physician have his/her own EMR or a separate patient list within a common EMR?

2. Do employees, medical students and residents, work for just one physician or all physicians in the group practice?

If the answers to these questions are yes then each custodian is solely accountable for the personal health information under his/her custody or control and must meet his/her duties under PHIA.

Even with several custodians in one clinic, each physician has their own separate database within the EMR and accordingly, sole custody or control of their patient's personal health information. There is however, an expectation that they develop common approaches to protecting the personal health information, including a single policy manual for the entire practice.

Where several physicians in one clinic share a single, common database within the EMR, it is essential the physicians develop a common approach to protecting the personal health information and develop a single policy manual for the entire practice.

Responsibilities of Custodians

It is important to determine the custodian model at each clinic. The type of model will influence the privacy accountabilities for each custodian. The following describes the responsibilities of each model of custodian.

A sole practitioner

- A complete set of privacy policies
- No clinic exit agreement is required; however there should be a policy with procedures to follow when the physician ceases to practice at that location that is consistent with their legal responsibilities and the CPSNL Bylaws and guidelines.
- No information sharing agreement internal to the clinic is required.
- Education/training of employees, medical students and residents on the clinic policies and procedures, and their responsibilities.
- Oath or affirmation of confidentiality signed with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal

health information.

- Information Manager Agreements
    - eDOCSNL Participation Agreement
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service
- Agreements requiring a privacy clause or schedule
    - Landlord
    - Cleaners
    - Other third parties who may have access to personal health information

Physicians in a group practice

- Complete set of common privacy policies including a clinic-information sharing agreement or an understanding of how information is shared within the clinic and documented at the beginning of the clinic policy manual and signed by all custodians at the clinic.
- Clinic exit agreement signed by all physicians and any other health professional who has patient records at the clinic. If this is addressed in another practice agreement the physicians may have, the clinic exit agreement will not be necessary.
- Education of employees, medical students and residents on the clinic policies and procedures, and their responsibilities.
- Oath or affirmation of confidentiality with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.
- Information Manager Agreements required with
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering services
- Agreements requiring a privacy clause or schedule
    - Landlord
    - Cleaners
    - Other third parties who may have access to personal health information

A physician in a group medical corporation, partnership or other legally recognized entity

If the medical corporation is a sole practitioner he/she should implement the responsibilities of the sole practitioner.

If the medical corporation is a group practice or a group of physicians who are each incorporated they should implement:

- A complete set of common privacy policies including a clinic-information sharing agreement or statement of how information is shared within the clinic and included at the beginning of the clinic policy manual and signed by all custodians at the clinic.
- Clinic exit agreement signed by all physicians and any other health professional who has

patient records at the clinic. If this is addressed in another practice agreement the physicians may have the clinic exit agreement will not be necessary.

- Education of employees, medical students and residents on the clinic policies and procedures, and their responsibilities.
- Oath or affirmation of confidentiality with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.
- Information Manager Agreements required with
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service
- Agreements requiring privacy clause or schedule
    - Landlord
    - Cleaners
    - Other third parties who may have access to personal health information

A contract physician

A physician who is on contract with another custodian, such as a regional health authority, may or may not be a custodian depending on the custody or control of the information. A physician, whose contract gives him/her responsibilities for the personal health information, including responsibilities when the physician ceases to practice on contract should be considered a custodian. He/she should have in place:

- Complete set of privacy policies with consideration of the policies and procedures of the custodian that holds the contract.
- Clinic exit agreement with the other custodian.
- Information sharing agreement with the custodian that holds the contract (e.g. Regional health authority).
- Clarity on who is responsible for the education/training of employees, medical students and residents on the clinic policies and procedures, and their responsibilities.
- Clarity on whose oath or affirmation of confidentiality employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information sign.
- Information Manager Agreements required with
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service
- Agreements requiring privacy clause or schedule
    - Landlord
    - Cleaners
    - Other third parties who may have access to personal health information

A physician who does not have custody or control of the personal health information he/she

collects, uses or discloses is not considered a custodian but is required by CPSNL Bylaw 6 to make themselves familiar with the information regarding compliance with PHIA available at the Provincial Government website including the

- PHIA Risk Management Tool Kit
- PHIA Policy Development Manual

A physician whose office is located on the premises of another custodian, such as a regional health authority, and from whom the physician avails many benefits such as Information Management services and provision of hardware:

- Complete set of privacy policies with consideration of the policies and procedures of the custodian that is the landlord.
- Information sharing agreement with the custodian who is the custodian-landlord.
- Education of employees, medical students and residents on the clinic policies and procedures and their responsibilities.
- Oath or affirmation of confidentiality with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.
- Information Manager Agreements required if not covered by the custodian-landlord
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service
- Agreements requiring privacy clause or schedule
    - Landlord
    - Cleaners
    - Other third parties who may have access to personal health information may have access to personal health information

A physician who practices at more than one location, sometimes as a custodian and other times on contract or as a primary care physician

A physician can be a custodian at one location and a non-custodian at another location. At the locations where the physician is not a custodian he/she is responsible for reading, being familiar with, and complying with the policies and procedures of the custodian at that location.

Note: What follows is best practice and recommended.

The physician, if not deemed as a custodian, should work to ensure best practices are implemented. If they are the custodian however, they would have responsibilities to ensure these recommended practices are implemented.

- A complete set of privacy policies must be in place. If the non-custodian has policies and procedures for the clinic the physician should approve them or make the necessary amendments to be in compliance with CPSNL Bylaw 6 and best practices.
- Clinic exit agreement signed with the non-custodian owner.
- Information sharing agreement with the non-custodian detailing the responsibilities of both parties.

- Physician has an obligation to ensure the non-custodian educates employees, medical students and residents, on the policies and procedures and their responsibilities.
- Physician has an obligation to ensure the non-custodian has signed an oath or affirmation of confidentiality with employees, medical students and residents, other health professionals working in the clinic, and third parties.
- Physician should strongly encourage the non-custodian to have:
  1) Information Management Agreements with:
     - IT support company
     - Storage company
     - Shredding company
     - Transcriptionist
     - Telephone answering service
  2) Agreements requiring a privacy clause or schedule
     - Landlord
     - Cleaners
     - Other third parties who may have access to personal health information

A physician working with a physician employed by another custodian, such as an RHA

The physician should enter into an agreement with the other custodian to clarify or establish who the custodian of the records is at the beginning of the relationship.

- If the physician is the custodian, he/she should develop a complete set of privacy policies with consideration of the policies and procedures of the other custodian.
- Clinic exit agreement signed by all physicians and any other health professional who have patient records at the clinic.
- Information sharing agreement with the custodian (ex: regional health authority) should state:
  - Who is responsible for the education of employees, medical students and residents, on policies and procedures and their responsibilities.
  - Who is responsible for ensuring an oath or affirmation of confidentiality is signed by the employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.
- Information Manager Agreements required with
  - IT support company
  - Storage company
  - Shredding company
  - Transcriptionist
  - Telephone answering service
- Agreements requiring a privacy clause or schedule if not covered by the other custodian
  - Landlord
  - Cleaners
  - Other third parties who may have access to personal health information

Other Custodians

During the time a custodian has custody or control of personal health information he/she may collect personal health information from or disclose personal health information to other people or organizations. It is important to know if the other person or organization is a custodian under PHIA, as the responsibilities differ. There is more information about non-custodians in the guidelines for collection and disclosure.

The following are key custodians under PHIA when they have custody or control of personal health information. See section 4 of PHIA for a full list.

- a department or branch of the Government of Newfoundland and Labrador when engaged in a function related to the delivery or administration of health care in the province;
- a health care professional, when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;
- the Centre for Health Information;
- regional health authorities;
- the Provincial Public Health Laboratory; or
- a person who operates:
    - a health care facility,
    - a licensed pharmacy as defined in the Pharmacy Act, 2012,
    - an ambulance service, or
    - a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider.

Custodian of the Electronic Health Record

As the Electronic Health Record (EHR) becomes fully operational in Newfoundland and Labrador and permits a seamless flow of personal health information from the EHR to the EMR, physicians should understand the custodian model for the EHR.

The Centre for Health Information is the custodian responsible for establishing the EHR however, other custodians maintain custodianship for the source data including:

- Medication Inf20ormation contained within the drug information repository (Pharmacy Network) – individual pharmacies
- Laboratory results – Regional health authorities
- Client demographics – Regional health authorities, pharmacies, etc.
- MCP data – Department of Health and Community Services

Custody or Control

Under PHIA, a "custodian" means a person described in Section 4(1) who has **custody or control** of personal health information as a result of or in connection with the performance of the person's powers or duties or the work described.

Indirectly Collected Personal Health Information

In general, having custody or control of personal health information does not apply only to personal health information the custodian collected from the patient but also to personal health information that has de facto become part of the physician's information holdings.

When a custodian receives reports, test results and other personal health information about a patient from another physician, custodian, or person, that information is considered part of the patient's record. The custodian is considered to be in custody or control of this indirectly collected personal health information and is responsible for the protection of this information, just as if it had been collected directly from the patient.

Personal Health Information in the Control of the Custodians

Control refers to having the power or authority to manage, restrict, regulate or administer the collection, use or disclosure of the record.

When a custodian contracts with another organization to process, store, or destroy patient information the custodian remains responsible for the privacy of that information.

Further, if the physician has asked a non-custodian to manage personal health information, it does not alleviate the physician from the responsibility of ensuring that the third party non-custodian continues to protect the personal health information.

When personal health information is disclosed by the custodian to another custodian for the purpose of providing health care or another disclosure authorized by PHIA, the custodian receiving the personal health information will become responsible for the protection of the information once it is within its custody or control.

Application of PHIA

(PHIA s. 5)

PHIA gives a clear de16
finition of what is and what is not personal health information. PHIA applies to all personal health information whether recorded or communicated orally, as defined in the act. For a definition of personal health information see glossary.

PHIA does not apply to the following information

- to a record related to the Child, Youth and Family Services Act or the Adoption Act, 2013 notwithstanding that the information would otherwise be considered to be personal health information or the person would otherwise be considered to be a custodian within the meaning of PHIA;
- A record in a court file or a record of a judge of the Trial Division, Court of Appeal or Provincial Court;
- A note, communication or draft decision of a person acting in a judicial or quasi-judicial capacity;
- A constituency record of a member of the House of Assembly.
- Personal health information collected before April 1, 2011 is not subject to the consent and use provisions of the Act.

Other Relevant Legislation

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is the federal legislation that applies to the collection, use and disclosure of personal information and personal health information by organizations that are involved in a "commercial activity". Independent medical clinics are considered a commercial activity however, custodians in Newfoundland and Labrador are governed by PHIA which has been deemed substantially similar to PIPEDA.

Newfoundland and Labrador Legislation

There are several other Acts that impact the collection, use and disclosure of Personal Health Information:

Centre for Health Information Act, 2008
Medical Care Insurance Act, 1999
Health Research Ethics Authority Act, 2006
Mental Health Care and Treatment Act, 2006
Pharmacy Act, 2012
Advanced Health Care Directives Act, 1995
Neglected Adults Welfare Act, 2011
Access to Information and Protection of Privacy Act, 2015

Personal health information obtained for the purposes of the following Acts are not subject to PHIA:

- *Child, Youth and Family Services Act, 2010*
- *the Adoption Act, 2013*

If a custodian collects, uses or discloses personal health information in accordance with any of these Acts, consideration should be given to including appropriate procedures in the clinic's policies and procedures.

Contact Person
(PHIAs. 18)

A custodian *may designate a contact person to perform the functions below***.** If a contact person has not been designated, the custodian *shall be considered to be the contact person***.** A privacy officer is more consistently the term used to describe a contact person.

There are several factors to consider when designating a privacy officer at a clinic:

- It is recommended that the privacy officer be a physician.
- Physicians in a group practice can select one of the custodians to act as the privacy officer for all of them.
    - The appointed person should be, or become, knowledgeable on PHIA and privacy best practices.
- If one physician is appointed as the privacy officer in a group practice, this does not negate the other custodians in the practice from their legal obligations under PHIA.
- If one physician is appointed privacy officer, all physicians are expected to agree to the policies and procedures of the clinic and be aware of how to comply with the procedures.
- A custodian can appoint a non-physician to assist in the privacy activities of the practice. This person is normally the senior office administrator.
- Large clinics may appoint the senior administrative person to be the privacy officer because of the large number of administrative functions undertaken by this individual. The custodians in the practice will still have legal obligations under PHIA and be responsible for decisions with respect to the personal health information they have custody and control of.

Responsibilities
A contact person shall:

- *Facilitate the custodian's compliance with PHIA and the regulations*
- *Ensure that employees, contractors, agents and volunteers of the custodian and those health care professionals who have the right to treat persons at a health care facility operated by a custodian are informed of their duties under PHIA and the regulations*
- *Respond to inquiries from the public in respect of the custodian's information policies and procedures*
- *Respond to requests by an individual for access to or correction of personal health information about the individual that is in the custody or under the control of the custodian*

Obligations of Employees, Agents, Contractors, and Volunteers

(PHIA s. 14)

This guideline applies to health professionals, employees, students, residents, and others who collect, use, and disclose personal health information on behalf of a custodian. **Custodians are required to ensure these individuals comply with PHIA and the clinic's policies and procedures.**

Physicians can meet this responsibility by

- Developing a policy and procedures manual (policy manual);
- Ensuring all employees are educated to increase their understanding of PHIA and the policies and procedures;
- Ensuring employees who handle personal health information are trained on the specific procedures that apply to their work;
- Ensuring all employees have signed an oath or affirmation.

Obligations of Health Professionals, Employees, Medical Students and Residents

Health professionals, employees, medical students and residents are responsible for

- Reading the policy manual and asking for clarifications on procedures they do not understand;
- Participating in all privacy and security education and training as requested by the custodian;
- Ensuring the protection and security of personal health information they collect, use, and disclose.

Health professionals, employees, medical students and residents who do not comply with this policy can be subject to employment discipline, contractual remedies or professional discipline.

Oath or Affirmation of Confidentiality

A custodian shall ensure that its employees, agents, contractors, and volunteers take an oath or affirmation of confidentiality.

The oath should be signed at regular intervals and as a condition of employment for all new employees, and engagement of health professionals, medical students and residents. The Newfoundland and Labrador Information and Privacy Commissioner recommends that oaths be revisited and amended as necessary when employees change roles[4].

[4] PH-2013-001, http://www.oipc.nl.ca/pdfs/ReportPH-2013-001.pdf

Privacy and Security Awareness, Education, and Training

(PHIA s. 16)

An important part of a privacy and security program is ensuring custodians, health professionals, employees, medical students and residents know the policies and procedures and understand their obligation to follow them. Knowledgeable custodians, health professionals, employees, medical students and residents are better at:

- Managing personal health information consistently and in compliance with PHIA;
- Responding positively and in an effective manner when patients make requests for access, correction or masking of personal health information;
- Avoiding and identifying privacy and security breaches.

Awareness Activities

- Making available high-level information about the legal requirement to protect personal health information and about the clinic's policies and procedures.
- Ongoing awareness activities contribute to a culture of privacy at the practice.
  Examples of awareness activities include:
    - Posting a news article about a privacy breach on a employees bulletin board;
    - Distributing buttons to employees that say, "We respect your privacy".

Employee, Health Professional, and Medical Students and Residents' Education Activities

- Providing education sessions about how they should protect personal health information.
- Responding to questions about how they should follow the procedures.
- Continuing education as new procedures are developed or existing ones revised.
- Providing information at employee meetings or at specially designated workshops.
- Inviting guest speakers to employee meetings, such as a privacy officer from a hospital, long-term care facility, or another clinic with which personal health information is regularly shared.

Employee training

Some policies and procedures require more detailed instruction, such as new procedures for faxing. Training on specific activities should be conducted for those who need to know it for their job or as support for the person doing the work.

Specific training should be given on the following:

- Faxing, emailing, and scanning
- Managing consent directives
- Managing patient requests for access to, or correction of, their personal health information
- Responding to breaches of personal health information
- Storing and destroying records
- Acceptable uses of technology.

New Employees, Health Professionals, Medical Students and Residents

All new employees should receive privacy and security orientation before being given a username and password for the EMR.

The new employee should be given the clinic's privacy and security policy manual to read prior to the start date or during the first few days of employment.

The orientation, which should be offered by the privacy officer or medical office administrator, will then involve reviewing and clarifying the policy manual and providing training on the procedures specific to the new employee's responsibilities.

New health professionals, employees, medical students and residents should receive privacy and security orientation.

Accuracy and Integrity of Personal Health Information

(PHIA s. 16 CPSNL Bylaw 6)

Before using or disclosing personal health information, Custodians have a responsibility to their patients to **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.**

A custodian must also **clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, completeness or up-to-date character of the information.**

A medical practitioner must ensure that there is recorded and retained an individual record for each patient which includes:

- The full name, address, date of birth and gender of the patient;
- The patient's Medicare health number, if he or she has one;
- The name and contact information of the patient's legal representative(s) or substitute decision maker(s), if applicable;
- In a consultant report, the name and address of the patient's primary care physician and of any health care professional who referred the patient;
- The date of each professional encounter of the medical practitioner with the patient, including each occasion on which the patient is seen or spoken to by telephone by the medical practitioner; and
- A contemporaneous record of the assessment and disposition of the patient by the medical practitioner for each visit

Additional steps physicians can take to improve the accuracy of the information they collect include:

- Be written in clear language with only common abbreviations used,
- Document current information on the care and condition of the patient as soon as possible, ideally at the time of the appointment or later the same day,
- Record the date, time, and the name of the author,
- Make additions and corrections in a manner that allows the original information to still be read,
- Ensuring scanned documents and photocopies are complete and readable,
- Train employees on how to keep accurate records.

Physicians are also responsible for the integrity of their patients' records, where integrity is the assurance that personal health information has not been modified, or in some other way interfered with such that the physician or patient does not consider the information reliable. The preservation of the records' content is maintained throughout storage, use, transfer and retrieval so that there is confidence that the information has not been tampered with or modified other than as authorized.

Steps physicians can take to protect the integrity of the personal health information include:

- Accurate recording of the personal health information,
- Accurate scanning and photocopying of personal health information,
- Perform daily backups and periodically confirm the reliability of the backups,
- Secure and environmentally safe storage,

- Auditing of accesses to personal health information,
- Use of up-to-date security software.

Identifying Purposes and Openness

Custodians have significant responsibility to be transparent on how they manage their patients' personal health information.

PHIA gives patients the right to be made aware of the purposes for which their personal health information may be used and disclosed at the time the information is collected. PHIA also requires that patients be informed of their right of access to their personal health information, to request a correction where the information is inaccurate or incomplete, and the right to consent to the collection, use, and disclosure of their personal health information, subject to some exceptions.

The general principle of openness is that it will be easy for patients to be aware of the privacy practices of any custodian collecting, using, and disclosing their personal health information and their rights under PHIA. This information will help patients achieve a greater degree of comfort that their privacy will be protected.

There are several ways a custodian can meet the expectations of openness:

- Discussing the purpose for collecting information with patients
- Discussing the clinic's privacy practices,
- Displaying a poster in a spot that is easily seen by patients before or when their personal health information is being collected,
- Making a pamphlet available where personal health information is collected,
- Posting the information on the clinic's website.

The information that should be made available includes:

- Contact information for the privacy officer,
- A description of the custodian's information practices, including the purposes for collection,
- A description of the anticipated uses and disclosures of the information,
- Contact information for the Office of the Information and Privacy Commissioner of Newfoundland and Labrador,
- An explanation of the patient's right to access and request correction of their own personal health information.
- The patient's right to manage consent through masking or alternative methods to restrict access, agreed to by the patient and the physician.

To meet these requirements physicians can display the posters available from the eDOCSNL. This should be supplemented by making available to patients the Department of Health and Community Services' PHIA pamphlet.

Challenging Compliance/Patient Complaint Process

PHIAs. 19;

It is important that physicians' accountability to their patients extends to how they manage complaints from patients and challenges to how the clinic adheres to its written policies. This is a **mandatory** activity **under PHIA and the *Personal Information Protection and Electronic Documents Act.***

- A clinic's complaints process will work best if it is known to all physicians, health professionals, employees, medical students and residents. This means a complaint can be received by anyone at the clinic. The person contacted by the patient about the issue should document and date the complaint.
- One person in the clinic should be assigned the responsibility for receiving and investigating complaints. This will probably be the privacy officer or the medical office administrator.
- The clinic policy should state that all complaints will be investigated.
- A patient should be informed at the time of the complaint that he or she can contact the Office of the Information and Privacy Commissioner of Newfoundland and Labrador and/or the professional regulatory body if the complaint is about a regulated health professional.
- A complaint investigation process should also include recommendations for how to avoid a similar type incident.
- Types of complaints include:
    - Reporting of an actual, suspected or potential breach,
    - Failing to comply with the clinic's policies and procedures.

Ceasing to Practice, Permanently or for a Period of Time, or Leaving a Clinic

(PHIA s. 39, CPSNL Policies)

Personal health information must continue to be protected after a custodian ceases to practice or leaves a practice.

CPSNL requires physicians to notify patients when ceasing to practice, or moving the location of their practice, by placing a notice within the clinic and *by publication of notice in the daily newspaper of widest circulation in the area of the medical practice. Publication should be made in three separate editions of the newspaper, one of which being a weekend edition if one is published, over a period of 2 weeks. The notice should include the following:*

a. *the name of the physician closing his or her practice, and the location of the practice which is closing;*
b. *the effective date on which the practice will be closing;*
c. *the identity and contact information of the physician who will assume responsibility for the medical practice, or if no physician will be assuming responsibility for the medical practice, then notice of that fact; and*
d. *the means by which a patient may access his or her medical record.*

Ceasing to Practice as a Custodian

A physician may permanently close his/her medical practice for a number of reasons including retirement, illness, or relocation.
When permanently closing a medical practice, a physician should consider:
• arrangements for the continuing medical care of patients in his/her medical practice; and
• patient access to their medical records.

When a Custodian Dies

Where a custodian dies, *the duties and powers of a custodian under PHIA shall be performed by a personal representative of the deceased until custody and control of the record of personal health information passes to another person who is legally authorized to hold the record.*

Failure to Transfer Records to another Custodian

Where a custodian fails to carry out his or her duties, the minister may appoint a person to act in place of the custodian until custody and control of the record fully passes to another person and may recover the costs and expenses of, and incidental to, the appointment, from the custodian.

When a Custodian Leaves a Practice

If a custodian leaves a clinic to join another practice, proper notice should be given to the other physicians in the practice and a notice to patients should be posted in the clinic. The physicians should agree on how the exiting physician's patient records will be transferred to the other clinic. These details should be included in documentation that all physicians in the clinic agree to. It could be in

the partners' agreement or a Clinic Exit Agreement.

The purpose of the agreement is to have a transition plan in place when a physician leaves a practice. The transition plan should include:

- Giving 30 or more days' notice,
- Managing the costs associated with the implementation and operation of the EMR,
- Managing the records in the EMR and any paper records associated with the leaving physician, specifically:
    - Retaining EMR records in a shared database at the originating clinic and the leaving physician can take a copy at a fair cost agreed to by all the physicians in the transition plan,
    - Transferring EMR records in a database only used by the leaving physician to the leaving physician, with cost assigned to the leaving physician,
    - Cooperating with the leaving physician and the EMR vendor to facilitate a smooth transfer,
    - Complying with any technical, security or other protocols in the clinic's policy manual,
    - Encouraging the EMR vendor to release the leaving physician from any contracts entered into between the clinic and the EMR vendor.
    - Physicians should not take records outside Canada.

Patient Rights

Patient Access to Their Own Information

(PHIA ss. 15, 52, 53, 55, 66; CPSNL Guideline - Patient Access to Office Medical Records and the Personal Health Information Act, CMA Code)

An individual has a right of access to a record containing his or her personal health information that is in the custody or under the control of a custodian. An individual may exercise a right of access to a record of his or her personal health information by making a request for access to the custodian that the individual believes has custody or control of the information.

Review of Current Practices

Custodians who currently have established procedures for providing patients access to, and copies of, their medical record, will probably be able to follow the same procedures.

Privacy officers should incorporate into the clinic's procedures the legislated timelines within which patients must receive access to, or a copy of, their own information.

Access Request Form

Physician can still provide patients with copies of reports without following the formal process set out in PHIA if the information requested is provided at the time of the request. However, *a custodian may require a request to be in writing unless the individual making the request:*

(a) has limited ability to read or write English; or

(b) has a disability or a condition that impairs his or her ability to make a request in writing.

Custodians should have a standard application form for patients to use to request access to their own information. The form should include all information the physician needs to find the correct information and a place to record that proper identification of the patient has taken place.

All written requests should be dated clearly with the date the request is received and if the request form is incomplete the date it is completed.

Copies of information given to patients should be clearly marked "patient copy".

Requirements under PHIA

A custodian shall not make a record of personal health information, or part of it, available to an individual without first taking reasonable steps to be satisfied as to the individual's identity.

A custodian may charge a reasonable fee for providing a copy of a record in response to a request for access and the fee shall not exceed the maximum fee set by the minister.

Fees

The CMA[5], NLMA[6], OIPC[7], and the Department of Health and Community Services[8] all provide advice and guidance relating to the fees charged for access to a patient record.

It is important to determine fees in-line with the CMA Code. The CMA code states an ethical physician:

- "Will practice in a fashion that is above reproach and will take neither physical, emotional, nor financial advantage of the patient."
- "When acting on behalf of a third party, will ensure that the patient understands the physician's legal responsibility to the third party before proceeding with the examination."
- "Will, upon a patient's request, supply the information that is required to enable the patient to receive any benefits to which the patient may be entitled."
- "Will consider, in determining professional fees, both the nature of the service provided and the ability of the patient to pay, and will be prepared to discuss the fee with the patient."

The fees listed by the NLMA are suggested minimum fees and may be adjusted accordingly. Your fees should appropriately reflect:

- the service provided
- your time
- your expertise
- your practice needs
- the patient's ability to pay

As an example, OIPC outlines a maximum, standard total fee of $25.00 for all of the following tasks:

1. Receipt and clarification, if necessary, of a request for a record.
2. Locating and retrieving the record.
3. Review of the contents of the record for not more than 15 minutes by the health information custodian or an agent of the custodian to determine if the record contains personal health information to which access may be refused.
4. Preparation of a response letter to the individual.
5. Preparation of the record for photocopying, printing or electronic transmission.
6. Photocopying the record to a maximum of the first 50 pages or printing the record, if it is stored in electronic form, to a maximum of the first 50 pages, excluding the printing of photographs from photographs stored in electronic form.
7. Packaging of the photocopied or printed copy of the record for shipping or faxing.
8. If the record is stored in electronic form, electronically transmitting a copy of the electronic record instead of printing a copy of the record and shipping or faxing the printed copy.
9. The cost of faxing a copy of the record to a fax number within the province or mailing a copy of the record by ordinary mail to an address in Canada.

Photocopying charges apply for files in excess of 50 pages at 25¢/page. This fee does not cover summary

[5] https://www.cma.ca/Assets/assets-library/document/en/advocacy/CMA_records_confidential_PD00-06-e.pdf#search=patient%20fees
[6] http://www.nlma.nl.ca/documents/guides/guide_2.pdf
[7] http://www.oipc.nl.ca/pdfs/ReportAH-2012-001.pdf
[8] Fee Schedule for Disclosure of Personal Health Information

of the patient's chart that can be billed using the hourly rate.

Consider the patient's ability to pay when establishing the fee to be charged, including the **custodian's ability to waive any fees**. The patient may also ask for a fee waiver.

Processing a Request

A written request shall contain sufficient detail to permit the custodian to identify and locate the record with reasonable efforts. If a request does not contain sufficient detail to permit the custodian to identify and locate the record with reasonable efforts, the custodian shall offer assistance to the person requesting access to reformulate the request.

A patient is not required to explain why the request is being made but the applicant may include this information as it will help in preparing the information for the patient.

In response to a request, a custodian shall:

- *where the custodian decides to grant access, make the record available to the individual for examination and, upon request of the individual, provide a copy of the record to the individual and an explanation, where necessary, of any information contained in the record*
- *give a notice in writing to the individual stating that, after reasonable efforts, the custodian has concluded that the record does not exist or cannot be found; or*
- *where the custodian is entitled to refuse the request, in whole or in part, give a notice in writing to the individual making the request stating that access to the record in whole or part is refused, together with reasons for the refusal, and that the individual may appeal the refusal to the Trial Division*

If Another Custodian has Custody or Control of the Information

A physician does not have custody or control of the personal health information requested by a patient, but is aware that it is in the custody or control of another custodian:

- *May transfer the written request for access to the other custodian.*
- *Must notify the patient of the transfer as soon as reasonably possible.*
- *The custodian to whom the written request for access was transferred must respond within 30 calendar days after the date of transfer of the request.*

Refusing Access

A custodian shall refuse to permit an individual to examine or receive a copy of a record of his or her personal health information where

- *another Act, an Act of Canada or a court order prohibits disclosure to the individual of the record or the information contained in the record in the circumstances;*
- *granting access would reveal personal health information about an individual who has not consented to disclosure; or*
- *the information was created or compiled for the purpose of*

- *a committee referred to in subsection 8.1(2) of the Evidence Act ,*
- *review by a standards or quality assurance committee established to study or evaluate health care practice, or*
- *a body with statutory responsibility for the discipline of health care professionals or for the quality or standards of professional services provided by health care professionals.*

A custodian may refuse to permit an individual to examine or receive a copy of a record of his or her personal health information where

- *the record or the information in the record is subject to a legal privilege that restricts disclosure of the record or the information;*
- *the information in the record was collected or created primarily in anticipation of, or for use in, a proceeding and the proceeding, together with all appeals or processes resulting from it, has not been concluded;*
- *the following conditions are met:*
  - *the information was collected or created in the course of an inspection, investigation or similar procedure authorized by law or undertaken for the purpose of the detection, monitoring or prevention of the receipt of a service or benefit under an Act or program operated by the minister, or a payment for that service or benefit, and*
  - *the inspection, investigation or similar procedure, together with all proceedings, appeals or processes resulting from it, have not been concluded; or*
- *granting access could reasonably be expected to*
  - *result in a risk of serious harm to the mental or physical health or safety of the individual who is the subject of the information or another individual,*
  - *lead to the identification of a person who was required by law to provide information in the record to the custodian, or*
  - *lead to the identification of a person who provided information in the record to the custodian in confidence under circumstances in which confidentiality was reasonably expected.*

A custodian may also refuse to grant a request for access to a record of personal health information where the custodian believes on reasonable grounds that the request for access to the record is

- *frivolous or vexatious;*
- *made in bad faith; or*
- *for information already provided to the individual.*

Timeline for Responding to an Access Request

A custodian shall respond to a request for personal health information, without delay and in any event not more than 60 days after receiving the request. A custodian may extend the time limit set out in PHIA for an additional 30 days where:

- *meeting the time limit would unreasonably interfere with the operations of the custodian; or*
- *the information consists of numerous records or locating the information that is the subject of the request cannot be completed within the time limit.*

A custodian that extends the time limit shall:

- *give the individual making the request written notice of the extension, together with reasons for the extension; and*
- *grant or refuse the individual's request as soon as possible and in any event not later than the expiration of the time limit as extended.*

Where a custodian fails to respond to a request for access within the time limit, he or she shall be considered to have refused the request for access.

It is recommended that the physician include information on how to contact the Office of the Information and Privacy Commissioner in the written response to the patient.

Patient May Appeal to the Information and Privacy Commissioner

Where a custodian has refused the request of an individual for access or correction the affected individual may file a complaint with the commissioner. Such a complaint shall be in writing and shall be filed with the commissioner within 60 days from the date

- *that the individual receives notice of the custodian's refusal*
- *that the custodian is considered to have refused the request*

A custodian that has custody or control of personal health information that is the subject of a request for access or for correction shall retain the information for as long as necessary to allow the individual to exhaust any recourse under PHIA that he or she may have with respect to the request.

Requests for Correction

(PHIA s. 60, 61, 62, 63)

Requests from Patients

Where a custodian has granted an individual access to a record of his or her personal health information and the individual believes that the record is inaccurate or incomplete, he or she may request, either orally or in writing that the custodian correct the information.

Responding to a Request for Amendment

A custodian shall respond to a request for correction without delay and in any event not more than 30 days after receiving the request. A custodian may extend the time limit set out for an additional 30 days, in accordance with PHIA.

The custodian

- *shall grant the request for correction where the individual making the request*
    - *demonstrates to the satisfaction of the custodian that the record is incomplete or inaccurate for the purposes for which the custodian uses the information, and*
    - *gives the custodian the information necessary to enable the custodian to correct the record; or*
- *may refuse the request for correction where*
    - *the record was not originally created by the custodian and the custodian does not have sufficient knowledge, expertise and authority to correct the record,*
    - *the information which is the subject of the request consists of a professional opinion or observation that a custodian has made in good faith about the individual, or*
    - *the custodian believes on reasonable grounds that the request is frivolous, vexatious or made in bad faith.*

Where a custodian fails to respond to a request for correction within the time period he or she shall be considered to have refused the request for correction.

Where a custodian grants a request for a correction, he or she shall

- *make the requested correction*
    - *by recording the correct information in the record and*
        - *striking out the incorrect information in a manner that does not obliterate the record, or*
        - *where it is not possible to strike out the incorrect information, by labelling the information as incorrect, severing the incorrect information from the record, storing the incorrect information separately from the record, and maintaining a link in the record that enables a person to trace the incorrect information, or*
    - *where it is not possible to record the correct information in the record, by ensuring that there is a practical system in place to inform a person accessing the record that the information in the record is incorrect and to direct the person to the correct information;*
- *provide written notice to the individual making the request for correction of an action taken under; and*
- *provide written notice of the requested correction, to the extent reasonably possible, to a person to whom the custodian has disclosed the information within the 12 month period immediately*

preceding the request for correction unless the custodian reasonably believes that the correction will not have an impact on the ongoing provision of health care or other benefits to the individual or where the individual requesting the correction has advised that notice is not necessary.

Where a custodian refuses to grant a request for correction, he or she shall

- *annotate the personal health information with the correction that was requested and not made and, where practicable, notify a person to whom the information was disclosed within the 12 month period immediately preceding the request for correction of the notation unless the custodian reasonably expects that the notation will not have an impact on the ongoing provision of health care or other benefits to the individual or the individual requesting the correction has advised that notice is not necessary; and*
- *provide the individual requesting the correction with a written notice setting out the correction that the custodian has refused to make, the refusal together with reasons for the refusal, and the right of the individual to appeal the refusal to the Trial Division or request a review of the refusal by the commissioner.*

Representatives

(PHIA s. 7)

Representatives

There are situations where a patient may have another person represent or make decisions on his or her behalf for care and treatment. PHIA provides the authority for a representative to make the same decisions for the patient regarding personal health information.

A right or power of an individual may be exercised

- *by a person with written authorization from the individual to act on the individual's behalf;*
- *where the individual lacks the competency to exercise the right or power or is unable to communicate,*
- *by 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;*
- *where the individual is deceased, by the individual's personal representative or, where there is no personal representative, by the deceased's 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 ;*
- *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*
- *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 PHIA.*

Decisions by, or on behalf of, a Minor

The age of majority in Newfoundland and Labrador is 19. Individuals under 19 years of age are said to minors.

A parent or guardian of a minor may execute the right or power of the 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.

For further direction related to this topic, see CPSNL **Guideline - Consent to Medical Treatment of Minors.**

Consent, Collection, Use, and Disclosure

Collection of Personal Health Information

(PHIA s 29, 30, 31, 32)

A custodian shall 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 PHIA.*

A custodian shall not collect more personal health information than is reasonably necessary to meet the purpose of the collection.

Types of Information Collected

- Identification and contact information, including
    - Name
    - Date of birth
    - Address
    - Phone/fax/email
    - Emergency contact information
    - Record of patient appointment times
- Billing information including
    - Provincial health insurance plan number
    - Private medical insurance details
- Health information including
    - Medical history
    - Presenting symptoms
    - Physical examination findings
    - Relevant medical history of family members
    - Test requisitions and results
    - Reports from specialists or other health providers
    - Diagnosis and treatment notes (including prescriptions)
    - Allergies
    - Information to be provided to third parties at the patient's request (Workplace NL, reports for legal proceedings, insurance claims)

Type of Collection

Physicians should only collect personal health information that is reasonably necessary for the purpose for which it is being collected.

Physicians must collect the personal health information directly from the patient, except where:

- *The patient consents to the collection by a different method*
- *It is not reasonably possible to collect the information directly from the patient*
- *A representative has been identified*
- *the information is reasonably necessary for providing health care to the individual and it is not reasonably possible to collect it directly from the individual*
- *the custodian collects the information from a person who is not a custodian for the purpose of carrying out a research project that has been approved by the research ethics board or a research ethics body*

- *the Collection is required by an act other than PHIA*
- *the information is to be collected for the purpose of assembling a family or genetic history where the information collected will be used in the context of providing a health service to the individual*
- *determining an individual's eligibility for a program or service*
- *the custodian collects information for the purpose of analysis or compiling statistical information respecting the management, evaluation or monitoring of the allocation of resources to, or planning for all or part of, the health care system, including the delivery of services, and the person from whom the information is collected has in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information.*

A custodian shall not collect personal health information if other information will serve the purpose of the collection. Therefore, physicians should only collect information they need to provide health care to the individual.

When a physician collects personal health information from another custodian and the information becomes part of the patient's record, this information is now considered to be in the custody or control of the collecting physician. The physician collecting the personal health information is accountable for the information in the patient's record.

Use of Personal Health Information

(PHIA ss. 2, 33)

A use of personal health information occurs when a physician, or other health professional, employees, or medical students or residents use the information for a purpose within the clinic. *Use means to handle or deal with the information or to apply the information for a purpose and includes reproducing the information, but does not include disclosing the information.*

- *A custodian shall not use personal health information about an individual unless it has the individual's consent and the use is necessary for a lawful purpose; or the use is permitted or required by PHIA.*
- *A custodian shall not use personal health information if other information will serve the purpose of the use.*
- *The use of personal health information shall be limited to the minimum amount of information necessary to achieve the purpose for which it is used.*
- *A custodian shall limit the use of personal health information in its custody or under its control to those of its employees and agents who need to know the information to carry out the purpose for which the information was collected or a purpose authorized under PHIA.*
- *Physicians should only use the minimal amount of personal health information that is necessary for the purpose for which it is collected.*
- *A physician must, whenever practicable, use de-identified health information if it will serve the purpose.*

Permitted Uses

A custodian may use personal health information in its custody or under its control for the following purposes:

- *for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose;*
- *for planning or delivering health care programs or services provided or funded by the custodian, in whole or in part, allocating resources to those programs or services, evaluating or monitoring those programs or services or preventing fraud or an unauthorized receipt of services or benefits related to those programs or services;*
- *for the purpose of risk management or error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of related programs or services of the custodian;*
- *for the purpose of 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 purpose of a proceeding or contemplated proceeding in which the custodian is or is expected to be a party or witness and where 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 an approved research project in accordance with PHIA;*
- *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;*
- *By a health authority, or a board, council, committee, commission, corporation, or agency established thereunder, a department of Executive Council, the Minister of Health, or the Centre for Health Information for the following functions within the geographic area in which the custodian has jurisdiction:*
    - *planning and resource allocation,*
    - *health system management,*
    - *public health surveillance, and*
    - *health policy development;*
- *another use to which the individual who is the subject of the personal health information consents; and*
- *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.*

Secondary Uses

Secondary uses as defined within the glossary, is permitted in certain instances. A decision to use or disclose personal health information for a purpose other than that for which it was originally collected should be thoroughly reviewed to ensure it aligns with what is permitted under PHIA. All secondary uses of personal health information should be documented and either outlined in a clinic's policies and procedures or through a standardized approval process.

Patient consent is required for some secondary uses of personal health information and therefore, custodians should review the consent section of this manual.

Where possible, personal health information should be made non-identifying in order to minimize the risk to the patient. *A custodian may strip, encode or otherwise transform personal health information to create non-identifying health information*. It is important to note however, that the extent to which personal health information is stripped, encoded or transformed varies and should not be done without consultation or guidance.

Furthermore, as it relates to employee's, personal health information does not include identifying information contained in a record that is in the custody or under the control of a custodian where the identifying information contained in the record relates primarily to an employee or agent of the custodian. Therefore, information obtained from employees at a clinic for the purposes of their employment must not be used in the course of their care.

Disclosure of Personal Health Information

(PHIA ss. 36, 37, 38, 39, 40, 41, 42, 43, 4, 45, 46, 47, 48, 49, 50)

A physician discloses personal health information when the information is transferred or released to another custodian, person or organization that is not required to follow the policies and procedures of the custodian.

A custodian shall not disclose personal health information that is in its custody or control unless it has obtained the individual's consent and the disclosure is necessary for a lawful purpose or the disclosure is permitted by PHIA.

A custodian shall not disclose personal health information if other information will serve the purpose of the disclosure.

A collection of personal health information made possible by a permitted disclosure as outlined in PHIA does not automatically make the recipient a custodian.

A physician must not disclose personal health information except with the consent of the patient or in accordance with PHIA, in particular Sections, 37, 38, 39, 40, 41, 42, 43, 45, 46, and 47.

Audit Record

A custodian that discloses personal health information shall make a note of the following:

- *the name of the person to whom the custodian discloses the information;*
- *the date and purpose of the disclosure and a description of the information disclosed; and*
- *the purpose of the disclosure, including with reference to the requirements of PHIA whether the disclosure was for the purpose of*
    - *further treatment of the patient;*
    - *health and safety of the patient or the public, including mandatory reporting requirements;*
    - *responding to a request from the College made under the Medical Act;*
    - *legal proceedings or enforcement purposes;*
    - *meeting another legal requirement;*
    - *research; or*
    - *payment for medical services.*

Audit Record within the EMR

A physician is not required to note the above information about a disclosure where *the physician permits access to the information stored in the electronic system and the system automatically keeps a log containing the following information:*

- *the user identification of the person that accesses the information;*
- *the date and time the information is accessed; and*
- *a description of the information that is accessed or that could have been accessed.*

Med Access provides all of the auditing capabilities outlined above.

Deceased Patients
A custodian may disclose personal health information about an individual who is deceased or presumed to be deceased without the consent of the individual who is the subject of the information

- *for the purpose of identifying the individual;*
- *for the purpose of informing a person whom it is reasonable to inform in the circumstances of the fact that the individual is deceased or presumed to be deceased and the circumstances of the death, where appropriate;*
- *to the personal representative of the deceased for a purpose related to the administration of the estate;*
- *to a spouse, partner, sibling or descendant of the individual where the recipient of the information reasonably requires the information 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; or*
- *for research purposes under the authority of PHIA*

Programs
A custodian may disclose personal health information without the consent of the individual who is the subject of the information 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;

A custodian shall disclose personal health information without the consent of the person who is the subject of the information to or via an information network designated in the regulations in which personal health information is recorded for the purpose of facilitating the delivery, evaluation or monitoring of a program that relates to the provision of health care or payment for health care,

Disclosure to a Successor

A custodian may disclose personal health information without the consent of the individual who is the subject of the information 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 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.

For the purpose identified above, a custodian who transfers a record of personal health information to its successor shall make reasonable efforts to give notice to the individual who is the subject of the information prior to the transfer or, where this is not possible, as soon as possible after the transfer that

it has ceased to be a custodian of the information and identifying its successor.

Disclosure related to Proceedings

A custodian shall disclose personal health information without the consent of the individual who is the subject of the information

- *to a body with statutory responsibility 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.*

A custodian may disclose personal health information without the consent of the individual who is the subject of the information

- *for the purpose of 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 in the proceeding or contemplated proceeding;*
- *to a committee listed below for the purpose of peer review or quality assurance activities;*
    - *the Provincial Perinatal Committee,*
        - *the Child Death Review Committee under the Fatalities Investigations Act*
    - *a quality assurance committee of a member, as defined under the Hospital and Nursing Home Association Act*
    - *a peer review committee of a member, as defined under the Hospital and Nursing Home Association Act*
- *to a proposed guardian or legal representative of the individual for the purpose of appointment of the person as a guardian or representative;*
- *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 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.*

Disclosure for Research Purposes

A custodian may disclose personal health information without the consent of the individual who is the subject of the information for research purposes but only where the research project has been approved by a research ethics board or research ethics body under the Health Research Ethics Authority Act.

Disclosure to Peace Officer

A physician in a clinic may be required to disclose personal health information for law enforcement

purposes. Whenever possible a custodian may obtain advice from CPSNL or NLMA before releasing information to the police under PHIA to disclose personal health information to the police.

Physicians' requirements to disclose information to police about gun shot and stab wounds are outlined in the Gunshot and Stab Wound Reporting Act. The Act imposes a mandatory duty on health care facilities to report to a member of the Royal Newfoundland Constabulary or the Royal Canadian Mounted Police any gunshot or stab wound within 24 hours of treatment of the injury, or offer of treatment. While the Act references health care facilities, the definition is not explicit and therefore, all physicians should be aware of the reporting requirements.

Managing Patient Consent and Masking

(PHIA s 23, 24, 25, 26, 27, 28)

PHIA outlines the elements of consent under the Act. *Where PHIA requires the consent of an individual for the collection, use or disclosure of personal health information by a custodian, the consent shall be a consent of the individual, knowledgeable, and shall not be obtained through deception or coercion.*

Limited Consent

There will be occasions when a patient gives only limited consent for the use and disclosure of his/her personal health information. Physicians are required to manage these limited consents according to the patient's direction whenever possible.

Withdrawing Consent

When a patient withdraws their consent, physicians must take all reasonable steps to comply with the withdrawal promptly after receiving it. Withdrawal of consent is not retroactive.

Patient Notice

The notice that the custodian uses when notifying patients of the clinic's information management practices and patient's rights, should include how the patient can manage his/her consent through masking or alternative methods agreed to by the patient and the physician. When a patient wants to limit consent the physician or qualified employees should provide the patient with the Consent Directive and Masking Form and have a conversation with the patient on the benefits and risks of limiting consent. This discussion should include who at the clinic will or will not be able to view the masked record and for what purposes.

The Med Access has the capability to mask personal health information from view by all or designated EMR users. Masking can be applied to the whole record, or selected elements of the record.

Implementing Consent Directives on Access or Use

The masking function helps physicians meet a request by a patient to restrict who can see his/her record in the EMR and what uses that personal health information can be subject to. It can also be used when a patient revokes consent to the further access and use of the information and the physician must take all reasonable steps to comply with the revocation.

If, through counselling, a patient agrees that masking might not be suitable at this time the patient and the physician can jointly monitor who accesses the patient's record.

The physician may be able to receive automatic alerts whenever someone has accessed the patient's record if that functionality is available in the practice's EMR. The patient could also ask to receive a regular audit report of who has accessed the record. It might be satisfactory to the patient to mask older information and leave current information available to authorized users of the EMR.

If the consent directive cannot be met through masking, auditing, or some other solution, the custodian should document the process of trying to find a solution. The result could be that the patient's record is masked and the authorize users of the patient's information will then have to override the masking with consent or without consent in appropriate circumstance.

Counselling a Patient on Consent Regarding Access or Use

Whenever a patient places a limit on who can access or on the uses of his/her personal health information it is important that the patient have a conversation with the person collecting or using the personal health information about the risks and benefits of the restriction.

The possible risks and benefits of a restriction on the access or use of personal health information by employees at the clinic can include:

- Inability to access necessary information during care outside the clinic, such as a hospital.
- No access by another member of the patient's care team within the practice to use for the patient's care.
- Care might be delayed as the Physician will not be able to prepare for the appointment.
- In extreme cases, when a patient refuses to allow an override of the mask, a health care provider might deny care because of lack of information and the patient will have to wait until the primary physician is available.

It is important to note, the patient's choice of consent cannot be coerced.

Implementing Consent Directives on Disclosures

When a patient requests that personal health information not be disclosed, the custodian should confirm what disclosures in particular the patient does not want.

Several disclosures are authorized without the consent of the patient. However, many of these disclosures without consent are discretionary in nature. This allows the custodian the opportunity to consider the consent directive of the patient and not disclose the personal health information.

Overriding a Consent Directive

When a record is unmasked, the EMR requires that a reason, consent type and duration be indicated.

A mandatory "Reason" field is presented to a user attempting to unmask a record. The reason provided should be as detailed as possible and at the very least include one of the following:

- 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

The type of consent used must also be indicated using the drop down list provided:

- Provider consent
- Patient consent
- Substitute decision maker
- Power of Attorney
- Report

The person authorized to unmask the record in the EMR should also indicate the time period the record is to remain unmasked. When unmasking a record in the EMR, a duration must be chosen. The duration should be the minimum amount of time required to carry out the identified purpose for accessing the record.

Safeguards

Organizational, Physical and Technical Safeguards

(PHIA Part II)

For the most part, PHIA establishes a general duty for custodians to implement safeguards. **COACH Guidelines for the Protection of Health Information** provide more specific direction on safeguards. More information regarding The COACH Guidelines are available from the Centre for Health Information.

Organizational Controls, relate to the activities and processes of the organization as a whole, including health professionals, employees, medical students and residents, contractors and other third parties that assist in protecting personal health information. Some examples are:

- Agreements,
- Staff Training,
- Breach Management Guidelines,
- Business Continuity/Disaster Recovery Policies,
- Retention, Storage, and Destruction Policies and Processes,
- Acceptable Use Guidelines,
- 6Email and faxing rules,
- Password rules,
- Retention schedules,
- Scanning rules.

Physical Measures are the physical actions that can be taken to protect personal health information. Some examples are:

- Locked building and locked office,
- Physically secured server,
- Lockable and fireproof filing cabinets,
- Location of equipment.

Technical Tools are security features found on computers, mobile devices, and other office equipment. Some examples are:

- User account management,
- Auditing of EMR users,
- System auditing,
- Technical controls restricting viewing of information,
- Data backups,
- Encryption,
- Anti-virus protection,
- Firewalls,
- Local Area Networks (LAN),
- Secure Wireless Network,
- Secure Portable Devices.

Agreements

(PHIA s. 22; CPSNL Bylaw 6)

The use of written agreements to document and formalize privacy and confidentiality obligations will assist custodians with meeting their general duties under PHIA. Using written agreements also has other practical benefits.

- The use of written agreements within a physician practice is recommended as a good business practice and risk mitigation tool.
- Good agreements will clearly state each party's responsibilities and liabilities and will provide documented evidence of the arrangements reached between the parties. When a dispute arises, the parties may not have the same recollection of the verbal arrangement. The use of a written agreement will reduce the risk of misunderstanding and disputes.
- Contracts and agreements are necessary when the disclosure is ongoing, usually in the course of services being provided by an external third party on behalf of the custodian.
- There are several types of agreement templates that are available in **Templates – Agreements** of the Privacy Resource Materials.

Information Sharing Agreement - These are used when personal health information is being disclosed by a physician to another custodian outside the regular referral process or to a non-custodian.

Information Manager Agreement - Where IT or information management services are being provided to a clinic and the service provider has access to the clinic's EMR system or other electronic systems, additional considerations will apply.

- A checklist has been prepared that can be used when reviewing agreements from an IT or Information Manager that uses its own agreement. This can be found in the **eDOCSNL Templates**.
- *Data Protection Schedule* – This schedule should be used as a supplement to a service agreement to protect the privacy and confidentiality of personal health information.
- *Third Party Confidentiality Agreement* – This agreement should be used as a supplement to a service provider's standard service agreement to address confidentiality and privacy concerns.

Clinic Exit Agreement -The purpose of a clinic exit agreement is to outline each physician's responsibilities when a physician leaves the clinic after the implementation of an EMR system. The agreement should establish each physician's rights and obligations with respect to the implementation, cost and ongoing operation of the EMR.

- Determine the terms and conditions that will apply in the event one of the physicians leaves the clinic.
- Description of the structure of the EMR and its database(s).
- The appointment of a lead EMR physician and the physician's responsibilities.
- The documentation of a transition plan including the required notice period, what original or copies of records the leaving physician is responsible for, and cooperation with the EMR vendor to facilitate the transfer of records.

- Commitment to comply with agreed upon technical, security or other protocols for the transfer of records.
- How to deal with the orderly transition of the information.

Clinic Information Sharing Agreement - This agreement outlines each custodian's roles and responsibilities for sharing/disclosing information with other custodians in the clinic and their commitment to ensure the security and confidentiality of the personal health information.

- Outlines physicians' roles and responsibilities for the sharing of personal health information between and amongst the signing physicians and their employees.
- Commitment to develop and use a common privacy and security policy and procedure manual.

Alternative to the Clinic Exit Agreement and the Clinic Information Sharing Agreements

Associates/Partnership/Management Agreement - Physicians use many different business structures to support the management and operation of their clinics. The issues addressed in the Clinic Information Sharing Agreement and Clinic Exit Agreement could already be addressed in the clinic's partnership or management agreement. Each clinic will need to check with their legal counsel to determine what is appropriate in each circumstance.

Managing Agreements

It is recommended that physicians establish a system to keep a record of all written agreements to which they are signatories. This record or a copy of it should be held off-site as part of the physician's business continuity plan. This is an example of a record of agreements.

Vendor	Subject of Agreement	Parties to the Agreement	Effective Date	Expiry Date	Location of Agreement
ABC Medical Storage Inc.	IMSP – storage and destruction of paper records	John Smith, ABC Medical Storage, and Drs. Jones, and Winter.	July 1, 2009	June 30, 2014	Filing cabinet in Dr. Jones' office E-version: admin/ contracts/storage

Breach Management

(PHIA s. 15)

The breach management process can be followed in situations involving personal health information in electronic and paper form that is under the custody or control of the physician. Breaches involving personal health information within the Electronic Health Record should be immediately reported to the Centre for Health Information Service Desk at 1-877-752-6006 who will assist in the management of the breach in cooperation with the clinic.

Understanding Breaches

Simply put, a breach is an unauthorized collection, use or disclosure of personal health information. The Information and Privacy Commissioner of Newfoundland and Labrador has described a privacy breach as:

A privacy breach is any collection, use or disclosure of personal health information that is not authorized under PHIA. For example, personal health information may be lost (a patient's file is misplaced), stolen (a laptop computer is taken from your office) or inadvertently disclosed to an unauthorized person (a letter addressed to patient A is actually mailed to patient B). However, a custodian may also become aware of breaches that are intentional; for example, an unauthorized access of patient files by staff[9].

Purpose

All custodians should write a breach management process to ensure they are able to respond quickly when they first become aware of any activity that is an actual or suspected breach involving personal health information. A written procedure ensures the physician and employees will be able to respond, investigate, analyze and remedy a situation quickly.

A custodian should also include in agreements with Information Managers and other third parties who have, or could have, access to personal health information, a requirement to report any actual or suspected breaches and to participate in the containment, investigation and analysis of the breaches. A copy of the custodian's written policies and procedures should be appended to these agreements as well.

Considerations When Writing Breach Management Policy and Procedures

- Identification of how the physician becomes aware of an actual or suspected breach and how this influences the response to the breach including:
    - Auditing users of the EMR – managing the response will primarily be internal, although patients might still need to be notified.
    - From the Patient – when patients report an actual or suspected breach they might exert influence on timelines and other aspects of the investigation.
    - From the Office of the Information and Privacy Commissioner – the OIPC might notify the physician of an actual or suspected breach and might become involved

[9] http://www.oipc.nl.ca/custodians/privacy-checklist

in the investigation if it considers that the physician needs assistance to conduct the investigation properly. The OIPC may also issue a public report regarding the breach.
  - Media – the actual or suspected breach might be reported in the media before the physician is aware of it. In these situations all actions by the physician will be in the public eye and the OIPC might become involved immediately.
  - Another custodian – other custodians could notify the physician of an actual or potential breach and, in some cases, it may result in or require a joint investigation.
  - IT support or EMR vendor – their involvement with the investigation will be from the beginning. They might have even contained the breach before contacting the physician.

Breach Management Process

The Newfoundland and Labrador Department of Health and Community Services has issued guidelines on managing breaches. For more information and to view these guidelines, download the PHIA Risk Management Toolkit found here: http://www.health.gov.nl.ca/health/phia/

Contain the Breach – stop the breach from continuing. If the breach is in the EMR, whether through an unauthorized access, a hacker, or a hijacking (viruses, worms, Trojans), disconnect the Internet and the LAN, then contact IT support to determine how to contain the breach.

Investigate the Breach – determine the cause and the events surrounding the breach. Document all aspects of the investigation, people involved, information involved, and timelines; this will be used in the analysis of the actual or suspected breach by the clinic's investigation team. If the Office of the Information and Privacy Commissioner or the police become involved they will need this documentation.

Evaluate the Breach and Associated Risks – understand what happened, if personal health information was involved and determine if patient notification is necessary.

Notification of Interested Parties and Patients – who needs to be notified and when.

- NLCHI – contact the NLCHI Service Desk at 1-877-752-6006 if the breach involved information that was received from or was being disclosed/transferred through the EHR.
- Other physicians in a joint practice – Other physicians in the same clinic should be involved either to aid in the containment or at the beginning of the investigation.
- Other Custodians - contact the Privacy Officer for the other custodian(s). If the breach involved information that was received from or being disclosed/transferred to the other custodian they might need to be involved in the containment.
- Police – contact the police when the breach is caused by a theft or other criminal activity. They might want to be part of or lead the investigation of the incident. If the breach is a result of an external intruder into the EMR, inform the police and they will indicate if they want to be involved and when.
- Newfoundland and Labrador Medical Association – the NLMA can provide advice and identify the necessary expertise to help physicians in the breach management process.
- Vendor – the EMR vendor might need to be contacted to assist in the containment of the breach if the breach involves the EMR.
- Other third parties – the notification of other third parties will depend on the type of

breach. Example: if the office was broken into the landlord should be contacted, or if it is information used in a clinic trial the researcher should be contacted.

- Research Ethics Board – if the breach was by a researcher in custody of the personal health information for research, notify the Research Ethics Board.
- Office of the Information and Privacy Commissioner – it is a requirement of PHIA to notify the commissioner of a material breach. In addition, the OIPC can provide valuable advice and guidance to physicians involved in a breach. Contacting the OIPC will not immediately open an investigation file.

Prevention

Conduct a thorough review of all privacy and security policies, procedures and activities to develop recommendations and strategies to minimize future risk.

Violation of clinic policy and procedures should be considered to be grounds for disciplinary action. Custodians should consider creating a progressive discipline policy that establishes penalties up to and including termination and/or reporting to the appropriate regulatory authority or body, depending on the seriousness of the violation.

Patient Notification (Breach)

(PHIA s. 15)

The **Breach Management** discussion provides guidance to custodians on what to consider when drafting a breach management policy and procedures. One of the steps in the breach management process is the notification of patients. This topic provides guidance on the factors to consider when drafting a policy for patient notification. Breach Management and Patient Notification can be written as two policies or one.

Obligations to Notify Patients

PHIA requires a custodian to notify the individual who is the subject of the information at the first reasonable opportunity where information is stolen, lost, improperly disposed, or disclosed to or accessed by an unauthorized individual.

It is recommended that physicians enter into contractual arrangements with Information Managers that include how breaches and patient notifications are managed. The custodian can also have information sharing agreements with other custodians and non-custodians for one-time or ongoing sharing of personal health information. These agreements should all include a requirement that only the custodian approves the notification of patients if a breach occurs involving that information.

Determining if the Patient(s) Should be Notified

The key consideration in deciding whether to notify affected patients is based on the harm or potential harm to the patient. Review and assess the breach to determine whether or not notification is required; document any analysis and decisions.

Considerations should include:

- The severity, scope, and nature of the breach,
- The sensitivity of the information,
- The expectations of the patient when information was collected, i.e. did the clinic provide information to patients that they would notify them if there was a breach,
- Where the personal health information was disclosed to a custodian or non- custodian;
- Probability and gravity of harm;
- Also consider the potential harm to the clinic, medical profession, or EHR system, including loss of trust, if the patient is not notified but becomes aware of the breach.

Preparing to Notify Patients

Patients should be notified as soon as possible once the breach is understood.

- Consider consulting legal counsel, CPSNL, the NLMA and/or the OIPC before notifying patients.
- If police are involved, confirm a notification timeline with them to avoid compromising their investigation.
- Designate one person to speak publicly on the matter, ensure this person has the most up-to-date information on the breach and can provide the official response.
- Prepare a statement for the clinic's receptionist should patients call.

- Ensure the custodian and/or privacy officer are prepared.
- If providing third party information in the notification, such as contact information for the Ministry of Health Privacy and Access Office or the OIPC, ensure they are contacted beforehand so they can prepare for inquiries from patients.

Notifying Patients

- Patients should be directly notified at the first reasonable opportunity via a telephone call. If a large number of patients need to be notified, a letter may be sent.
- Notification should be adapted for patients who have difficulty understanding why they are being contacted.

Indirect Notification of Patients

- Indirect notification could be through a clinic's website, posted notices or through the media.
- Indirect notification is appropriate addition to a formal letter in situations where:
    - direct notification could cause further harm to the patient,
    - contact information is not available or is out-of-date,
    - a very large number of people are affected by the breach

Details Included in Notification

The notification, whether direct or indirect, to a patient(s) about a breach should include:

- Date of breach,
- Details of the breach and the personal health information involved,
- Steps that have been taken to address the breach,
- Potential risks to the patient,
- Contact name at the clinic for the patient to get more information and,
- Contact information for the OIPC and other third parties patients might wish to contact, such as the MCP and the Department of Health and Community Services to inquire about possible inappropriate use of the MCP number.

Developing a Business Continuity Plan

Business continuity planning is a process that helps organizations prepare for disruptive events. A business continuity plan assesses all aspects of an organization's operation for critical activities that need to be restored quickly and the steps to achieve this. Such a plan will allow a clinic to continue operations in the event of a disruptive event.

Planning in advance will allow clinics to respond quickly in an emergency to facilitate the return to delivering patient care with minimal loss of time and patient information whether the event is a power outage or a pandemic.

For a breach that involves the inability to access personal health information use the **Breach Management** guidelines in conjunction with the plan.

As part of eDOCSNL, an automatically scheduled business continuity copy of a portion of the clinic's EMR data will be retained by staff at the end of each business day. The business continuity copy is stored on a local continuity workstation and will contain the clinic schedule and a patient detailed chart summary. This process will assist clinics in ensuring that necessary patient data is available in the event the EMR is unavailable. Physicians should periodically confirm this process has been carried out to ensure patient data is available if needed.

Clinics are encouraged to develop a business continuity plan to complement the availability of EMR data in the business continuity copy. A business continuity plan should include:

- Emergency contact numbers
- Employees contact numbers
- Vendor and other third party contact numbers with account numbers for the medical practice
- Recommended alternative sites for patients to receive care
- A plan on how to notify patients if their appointment is cancelled or they should go to an alternate location.

Retention Periods for Personal Health Information

(PHIA s. 15; CPSNL Bylaw 6)

It is important that physicians establish and follow a written retention period for records of personal health information. As long as the record exists, or until the physician transfers the records to another custodian, the physician has responsibility for it. These responsibilities include secure storage and destruction, availability of the personal health information upon patient request for access, and ensuring the information remains retrievable, readable and useable for health care purposes even if it will not be used for that purpose again.

As a clinic shifts to an EMR, physicians should place an emphasis on ensuring their records are retained in compliance with PHIA and Bylaw 6. The impact of any upgrade to an EMR on patient records should be discussed with Telus prior to installation.

There are several sources to consider when determining how long records should be retained. While PHIA does not specify a retention period for personal health information, CPSNL Bylaw 6 requires physicians to maintain a patient's medical records for a minimum of 10 years after the patient was last treated. In the case of a patient under the age of 19, records must be retained until the patient has turned 21 years of age or for 10 years following their last treatment, whichever is the longer period.

Physicians should set a retention period that at a minimum complies with the CPSNL By-Laws and allows for records to be held as long as necessary for patient care, and within the policy include an exception to allow for individual records to be held longer if determined necessary.

Physicians may be concerned about destroying records that are then required for a legal reason. Both the courts and the Privacy Commissioner of Canada have deferred to retention periods established by organizations thoughtfully and in good faith. A policy of permanent retention of records is generally not an acceptable retention period.

Patients could request that a record be destroyed earlier than the retention period. If a physician has established a written policy based on medical and legal factors the request does not need to be met.

Storage of Personal Health Information

(PHIA s. 13, 17, CPSNL Bylaw 6)

Secure storage of records of personal health information is essential for all custodians. Secure storage integrates the three types of safeguards: organizational, physical, and technical. For more information about safeguards see Organizational, Physical and Technical Safeguards.

Storage at the Clinic

Best practice suggests that three locks should be used to protect personal health information. For paper records physical measures such as a locked building, locked office and locked filing cabinets are appropriate.

Many clinics have their active paper records conveniently located behind the reception desk in open shelving. During the time the clinic is open to patients the reception counter acts as a physical barrier. However, these shelving units should be locked at night.

Practices should consider other ways of physically securing the records, such as a motion sensor that detects after hour intruders. If physicians purchase new storage units for active records they should consider fireproof filing cabinets.

Inactive Paper Records

The same principle applies to records in long term storage before destruction; locked building, locked office, and locked storage room.

The storage room should be single purpose, or if it is a room used for storage of supplies and other things it should be accessible by a password keypad (available at local hardware stores) or swipe card.

Electronic Records

Active records stored in the clinic's EMR will be managed by Telus Health.

Off-Site Storage

If a custodian arranges off-site storage that is still managed by the custodian, such as a physician's home, be sure it has greater protection than onsite storage as there will not be the same daily oversight by employees at the clinic's office. If an Information Manager is used for offsite storage, an agreement should be in place.

Scanning and Destruction of Original Paper Records

(CPSNL Bylaw 6)

With the adoption of the EMR, many physicians who have a vision of a paperless office find that even after scanning they are still responsible for the old paper records and new patient information received by mail and fax.

CMPA advises that if paper records have been converted to electronic files, it may be reasonable that they be destroyed[10].

The scanning process must create an unalterable digital image of the original paper record which, if done correctly, will be admissible in a legal proceeding in place of the original paper record. Portable Document Format or PDF is a popular format for a scanned document. A quality assurance process should be developed to assist clinic staff with managing the quality of scanned records.

The physician is required to develop and document scanning, quality assurance and destruction procedures that are consistently followed in the clinic.

The types of procedures that should be in place include:

- Assigning one person to be responsible for scanning,
- Training employees regularly on the scanning procedures,
- Document how the paper record is to be scanned to ensure the accuracy, completeness, retrievably, readability and usability of the information,
- Scanned document must be saved in a read only format,
- Document results of quality assurance test,
- When and how the paper original is destroyed,
- If a partial paper chart is scanned and destroyed, a note in the paper record should indicate that personal health information was scanned into the EMR, the date of the scanning, and the date of the destruction after scanning,
- If a full paper chart is scanned follow the documentation procedures for destroying records.
- Procedures to ensure scanned documents are complete, retrievable, readable, and useable could include:
    - Random checking of several originals against the scanned documents,
    - Retaining the original paper document for a short time period as a reference.

[10] https://www.cmpa-acpm.ca/documents/10179/24937/com_electronic_records_handbook-e.pdf

Destruction of Paper Records of Personal Health Information

(PHIA s. 15)

Records should be stored securely and according to the policy of the clinic.

Records need to be retained for the minimum time period established in the clinic's retention policy.

Records must be stored in a format that is retrievable, readable, and useable for the purpose for which it was collected and for the full retention period set by the clinic.

Scanned records should only be securely destroyed in accordance with the scanned records policy.

Before any records are destroyed it is recommended that the custodian sign a confirmation of the records to be destroyed. This confirmation should include several details:

- Who will be performing the destruction?
- What method will be used to destroy the records?
- The date the records are scheduled for destruction.
- Location of records to be destroyed, i.e. in office or offsite storage.
- A list of the records with the patients' name, physician's name, and the last year an entry was made.

Paper records need to be destroyed to a degree that they cannot be recreated. Methods include:

- Crosscut shredding not strip shredding, crosscut shredding can then be recycled,
- Private companies can be hired to shred records this may be done either on site or off. One needs to ensure that the proper agreement is in place (see Agreement Templates),
- Burning to a white ash with no partially burned pieces remaining,
- Pulping or pulverizing.

Personal health information stored in other mediums such as X-rays, labeled prescription bottles, etc. need to be destroyed in a secure manner.

Acceptable methods of destroying confidential information recorded on microfilm, photographic negatives, motion picture films, or other photographic media include pulverization and chemical disintegration.

Containers used for prescriptions and bodily substance samples can have their labels removed and then the labels are securely destroyed, or the bottles with labels can be given to a private company to destroy.

Using a Private Company for Destruction of Records

A private company can be engaged to securely destroy (i.e. shred, burn, pulp) medical records.

- In such cases, the physician should enter into an Information Management agreement with the company. The agreement should include requirements that the company:
    - Have written privacy and security policies that are made available to the

physician,

- Provide a Certificate of Destruction for each time records are destroyed and a verification that includes the method of destruction used,
- Have a confidentiality agreement with each employee,
- Is willing to submit to independent audits by the physician or the physician's representative.

It is recommended that custodians contract the destruction of records to a certified member of the National Association for Information Destruction (NAID) or a company that adheres to the principles of NAID. NAID's website is www.naidonline.org. As of May 2016, there was one company NAID certified in Newfoundland and Labrador, Iron Mountain. The physician needs to ensure there is secure transfer of the records to the destruction site.

After Destruction

Upon completion of destruction whether by employees or a private company a confirmation of destruction should be signed by the person supervising the destruction. This can be managed by using a log in the clinic which is signed when records are destroyed.

Destruction of Non-Confidential Records

Records that contain non-confidential information can be discarded by any means consistent with the clinic's waste management practices and the waste removal requirements of the locality where the records will be discarded. Recycling is an acceptable method of destroying records that contain non- confidential information.

Reference

Ontario Information and Privacy Commissioner and National association for Information Destruction, Inc., Get Rid of it Securely to Keep it Private: Best Practices for the Secure Destruction of Personal Health Information http://www.ipc.on.ca/English/Resources/News-Releases/News-Releases- Summary/?id=899

Destruction of Devices containing Personal Health Information

(PHIA s. 15)

Devices, such as servers, computers, laptops, fax machines, and photocopiers, retain personal health information on their hard drives even after the user has deleted the information using the application delete functionality.

To securely and permanently delete this information, the hard drive should be destroyed. A company certified by the National Association for Information Destruction (NAID) or a company that adheres to the principles of NAID should be used. NAID's website is www.naidonline.org. They will degauss the hard drives or use some other method of destroying the information permanently. As of May 2016, there was one company NAID certified in Newfoundland and Labrador, Iron Mountain.

- Physicians should maintain an up to date list of all office and medical equipment that retains personal health information.
- Media must be securely stored pending destruction.
- Before a device that contains personal health information is destroyed the information should be backed-up or archived.
- The policy and procedures for retention and destruction of personal health information should be followed when destroying these devices.

User Account Management

(PHIA s. 48, CPSNL Bylaw 6, 19(f)(i))

Custodians need to ensure the proper ongoing management of the accounts of users of the EMR.

- One person should be assigned the responsibility for account management.
- The activities that could require changes in a user's account include:
    - Disable generic or shared user accounts,
    - Disable inactive accounts,
    - Changes in employment status. This is particularly important when someone is terminated.
- Role-based access controls use technology to ensure that access to the patient record is based on the "need to know" principle. Only users that require access as part of their job function should be provided with credentials to access the EMR.

Access Privileges

- The EMR system requires that each user has defined access privileges. The user account manager should ensure that each user's access is determined according to their need to know information to complete their work. Do not use a default setting of full access.
- The user account manager should ensure that each user's access to the EMR solution is based on the "least privilege" principle. Systems must enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The default setting of full access should not be used.
- Access to security functions within the EMR as well as security-relevant information, such as audit logs, should be restricted to authorized users only.

Passwords and Logins

- EMRs should be accessed by multi-factor authentication – In the provincial EMR, this will be a combination of a user name and password, as well as a randomly generated code.
- Passwords should be treated as sensitive, confidential information and never shared with others or revealed in email, chat or other electronic communication.
- Passwords should never be written down or stored online without encryption.
- Require the use of strong passwords and PINs that have a minimum of 8 characters and a mix of letters, numbers, symbols, and upper and lower case.
- Require automatic password protected screen savers that are activated after a maximum of 10 minutes and sooner in high traffic areas.

HEALTHe NL

Custodians are also responsible for authorizing employees, other health professionals, students and residents access to HEALTHe NL.

EMR and EHR Auditing

(PHIA s. 48, CPSNL Bylaw 6, 19(f))

The auditing function in the EMR is valuable for supporting the custodian's responsibility to restrict access to personal health information to those who need to know, making available to patients a record of activity associated with their electronic record, and when investigating a breach.

As valuable as auditing user activity is, it will only detect when a breach has happened, it will not prevent an inappropriate use or disclosure. Educating EMR users on the auditing functionality might reduce the chance of them browsing records and other inappropriate uses.

The audit logs and audit reports from the EMR are personal health information about the patient. They should be retained as long as the personal health information it is associated with and in compliance with the clinic retention policy.

Responsibilities for Audit Logs

The custodian is responsible for the proper management and use of the auditing information.

These responsibilities include:

- Ensuring at least one person within the clinic is trained on how to use the auditing function,
- Restricting access to the audit logs and reports to those who need to know,
- Ensuring employees, other health professionals, and medical students and residents are aware that all actions within the EMR are audited,
- Determining what information will be collected in the audit log,
- Developing a standard report for audit logs, one by user and another by patient and an understanding of how to run ad hoc reports,
- Establishing a regular schedule for reviewing audit logs,
- Implementing an automatic alert if there is an override or an attempt to override the masking of a record, if it is a function available in the EMR,
- Establishing procedures for storage, retention, and destruction of audit logs consistent with personal health information,
- Ascertaining from Telus if their users can be audited,
- Ascertaining from Telus if the audit function can run a report on the physicians and custodians that should be notified when an amendment is made to a patient's record,

Information in an Audit Log

Custodians need to determine what information they would like collected in the audit log. Telus will confirm if the audit log can record the information. The recommended information is:

- Name and/or ID number of the patient,
- Name and/or ID number of user,
- Date and time of access,
- Name of the patient's primary physician at the practice,
- Information that was accessed,
- Access to masked information,
- Overrides of masked information,

- Failed attempts to access masked information,
- Changes in consent directives,
- Action performed related to personal health information – create, add, modify, delete, view, or disclose,
- Successful and failed login attempts,
- Preserves the original content of the recorded information when changed or updated,
- Account creation, modification, and deletion.

The Metadata in the audit logs is considered personal health information and should be retained as long as the personal health information it is about.

Monitoring Program

- Custodians should develop procedures documenting the monitoring of EMR users.
- There should be a designated person responsible for the audit monitoring program.
    - The person responsible for authorizing ad hoc reports on user activities should not be the one who runs the reports. This separation of duties might not be possible in small practices.
    - The person who will receive automatic alerts of overriding of masking.
- What action will be taken if the audit report shows an EMR user has accessed a record without authorization?
    - Who will this action be reported to?
    - Will EMR privileges be revoked immediately until an investigation of the breach has been completed?
- Custodians should consider creating a progressive discipline policy that establishes penalties up to and including termination and/or reporting to the appropriate regulatory authority or body, depending on the seriousness of the violation

Auditing Users of the EHR

If a physician has concerns about an employee's access of HEALTHe NL , the Centre for Health Information should be contacted.

Acceptable Use of Technical Resources

It is important for clinics with EMRs to establish expectations for all employees, physicians, and third parties around the appropriate use of the practice's technical resources. The intent of an acceptable use policy is to ensure awareness and understanding of each person's accountability for using resources in a secure and privacy protective manner.

The clinic's technical resources include the EMR, operating systems, storage media, network accounts, email accounts, Internet, and mobile technology such as laptops, cell phones, and tablets.

Inappropriate uses expose the clinic to risks that include virus attacks, compromised network systems and services, and illegal activities.

Acceptable Use Agreement

- Each user is assigned a user name and a password or some other method for the EMR to authenticate the user.
- Together a user name and password give each authorized user of the EMR a user account.
- Before a user is assigned a user name and password they are expected to sign an acceptable use agreement which explains the responsibility for appropriate use of technical resources.
- The acceptable use agreement is in addition to any confidentiality agreement the person might have signed.

Acceptable Uses

For purposes related directly to patient care and the administration of the clinic. All users should be monitored for access to the EMR and other equipment, systems and networks where the password and user name are used.

User Responsibilities

Users are responsible for any and all use of their user accounts including protection against unauthorized access to their accounts. Therefore, users should not share passwords or any other access control information for their accounts.

Users are responsible for ensuring the confidentiality of all personal health information they have been granted access to, including:

- Ensuring the information is not observed by others while working at a computer,
- Ensuring they are logged out of their accounts when not at their computer,
- Exercising discretion when printing personal health information which can be viewed or observed by unauthorized persons,
- Refraining from copying, sending, duplicating or transmitting by any means, personal health information for any purpose other than patient care or a purpose identified to the patient or required by law.

Users are required to comply with all copyright and license conditions, such as:

- Refraining from moving, copying or transferring programs, files or other forms of software from one computing system to another without proper authorization to do so,

- Refraining from distributing, selling or making available software to any person where prohibited by copyright or license,
- Refraining from accessing and using software without proper authorization and license rights.

Passwords and Security

Employees and physicians are required to take all necessary steps to prevent unauthorized access to personal health information.

- Keep passwords secure and do not share accounts or passwords.
- Change passwords at least quarterly.
- All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the user leaves the computer.
- Employees and physicians need to use extreme caution when opening e-mail attachments received from unknown senders, which can contain viruses, e-mail bombs, or Trojan horse code.

Personal Use

The custodian should establish acceptable practices for employees to use the computers for personal activities such as e-mail and Internet access providing such activities do not interfere with the person's work schedule or responsibilities. The custodian should not allow:

- Any use that involves discriminatory, disparaging, defamatory or harassing comments,
- Employees to access or view inappropriate content on the internet, such as websites that promote hate or that offer pornography, or to participate in electronic gambling,
- Posting on Facebook, twitter, blogs, and other similar media cannot mention, harm or tarnish the image or reputation of the practice, its patients, employees or physicians,
- Employees to use the practice's resources for streaming or downloading videos,
- Employees to use the practice's resources for personal gain.

Unacceptable Uses

Unacceptable uses include breaching legal and security protections provided by legislation, copyright and/or license to computer programs, technology or data. In addition, the use of technical resources to engage in any behaviour that might jeopardize the practice's security, including, but not limited to:

- Willfully bypassing or subverting the administrative, physical or technical electronic or procedural security controls,
- Attempting to alter or destroy resources (e.g. data, networks, electronics),
- Deliberately propagating malicious code (e.g. viruses, worms, Trojans),
- Generating or transmitting unsolicited commercial or advertising material such as spam or chain mail,
- Send anonymous messages.

Examples of the Acceptable Use of Office Technology Policy

Technology	Core	Incidental	Incidental/ Unacceptable	Unacceptable	Against Existing Policy	Illegal
Phone	Making appointments for patients	Making a brief personal call	Spending a lot of time on personal calls resulting in work not being completed	Phoning 1-900 numbers on the clinic phone	Discussing personal health information in a manner or place that allows others to overhear.	Discussing personal health information with a drug rep
Mobile Phone	Making a work related call, email, text message or ping	Making a brief personal call, email, text message or ping	Making personal use of mobile phone that results in work calls or duties not being done	Phone 1-900 calls on a work mobile phone	Sending personal health information in an unencrypted email, text message or ping.	Sending personal health information in an email, text message or ping to a drug rep
Photocopier	Making copies of test results for a patient	Making a copy of a son's hockey schedule	Making copies of the hockey schedule for all the team members	Making a large number of copies of a garage sale	Copying a patient's chart without permission of the physician or privacy officer	Copying a patient's chart to give to a drug rep
Fax, including from the EMR	Faxing a referral letter	Faxing a trip itinerary to one family member	Faxing the full hockey team with the team's stats	Faxing your resume to potential employers	Faxing personal health information to another clinic without attempting to eliminate or minimize the amount of personal health information included in the fax	Faxing a list of patients to a drug rep

Email	Sending an email to a patient with education information requested by the patient	Emailing a friend to confirm lunch	Emailing the hockey team organizing rides to practices and games	Forwarding chain emails	Sending personal health information in an unencrypted email	Making libelous statements about co-workers in an email
Computer/ Tablet	Viewing a patient chart	Preparing a to do list for the kids' sitter	Writing a lengthy personal letter to a friend	Work is not done on time because you are playing solitaire	Viewing a patient's chart without permission	Installing a pirated version of software onto the office computer
Internet	Researching training courses and conference for the physician	Checking the hockey team's standing	Researching issues of personal interest during work hours	Watching YouTube during office hours.	Turning off the security features so you can play online poker	Downloading or sharing copyrighted movies or music
Social Media and Websites	Posting a job opening on a job site.	Checking Facebook on a coffee break	Watching videos that cause the network to operate slowly	Checking Facebook and Twitter during work hours	Tweeting about patients even if names are not used.	Posting personal health information about a patient who plays for the Rough Riders on a gossip website

Transmitting by Fax and Email

Clinics need to transmit personal health information by fax and/or email many times a day. In doing so, custodians need to recognize that this is a high risk activity that can potentially result in a breach of personal health information. Some of the risks from using faxes and emails include:

- Sending the document to the wrong number/email address resulting in the document being received by an unintended recipient without a legitimate 'need to know'.
- Sending the document to the correct number/email address but it is viewed by an unintended recipient (example, the faxed information is left unattended or the fax machine is located in an area where multiple people have access or the email address is one used by several people in the clinic).
- The fax number/email address of the recipient has changed or the intended recipient is no longer employed by the organization.
- Emails pass through several points on the Internet during the transmissions that are not secure and are a potential breach point.

When using email as a method of communication with patients, CMPA recommends obtaining consent from the patient first[11]. If clinics proceed with using email, only the minimum amount of personal health information necessary should be sent via email. If possible, clinics should remove any unnecessary personal identifiers.

Secure Email and Fax Tips

- Use an email provider that supports secure, SSL-enabled POP and IMAP connections. Do not use Hotmail, Gmail or other free email for transmitting personal health information.
- Use person-specific email accounts. Do not use a general office email address to send or receive personal health information.
- Send personal health information as an attachment that is encrypted with strong encryption.
- Always use a covering letter or text in the email and attach the personal health information as a second page in the fax or an attachment in the email.
- Ensure there is a warning that the information is only intended for the person identified as the recipient.
- Ensure the covering letter/email text includes the name of the intended recipient and the person sending the information.
- Use saved speed-dial numbers for frequent fax recipients to prevent numbers being misdialed. Test these numbers periodically.
- Put email addresses in the email address book. Confirm email addresses periodically.
- For any new recipient, fax or email, verify the fax number or email address with a test sent before sending health information.

[11] https://www.cmpa-acpm.ca/safety/-/asset_publisher/N6oEDMrzRbCC/content/using-email-communication-with-your-patients-legal-ris-1

- Develop policies on what to do if a fax was sent to the wrong place.
- Configure the fax machines to never save copies of received faxes.
- Make sure that faxes do not remain on the fax machine after receipt, and that they are promptly delivered to the intended recipient. Assign this responsibility to one or two employees.
- Policies on the storage and destruction of records should include procedures for faxes and emails.
- As with all disclosures of personal health information based on deemed consent, custodians must only disclose personal health information to another health professional in accordance with the ethical practices of the profession and in accordance with their policies.

Risks of Using Email

- Email transmission is not guaranteed to be secure or confidential; unauthorized individuals may be able to intercept, read and possibly modify e-mail you send or are sent by your physician or clinic.
- Email may inadvertently be sent to wrong destinations or to the wrong individual.
- Employers may monitor email sent or received by employer-owned systems.
- Email can be used to spread viruses, some of which may cause unauthorized email distribution.
- Email can be forwarded without the authorization or detection of the source author.
- Shared family email accounts can jeopardize confidentiality.

Acceptable Use of Email

- Email should only be used for non-urgent issues such as routine enquiries or appointment information.
- Never use email for communication of serious, urgent or time-critical medical issues like suffering from chest pain or severe low blood sugar levels.
- We do not advise using email when discussing sensitive information such as sexually transmitted diseases, mental health problems, drug treatment or alcohol-related disorders.

Formatting an Email

- Type “CONFIDENTIAL” and the reason for the communication in the Subject line. Example: “Subject: CONFIDENTIAL – Medical Question”
- State your message simply and include the following:
    - your full name
    - telephone number (where we can reach you)

Fax and Email Upgrades

- Use email encryption software, and consider the use of a fax machine or fax modem that encrypts transmissions.
- Ensure access to fax modems and emails are password protected.

Other advice

- Provide CPSNL with any changes to physician fax numbers.
- Inform people who regularly fax or email personal health information of any changes in the fax number or email several times.
- Establish procedures to addresses faxes and emails received in error.
- Use a secure location for fax machines, computers, and monitors.

Wireless Devices and Networks

The use of wireless devices is becoming more common in clinics. Custodians need to ensure they meet the highest standard of security for these tools if there is any possibility they will be used for viewing or storing personal health information. Today encryption is considered the standard for making information unreadable. More information about encryption is included in the discussion of General Security Software. Physicians and their IT support should monitor evolving best practices in this area to ensure continued security of the practice's network and wireless devices.

Risks of Wireless Networks

Unsecure wireless networks can provide access to the medical practice's network by a knowledgeable person.

- Only use secure wireless networks; those where a password is required to connect to the network.
- Only use secure websites when personal health information is involved; look for the padlock symbol in the address bar or the icon tray, or only use sites with an address that begins **https://** and has it on every page.

Data on unencrypted wireless networks is easily captured by an unauthorized person.

- Encrypt all information on wireless devices, although this only addresses information sent not received.

Use WPA2 security in the modems purchased for use in the clinic and at home.

- Do not provide the wireless encryption key to people who do not have authorization to access personal health information at the clinic.
- Use a minimum 128bit encryption standard.
- Have an IT professional test the wireless network periodically for weaknesses.
- Do not rely on WEP encryption.

Risk of Wireless Devices

Wireless devices such as laptops, Smart-phones, and tablets are easily lost and therefore require greater protection than stationary devices.

- Personal health information should not be stored on mobile devices except for those that are designed and will be used for long term encrypted storage.
- Occasionally personal health information and other confidential information are stored on mobile devices for short time periods.
    - Ensure the device is password protected and the information is encrypted.
    - Some devices have software that allows for all information to be deleted from the device remotely if the device is lost.

Before a new wireless device is used, an assessment should be made of its security. Ask questions such as:

- Does this device use encryption and if so how well tested is the encryption protocol?
- What is the cost of implementing a secure encryption protocol?
- Has this type of device been used on our network before?
- Can this device be configured to only allow authorized users to access it or the network

through it?

- How easy will it be for an attacker to fool this device into allowing unauthorized access? What methods could be used?
- What secure authentication schemes are available and what cost or overhead is associated with their implementation and maintenance?
- How practical is wireless use considering the cost, potential loss, and added convenience?
- How secure is the authentication mechanism to be used?
- How expensive is the authentication mechanism to be used?
- How secure is the encryption mechanism?
- How sensitive is the data traveling through the wireless device?
- How expensive is the encryption mechanism?

General Security Software Encryption, Firewalls, Malware, and VPNs

Encryption

Encryption is the altering of data so that it is unreadable by anyone who does not have the key to unscramble the information.

- Encryption can be either hardware or software.
- It can be used on hard drives of servers, computers, and mobile devices
- It is very important to use encryption on laptops, USB keys, and other mobile devices like Smart-phones and tablets.
- There is also encryption software for email attachments.
- Web browsers will encrypt text automatically when connected to a secure server.
- Without encryption, information passed over the Internet is not only available for virtually anyone to capture and read, but is often stored for years on servers that can change hands or become compromised in any number of ways.
- For more information see two publications from the Ontario Information and Privacy Commissioner, Healthcare Requirements for Strong Encryption, and Encrypting Personal Health Information on Mobile Devices. www.ipc.on.ca

Virtual Private Network

If the EMR is accessed remotely by physicians or vendors, custodians are advised to set up a virtual private network. This can be accomplished through a hardware or software.

Virtual Private Networks or VPNs are strongly recommended if the physician is using a wireless network or if the backups are done remotely.

Security Software

Security software is essential for all computers. Custodians are advised to work with an IT professional to determine the appropriate software for the clinic and an update schedule.

- Updates to security software will be an ongoing cost to the clinic.
- Install all vendor supplied updates
- Physicians should get annual contracts for upgrades to firewalls, anti- virus, and malware.

Firewalls

A firewall is a device or set of devices, either hardware or software, designed to permit or deny network transmissions based upon a set of rules.

- Firewalls are used to protect networks from unauthorized access while permitting legitimate communications to pass.
- Medical practices should install a network firewall and personal firewall software on all computers.
- The clinic should never turn off the firewall.

Anti-virus Software and Malware

Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior.

Anti-virus software is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, Trojan horses, spyware, and adware.

- Ensure the anti-virus software is set to receive the latest virus definitions and scanning updates from your Internet service provider automatically.
- Purchase anti-virus software for computers and services and set to receive the latest virus definitions and scanning updates from the vendor of the product automatically.

General Office Security

(PHIA s 15; CPSNL Bylaw 6)

The importance of the physical security of the clinic's office cannot be overlooked.

Office Area

The full office needs to be securely locked after hours with a limited number of access keys available.

- Windows can be a point of entry and efforts should be made to secure these particularly if office equipment is visible through the windows.
- Ensure the landlord agreement includes conditions around when the landlord can access the office area.
- Consider locks that require using an access card and that records all people who access the office.
- Ensure keys are returned or locks changed when an employee, other health professional, medical student or resident ceases to work at the clinic.
- Larger clinics should consider implementing security badges.

Office Equipment

Place monitors, printers, and fax machines where patients, unauthorized employees and others cannot see personal health information on them.

- If possible, keep office equipment in an office that can be locked.
- Place servers in an environmentally safe area and secure it to the floor or wall, or place in a locked cupboard.
- 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 these small storage media.
- Never leave portable equipment unattended when taken outside the office, such as in cars or hospital cafeterias.
- Require employees to set the lock screen or log off whenever they leave their workstation unattended.