The Newfoundland and Labrador
Council of Health Professionals (NLCHP)

Privacy, Confidentiality and Consent

Standards of Practice and
Resource Manual

May 29, 2015

Table of Contents

**The basis and format of this text was inspired by a similar document created by the Newfoundland and Labrador Pharmacy Board (NLPB) in September 2002. The NLCHP gratefully acknowledges the permission of the NLPB to use this work in its preparation of privacy standards for those professionals within its jurisdiction.*

Glossary of Terms[1]

Circle of Care

The expression includes the individuals and activities related to the care and treatment of a client. Thus, it covers the health care providers who deliver care and services for the primary therapeutic benefit of the client. It also covers related activities such as laboratory work and professional or case consultation with other health care providers.

Confidentiality

Confidentiality is defined as the obligations of one person to preserve the secrecy of another's personal information.

Consent

Consent is voluntary agreement or authorization from a patient/client, or his/her legally authorized representative, to collect, use, retain, disclose, and retain his/her own personal health information.

Disclosure

Disclosure is the transfer or release of personal information to a third party.

Express Consent

Express consent means that verbal or written permission or authorization has been obtained from the patient for the collection, use or disclosure of his/her own personal health information. Express consent is indisputable.

Health Organization

A health organization is any organization engaged in the planning, funding, management, manufacture, or delivery of health services and products.

Implied Consent

Implied consent is consent that can be reasonably inferred from the action (or inaction) of a patient who has been informed of his/her privacy rights.

Knowledge

Knowledge is achieved when the individual is informed about what information is being collected about them, the purpose of that information collection, and how the information will be used, retained, disclosed and retained.

Personal Information

Personal information includes any factual or subjective information, recorded or not, about a particular individual that makes that individual identifiable.

Primary Purpose

Primary purpose means the collection, use and disclosure of information for the purpose(s) for which it was collected, for example; the provision of care and treatment of the client.

Privacy

Privacy is the right of individuals to be left alone, and to determine when, how, and to what extent they share information about themselves with others.

[1] Government of Canada, Industry Canada: PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector. Feb 24, 2013 http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00223.html

Reasonable Person

The concept of "reasonable person" is intended to ensure that personal information is only collected, used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances. The reasonable person test is contextual and objective.

Research

Research is defined as a class of activities that have as their purpose the creation of, or contribution to, generalizable scientific knowledge, based on theories and principles that can be corroborated by commonly accepted scientific methods of observation, inference and/or experiment.

Retention

Retention refers to the process of conserving data or information in a secure or intact manner, usually for a defined period of time, after which it may be destroyed.

Review

A review is defined as a series of activities whose primary purpose is to provide a retrospective assessment or analysis to assist in making judgements about the appropriateness, safety, quality, effectiveness, and efficiency of care and treatment.

Secondary Purpose

Secondary purpose refers to the use of information for a purpose other than that for which it was originally collected.

Security

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

Third Party

Third party refers to any individual or organization that is not the client, the original collector/provider of information, or the organization where a client is directly seeking care/treatment/services.

Introduction

Health professionals have an ethical and legal obligation to protect the patient's right to privacy and confidentiality of personal health information. Privacy information in Newfoundland and Labrador (NL) is guided by legislation. The *Access to Information and Protection of Privacy Act* (ATIPPA) is provincial legislation guiding public sector privacy law.[2] The *Personal Information Protection and Electronic Documents Act* (PIPEDA), is the federal law governing privacy in the private sector.[3] Health professionals in the province of Newfoundland and Labrador (NL) are bound to both by the provisions of the *Personal Health Information Act (2011)* (PHIA). PHIA is the provincial law that governs the collection, use of and disclosure of personal health information by individuals and organizations, also known as custodians, involved in the delivery of health care services. The law is intended to ensure that personal health information is kept confidential and secure while allowing for effective delivery of health care services in the province. Effective January 1, 2105 all registrants of the NLCHP must complete mandatory education on PHIA.

In addition to legislation in Newfoundland and Labrador (PHIA) the *Personal Information Protection and Electronics Documents Act* (2011, Canada) (PIPEDA) is the Canadian law related to data privacy and governs how private sector organizations collect, use and disclose personal information. The law gives individuals the right to access and request correction of the private information that an organization has collected. PIPEDA sets out the operational principles for consideration with respect to privacy of personal information and when read in combination with PHIA provides a backdrop for understanding privacy and confidentially in its fullest context.

Within the context of privacy and confidentiality there are many components (legislative compliance, consent considerations, security of information, and appropriate release of information etc.) that are important to clients and have implications for the health professional and employers of health professionals. The NLCHP has collaborated with the designated health profession Colleges to develop resources to include common standards, policies, guidelines and position statements in the area of privacy and confidentiality.

[2] Government of Newfoundland and Labrador: *Access to Information and Protection of Privacy Act* (2002, NL) http://assembly.nl.ca/Legislation/sr/statutes/a01-1.htm

[3] Government of Canada: Personal Information Protection and Electronic Documents Act (2011, Canada) https://www.priv.gc.ca/leg_c/r_o_p_e.asp

Definitions of Personal Information

When considering the issues of privacy and confidentiality individuals need to understand what is and is not considered personal information. Listed below are definitions contained within the laws of Canada and the laws of the province of Newfoundland and Labrador. The PIPEDA (2011 Canada) legislation defines "….Personal health information, with respect to an individual, whether **living or deceased**, means:

Section 2:

(*a*) information concerning the physical or mental health of the individual;

(*b*) information concerning any health service provided to the individual (including payment for services);

(*c*) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(*d*) information that is collected in the course of providing health services to the individual; or

(*e*) information that is collected incidentally to the provision of health services to the individual…"

Legislation in Newfoundland and Labrador defines personal information "… as **recorded** information about an identifiable individual, including

(i) the individual's name, address or telephone number,

(ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

(iii) the individual's age, sex, sexual orientation, marital status or family status,

(iv) an identifying number, symbol or other particular assigned to the individual,

(v) the individual's fingerprints, blood type or inheritable characteristics,

(vi) information about the individual's health care status or history, including a physical or mental disability,

(vii) information about the individual's educational, financial, criminal or employment status or history,

(viii) the opinions of a person about the individual, and

(ix) the individual's personal views or opinions, except where they are about someone else…"

Taken together these definitions are very explicit about what is considered personal information about an individual (whether living or deceased) and information that must be kept confidential and only released with the consent of the individual or their designated substitute decision maker.

Privacy is not an absolute right. In certain situations it may not be desirable, practical or even possible to maintain confidentiality of an individual's information. As well there may be legislation that requires disclosure of information to authorities i.e. in the case of child or elder abuse. It should be understood that, non-identifiable information that is not specific to an individual, including information on diseases, treatment and services can be made available to the general public. In releasing non-identifiable information health professionals must always consider that although the information qualifies as non-identifiable information, where there is any question about the ability to potentially link the information to an individual the health professional must always err on the side of non-release. Health Professionals must always be aware of employer policies and seek direction from the employer and or alternatively the health professional may contact the Office of the Privacy commission (NL) to determine if the information is personal information and subject to non-release.

Health professionals often work in teams and/ or are consulted to provide advice regarding client care and services. Consultation among health professionals is a complex process, often based on informal communication conducted in good faith with the aim of providing the most appropriate service for a client. However, the use of personal identifiable information must be guided at all times by professionalism and respect for the patient. Although legislation offers protection of privacy, personal health information **can, and should** be shared among health providers within the "circle of care" in order to provide appropriate, coordinated care and services to the client.

Employees in large organizations and health professionals in private or small group practices all share the same responsibilities for adhering to privacy legislation, Standards of Practice, best practice guidelines, policies, and process.

The Office of the Privacy Commission of Canada (OPC) outlines ten (10) **Guiding Principles** identifying the legal and ethical obligations of health professionals with respect to privacy and confidentiality of personal health information. Using these guidelines, an individual shall be able to address a challenge concerning compliance with privacy legislation when addressed to the designated individual or individuals accountable for the organization's privacy compliance.

These principles, often referred to a "fair information principles" may be viewed in full on the OPC website and are included in PIPEDA:
https://www.priv.gc.ca/leg_c/r_o_p_e.asp

Principle 1 – Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals (custodian) who are accountable for the organization's compliance with the following principles.

Principle 2 – Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 – Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Principle 6 – Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 – Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9 – Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 – Challenging Compliance

A client shall be able to address a challenge concerning compliance of the custodian, with the privacy standards.

(PIPEDA) Guiding Principles and Operational Guidelines

The NLCHP and the Colleges use the PIPEDA Guiding principles to develop a common set of operational guidelines that outline the expectations of health professionals with respect to privacy and confidentially of personal information

Principle 1: Accountability

Health professionals in NL are individually responsible for personal health information within their practice and are jointly responsible with the custodian (as defined under the PHIA legislation) for ensuring compliance with PHIA. Accountability for the security of the record even though other individuals within the work setting may be responsible for the day-to-day collection and processing of personal health information is the ultimate responsibility of the custodian. This accountability includes ensuring that there are appropriate policies and procedures in place that provide direction for staff and that staff are educated in these policies and procedures.

Operational Guidelines

1.1 Policies and procedures set by the employer (or the health professional if they are the custodian) must reflect the direct accountability of the health professional and employer to the client.

1.2 The health professional:

- is accountable for the security of all personal identifiable information for which they have responsibility;
- must ensure that only authorized individuals (other health professional, clerical staff etc.) have access to personal identifiable information and only as necessary to fulfill authorized purposes;
- must inform anyone with access to personal identifiable information of their responsibility to protect personal identifiable information. They must agree to accept those responsibilities (preferably in a written format i.e. oath of confidentiality) and recognize that failing to protect confidentiality may result is an allegation and investigation of breech of privacy by the NLCHP;

investigation and potential charges being laid by the employer and /or being subject to an investigation by the Office of the Information and Privacy Commissioner.

1.3 The custodian must have the autonomy, authority and resources necessary to ensure adherence to these Standards.

1.4 The custodian will ensure that policies, procedures and practices that give effect to these Standards, including those that:

- protect the security of personal identifiable information;
- receive and respond to inquiries and complaints;
- ensure that persons who collect, use or disclose personal identifiable information in the work setting are held accountable to the custodian , and
- ensure that individuals are adequately informed about the collection of their personal identifiable information, and that their informed consent is sought and obtained prior to the collection of any personal identifiable information.

Principle 2: Identifying Purpose

Clients are entitled to know the purposes for which personal health information is being collected, at or before the time the information is collected. The client is also entitled to know the potential uses of this information and who may be expected to have access to it. The health professional has a duty to inform the client of the anticipated use (other than internal) or disclosure of personal health information collected.

Operational Guidelines

2.1 Personal identifiable information must only be used for the purposes identified to the individual at or before the time it is confided or collected.

2.2 The health professional must ensure individuals are provided information about the uses to which their personal data will be applied. This includes:

- the information disclosed will become part of their electronic record;
- the reasonably foreseeable purposes for secondary use;
- other individuals, groups or organizations who may have access to, collect, use or disclose information as it pertains to the primary purpose (for example provision of personal information as a condition of an agreement the patient may have made with a third party insurer).

2.3 In health care, personal information is also collected for the prevention, treatment or management of symptoms of disease. Personal information may be collected for reasons other than direct individual care, including:

- public health;
- resource planning;
- quality assurance;

- research, and
- legal requirements

Principle 3: Consent

The health professional can only use or disclose personal health information with the consent of the patient, unless consent is exempted by law. Consent can be either explicit (written and or verbal), or inferred if the health professional has had discussion with the client and has fulfilled the duty to inform the client and has sufficient reason to believe that the patient would consent under the circumstances. Health professionals can disclose personal information without the consent of the client in the following circumstances:

-in order to prevent harm to the client or others;

-is in the patient's best interest (where lawful authority exists);

or for any other purpose such as research where the research has been approved by the NL Health Research Ethics Authority which is established under the *Health Research Authority Act (2011)*

Operational Guidelines

3.1 Informed consent of the individual is required for the collection, use, or disclosure of personal identifiable information, except where required by law.

3.2 Consent or choice as to who has access to one's personal identifiable information is a fundamental component of privacy. To be meaningful, consent must be informed, voluntary, and not obtained through misrepresentation or fraud. The individual must be competent to understand what their consent entails. A statement in clear and simple language about how the information will be used or disclosed is required to obtain informed consent.

3.3 Other than for primary or previously identified secondary use of information, written consent from the client should be obtained for the disclosure of personal identifiable information. At a minimum, the health professional should be satisfied that the client has expressly permitted the disclosure and this should be documented in the client file.

3.4 In emergency care situations consent for the collection, use or disclosure of personal identifiable information may be implied. The implied consent must be consistent with legislation governing emergency care.

3.5 There may be other situations where an individual may be unable to give informed consent, and these situations are governed by law i.e. consent via the clients substitute decision maker.

3.6 Implied consent does not deprive the individual of the right to refuse consent or subsequently challenge the health professional's assumption of implied consent.

3.7 The client may revoke consent at any time but such revocation cannot be retroactive.

3.8 Consent or revocation can be given verbally or in writing. When consent or revocation is given verbally, the health professional must document that direction

Principle 4: Limited Collection

The health professional may collect personal health information only for the purposes of providing care/services, or as required by law. Information shall be collected by fair and lawful means.

Operational Guidelines

4.1 The primary purpose of the collection of personal identifiable information is to benefit the client who permits information to be collected. Collection for legitimate secondary use of information shall be restricted to what is necessary and shall not impede the giving or collection of information for the primary purpose.

4.2 Collection of personal identifiable information for the primary purpose may be as extensive as necessary.

4.3 Collection of personal identifiable information for secondary purposes shall be as minimal as necessary, in recognition of the need to protect the individual's right to privacy.

4.4 Collection of personal identifiable information without individual consent shall only occur in circumstances where required by law i.e. mandatory infection disease reporting, or when ordered by a court of law.

4.5 Personal identifiable information shall not be collected by means that are unlawful, unfair or exploit the client's vulnerability. Nor shall any of the client's beliefs or potentially false expectations about subsequent collection, use, disclosure or access be exploited.

4.6 If a fax machine, or other electronic equipment, is used by the health professional to receive and or send any type of personal identifiable information, the fax machine, or other electronic equipment, should be physically located in a non-public area and access to the equipment must be restricted to authorized persons only.

Principle 5: Limiting Use, Disclosure and Retention

The health professional shall not use or disclose personal health information for purposes other than those for which it was collected, except with the consent of the individual or as required by law. The health professional may disclose personal health information only to those who have a legitimate need for that information. Where others individuals have legitimate access (within the "circle of care") have access to personal health information collected and stored by the health professional the health professional shall ensure that policies or formal agreements exist to ensure that the individual respect the patient's right to confidentiality. All individuals should be required to sign a confidentiality declaration (see Resources-Section B for template, pp. 26). Personal health information shall be retained for as long as necessary for the fulfillment of the purposes for which it was collected, or as required by law. In any case, personal health information collected by the health professional (see Resources-Section B - Client File Management, pp. 27).

Operational Guidelines

5.1 The primary purpose for the use, disclosure, and retention of personal identifiable information is to benefit the individual client who permits information to be collected. Use and disclosure for legitimate purposes shall be restricted to what is necessary and shall not impede the giving or collection of information for the primary purpose.

5.2 Examples of situations in which a health professional may be required by law to disclose personal identifiable information include but are not limited to:

- the health professional is presented with a warrant by a police officer;
- the health professional is served with a subpoena which requires delivery of documents containing client records;
- release of information is required by rules of court that relate to production of information in a lawsuit;
- an inspector or investigator authorized under the Health Professions Act (2010) section 22 (b) Quality Assurance to have access to the records makes a request to access the records;

5.3 Health professionals must use caution and professional discretion when:

- police or other law enforcement agencies or officials request the information, pursuant to regulation, and the health professional; deems it to be in the best interest of the patient or public to provide such information;
- information is requested by third party payers. Generally, third party payer's rights to personal health information are governed by the agreements they have with the client. Health professionals should refer to those agreements and have client consent to provide such information. Steps should be taken to ensure that the person requesting the information legitimately represents the third party payer and only the information authorized by the client should be disclosed;
- information is requested by family members or other agents. The health professional must confirm with the client their consent to the release of personal health information to that family member or other agent;
- information is requested concerning a deceased client. The executor of the estate is entitled to ask for personal health information. The health professional must confirm that the executor has legal authority to handle the deceased patient's affairs before personal health information can be released ie deceased clients legal will etc.;
- information is requested by the parent of a minor. Confidentiality is owed to all clients regardless of age. In the case of a mature minor, the consent of the child should be obtained prior to the release of personal health information.

5.4 Custodians and their employees who use information systems that link several databases must implement systems of control over appropriate access or disclosure.

5.5 The health profession must take appropriate measures to ensure that personal identifiable information is not seen or overheard by other individuals who may be in the work setting.

5.6 Client communication should take place in an area where discussion cannot be overheard by others. An appropriate area should be established for consultation purposes which provides either a private consulting room, or a semi-private area with suitable traffic/noise barriers.

5.7 The health profession must ensure patient confidentiality when disposing of files, computer records, labels or receipts, patient scheduling sheets, and any other manner of form that contains personal identifiable information.

Principle 6: Accuracy

Before using or disclosing personal health information, the health professional must take reasonable steps to ensure that the information is accurate, complete, and not misleading. Personal health information shall be as accurate as possible, and up to date as is necessary for the purposes for which it is to be used.

Operational Guidelines

6.1 The accuracy and integrity of personal identifiable information are necessary to support the client's right to privacy and to meet the requirements for its collection, use, or disclosure.

6.2 The health professional is responsible for the accurate recording of information.

6.3 Where a client believes there is an error or omission in his or her personal record, an amendment may be made. The requested amendment shall be made by adding it to the record in such a manner that it will be read with and form a part of the record, or be adequately cross-referenced.

6.4 When the accuracy of information is in dispute, it shall be clearly marked in the original record.

6.5 The health professional must protect the integrity of the personal health information in their custody and have assurance that the integrity of information received from, or passed onto, other individuals in the "circle of care" or organizations such as third party payer has been, and will continue to be, similarly safeguarded.

Principle 7: Safeguards

The health professional shall protect personal health information from accidental or malicious disclosure, interruption, modification, removal or destruction. The custodian must establish policies governing the retention, security and destruction of personal health information to maintain client privacy and confidentiality. Heath professionals must be aware of educated and adhere to the policies of the employer/organization.

Operational Guidelines

7.1 Personal identifiable information shall be protected by security safeguards appropriate to the information, and against unintended or unauthorized access, use or intrusion, or such dangers as accidental loss or destruction.

7.2 The custodian shall establish policies and procedures to protect data integrity:
- physically, (e.g. locked doors and locked cabinets);
- technically, (e.g. passwords and security codes); and
- organizationally, (e.g. education and policies on access).

7.3 Security safeguards shall be established to protect all personal identifiable information that will not unreasonably impede the collection, use, or disclosure of information by authorized persons.

7.4 Persons authorized to access information must be informed of the authority, parameters, purposes and responsibilities of their access, and the consequences of failing to fulfill their responsibilities.

7.5 Access to information shall be limited to only that information which is required for the authorized purpose.

Principle 8: Openness

The custodian/organization or health professional shall make readily available to individuals specific information about the policies, procedures and practices relating to the management of personal health information. Individuals must be able to clearly understand the extent and circumstances of the collection, use and disclosure of their personal health information.

Operational Guidelines

8.1 An organization/custodian, or health professional must make information on its policies and practices relating to the management of personal identifiable information available upon request. Methods may include, but are not limited to, brochures, mail, electronic and print media, online access or a telephone number.

8.2 Clients shall be able to discuss the organizations/health professional's policies, procedures and practices concerning their personal identifiable information with a knowledgeable person.

Principle 9: Individual Access

Clients have a right of access to their personal health information. Upon request, a client shall be informed of the existence, use, and disclosure of his or her personal health information and shall be given access to that information upon their inquiry. In rare and limited circumstances, withholding personal health information from a client is permissible if disclosure may have a significant likelihood of substantial adverse effect on the physical, mental or emotional health of the client or a third party. The

onus lies on the custodian/health professional to justify to the client a denial of access. A client shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Operational Guidelines

9.1 Clients have a right to access their personal identifiable information and to obtain a copy of that information. The custodian may charge a reasonable fee for providing a copy of the record (PHIA section 57) A custodian shall respond to the request within 60 days after receiving the request (PHIA section 55).

9.2 If an individual is denied access to their file for review and or for correction of information in the file that client has a right to make a formal complainant under section 65 of the PHIA.

9.3 Lawful agents (such as a legal guardian, substitute decision maker or the executor of an individual's estate) can exercise the rights of the individual.

Principle 10: Challenging Compliance

Clients, upon request, must be informed and understand that the organizations or health professional's policies, procedures and practices are open to scrutiny and challenge. A client shall be able to address a challenge concerning compliance with the above standards to the custodian for the client record.

Operational Guidelines

10.1 The custodian shall respond to all complaints about their compliance with PHIA and when necessary take appropriate measures, including amending its policies and procedures to improve compliance.

10.2 Complaints about compliance with PHIA which have not been handled to the satisfaction of the patient by the custodian may be made to the Office of the Information and Privacy Commissioner.

10.3 Complaints about compliance with these standards which have not been handled to the satisfaction of the client by the health care professional may be made to the Registrar of the NLCHP using the allegation process outlined on the web site www.nlchp.ca. .

Ownership of Information

In addition to the principles outlined above it is important for health professionals to clearly understand the nuances of who owns the information that is contained in a client file and who owns the clients file.

Individuals are the owners of any, and all personal identifiable information pertaining to them regardless of where it is held. Health related information about a client (personal health information) belongs to the client, but the electronic and paper records that carry this information are the property of the custodian whether that is an organization, or health professional. Such records include, but are not limited to client notes, patient profiles and reports, which contain certain information that identifies the client. The client has a right to review the information that is part of the file, ask that corrections be made to the file, and can ask for a copy of their file as identified in the principles of *Accuracy* and *Openness*. However, they cannot request that the personal information be deleted from an existing file. As identified under the principle *Safeguards,* the responsibility for maintaining security of the client record is the responsibility of the custodian and the health professional.

Where a health professional uses personal identifiable information to publish a professional study or article, the anonymity of patients involved must be protected. Copyright shall rest with the author because the basis of the study or article is the health professional interpretation, or assessment of a series of personal identifiable information and data of various clients.

In Newfoundland and Labrador we have additional legislation called the *Human Research Ethics Authority Act* (2011) which applies to all research conducted on human subjects. This act focuses on the review process and makes provision for the approval of research proposals on human subjects. Special consideration is placed on the issue of consent, research without consent and the obligations of researchers with respect to disclosure of information. For additional information this act please view the Health Research Ethics Authority website at www.hrea.ca [4]

[4] The Health Research and Ethics Authority, http://www.hrea.ca/About-Us.aspx

Resources

Section A:

Position Papers

NLCHP Position Statement: Social Media

Draft Guidelines- Closing a Practice, Re-locating and Referring Care

This section contains resources with additional direction for registrants and college members. These documents are approved by the NLCHP and approved and /or have been modified by the colleges. For college-approved documents, please visit the health profession college web sites.

NLCHP Position Statement:

Social Media

Approved: January 2015

The NLCHP recognizes the use of social media as an effective means of communication for health practitioners and their businesses, as well as a method for communicating health information. Networking with social media also provides a nominal platform for communicating and information sharing with health professional groups and colleagues.
Social media is a collection of Internet based programs (Facebook, You Tube, Twitter, LinkedIn and blogs, as well as chat rooms) used for information sharing. Transferring information through social media by any format (text, photos, audio, and video) is rapid and easily accessible. While the fluidity of social media may provide a communication advantage, there are important points to consider when choosing to communicate through social media that require attention and give caution to this approach of communication.
This position statement serves as an advisory for health professionals within the jurisdiction of the NLCHP who use social media in their personal and/or professional practice, but also for professionals as registrants of the NLCHP who may have questions around the use of social media.
The use of social media can encourage and facilitate a culture of collegial and professional respect among professionals, and provide a welcome resource for clients. However, users must appreciate the responsibility required to manage the personal and professional risks.

Privacy and Confidentiality

First and foremost the confidentiality of client and registrant information must be strictly maintained. No information that can identify an individual should be publically communicated through social media, and communicating health status information must be contained in a manner dictated by organizational or employer policy. Even posting information that may be perceived as non-identifiable is not exempt from this position as clients and their families can easily identify themselves.

Professionalism

All registered health professionals must continue to act according to professional and ethical standards while conducting any online activity. Registered health professionals are obligated to uphold public trust in their profession and are accountable to their actions. Any inappropriate use of social media may be considered **conduct deserving of sanction** where a breach of practice standards can be demonstrated.

Additionally as per professional ethics codes, all health professionals are required to respect professional boundaries. "Friend" requests from clients, friends or family can transition relationships from professional to more personal leaving the professional responsibility less defined and exposed to risk in terms of privacy, confidentiality and the sharing of information.

Guidelines to Consider

1. Do abide by organizational policies regarding the professional and personal use of social media. Employers and professional regulatory bodies have strict policies on professional conduct and will reprimand individuals who breach conduct policy.

2. Be judicious. Elect to use the strictest privacy settings on social media sites but remember nothing is private. Do not post anything on a social media site you would not want viewed by prospective clients, business associates, employers or regulators. Derogatory comments, inappropriate photos, foul language and crude jokes can be viewed as a reflection of character, and by extension your profession.
3. Be prepared. Check your profile regularly to view what others may post on your pages and remove what may be considered inappropriate. Use search engines to find where your name may be associated on other sites and check to have it removed if it could be detrimental to your professional or personal reputation.

4. The NLCHP does not monitor personal pages on social media sites but information found on these sites can be used in an investigation of a complaint against a health professional registered with the NLCHP.

5. Offering health related information or recommendation is subject to the same verification as that given in a professional environment and if inaccurate, false or misleading could be grounds for a professional liability claim.

6. Posting information anonymously or under a pseudonym will not protect against possible consequences of breaching of confidentiality or defamation.

7. Be aware of the risks associated with email and electronic communication with clients; interception by friends or family members, misdirection to a similar address, altered diagnostic or treatment reports and loss of important electronic information. Just an email header with a clinic name can offer a certain amount of information to friends or family when the email platform is open and the inbox subject line is revealed.

8. Registered health professionals as custodians of personal information must implement privacy safeguards and policy and should, where possible limit the amount of health information transferred electronically and by email.

9. Professional boundaries must be respected. In cases where a client may make a request for information or services through a professionally designated social media website, efforts should be taken to ensure that the relationship is strictly professional. If a client continues contact but for more personal or social responses then they should be informed that the website is for professional contact and information only.

Resources

Association of Registered Nurses of Newfoundland and Labrador (ARNNL): Social Media Position Statement, April 2013
http://www.arnnl.ca/documents/publications/Position_Statement_on_Social_Media_2013.pdf

College of Registered Nurses of Nova Scotia (CRNNS): Position Statement, Social Media, 2013
http://www.arnnl.ca/documents/publications/Position_Statement_on_Social_Media_2013.pdf

College of Medical Laboratory Technologists of Alberta (CMLTA): Social Media Practice Advisory Statement
http://cmlta.org/wp-content/uploads/2013/03/Social-Media-March2013.pdf

College of Registered Dental Hygienists of Alberta (CDHRA): Communicating Through Social Media: A regulatory perspective. *In Touch*: July 2013, p 8-11.
http://www.crdha.ca/media/17100/in_touch_july_2013_final.pdf

DRAFT-Closing a practice, Re-locating and Referring Care

Date: March 2015

There are any number of occasions when a health professional may find reason to discontinue their practice, or deem it necessary to refer client care. In most instances the transfer of care can be done quite effectively and with sufficient notice for clients to resume care and make other arrangements. However in all cases the referral must follow a process that protects clients' personal information and their health. In circumstances where a practice is closing, and/or client files are moved, health professionals as custodians of personal and health information are bound by legislation governing access to information and the protection of personal health information.[5] Health professionals are well advised to have firm policy and procedure on how clients and their files are managed in these instances so that there is no abandonment of treatment, or misdirection and loss of personal information.

Abandonment of care is described "when a {health practitioner} intentionally and unilaterally terminates an existing {practitioner} -client relationship when services are still indicated and when the withdrawal of services by the practitioner is not justified or has been done without reasonable notice."[6]

Processes to follow regarding the withdrawal of services can be written in the legislation or other governing documents such as Codes of Ethics and Standards of Practice. These will often describe the conditions for referring client care, and /or closing a practice. There are only a few conditions where a health professional may actually refuse services to a client and in some of these cases, reasonable notice is still required. Generally a health practitioner can withdraw care when:

1. A client refuses to follow treatment advice;
2. A client is abusive to, or harassing the practitioner; or
3. When a client refuses payment after sufficient and reasonable time is given to make payment of fees.

Other than these circumstances a practitioner may be seen as abandoning the client or the treatment when insufficient notice is given. Notice may be given verbally and/or in writing. Written notices in the form of a letter should be confirmed by registered mail with a copy of the letter entered into the client file (s) as well as the practitioner's administrative file.

Closing a Practice

If a health professional is closing their practice they must make an appropriate transition of care and/or storage of client files. A health practitioner may own client files and is custodian of all the information in the file, including the client's personal information. However, the client receiving care owns their personal information and is entitled to its access.[7] Therefore it is incumbent on the practitioner to ensure that proper notice is given to transfer care and the information if requested by the client, or a designated representative. In many cases there is also a requirement for the health professional to retain records for a period of time even after the

---

[5] Government of Newfoundland and Labrador (2011) *Personal Health Information Act* http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

[6] College of Chiropractors of British Columbia: Professional Conduct Handbook July 2009 http://www.bcchiro.com/bccc/documents/PCHJuly202009.pdf

[7] Government of Newfoundland and Labrador (2011) *Personal Health Information Act* http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm Section

information is transferred. It is not unusual to have a nominal fee associated with copying and forwarding client information at the request of the client or a named designate.

Where a practitioner is relocating or closing their practice, announcements may be published through local media, as well as letters written to each client. In some circumstances there maybe agreements between practitioners in a group practice to assume client care when one leaves or retires. These agreements must be clearly written and understood by clients, though clients are not obligated to the services offered in the same office by a different practitioner. It will be the client's choice if they choose to receive care.

Relocating or Storing Client Files

When a health practitioner has sold their practice or dies unexpectedly, client files may be relocated and notice must be given by public advertisement or personal letter. In cases where the practitioner has passed away, it is the executor of the estate who provides notification. Information would include that a copy or the original file may be transferred to another practitioner if requested, and that records shall be retained for a specified period of time.[8] In most cases there will be a timeline associated with transferring the records and a limited time by which a client may request the file or the information from the custodian or designated custodian.
The matter of relocating and appropriately storing personal health information is an essential responsibility of the health practitioner. The College of Chiropractors of British Columbia stipulates in its practitioner handbook that not declaring the proper storage and making provisions for client information when closing or relocating a practice can jeopardize professional standing in the College if inappropriately managed.

Guidelines

1. A plan for client files and personal information is a component of professional behaviour that protects client care and personal information.

2. There are only a few occasions where a health professional can refuse to treat a client, otherwise discontinuing client treatment or care without sufficient notice could be interpreted that care was abandoned.

3. If a health professional is closing or relocating their practice, reasonable notice must be given by public announcement and/or personal letter. Written notices should be forwarded and confirmed by registered mail.

4. In the event that a practitioner dies, the executor or representative must send out notice advising clients of how their files may be transferred and/or stored, as well as how clients or their appointed designate may access the file if necessary and for how long.

5. According to the *Personal Health Information Act* (PHIA, 2011, NL) a health professional owns a client file and is a custodian of the personal and health information but it is the client who owns the information.

6. When a request is made for a client file, it is recommended that a copy be made and forwarded on the client's behalf at their request. Copies and original files must be retained by custodian (designated custodians) for a period of time even after the transfer of care is made.[9]

[8] The Newfoundland and Labrador Dental Board Information for Licensees: Guidelines and Policy Statements: Protocol for Dental Records (2012) http://www.nldb.ca/info_licensees/info_licensees.aspx

[9] Government of Newfoundland and Labrador (2011) *Personal Health Information Act* http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm Section 15. (8)

7. The timeline for responding to a request of client files under varying circumstances is outlined in the *Personal Health Information Act,* NL 2011.

8. It should be noted that the *Access to Information and Protection of Privacy Act* (2002, NL) does not apply where the information requested is personal health information and the custodian is a public body (i.e. Regional Health Authority, School District) and the governing legislation is PHIA.[10]

References

Government of Newfoundland and Labrador (2011) *Personal Health Information Act*
http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

College of Chiropractors of British Columbia: Professional Conduct Handbook July 2009
http://www.bcchiro.com/bccc/documents/PCHJuly202009.pdf

The Newfoundland and Labrador Dental Board Information for Licensees: Guidelines and Policy Statements: Protocol for Dental Records (2012)
http://www.nldb.ca/info_licensees/info_licensees.aspx
Government of Newfoundland Labrador (2002) *Access to Information and Protection of Privacy Act*
http://assembly.nl.ca/Legislation/sr/statutes/a01-1.htm#5_1

Other Resources

College of Physicians and Surgeons of Newfoundland and Labrador (2010) Guideline-Physician's Responsibilities When Closing his or her Medical Practice for an Extended Period.
https://www.cpsnl.ca/default.asp?com=Policies&m=329&y=&id=13

Government of Ontario, *Optometry Act* (1991)
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_91o35_e.htm

Government of Nova Scotia *Dental Act* (1992) Regulation No. 3 –Code of Ethics
http://www.pdbns.ca/regulationno3.aspx

College of Traditional Chinese Medicine Practitioners and Acupuncturists of Newfoundland and Labrador Professional Misconduct Regulation and Rationale
http://www.ctcmpanl.ca/wp-content/uploads/2012/07/Misconduct-CTCMPA-NL.pdf

[10] Government of Newfoundland and Labrador (2002) *Access to Information and Protection of Privacy Act* http://assembly.nl.ca/Legislation/sr/statutes/a01-1.htm#5_1 Section 5.1

Section B

Policy Templates and other resource material

1. Privacy and Confidentiality **(Principle 1-Accountability)**
2. Client File Management **(Principle 5-Limiting Use, Disclosure, and Retention)**
3. Correction of Client File **(Principle 6- Accuracy)**
4. Communication: Personal Information Via Facsimile **(Principle 7- Safeguards)**
5. Maintaining Client Files **(Principle 7-Safeguards)**
6. Information brochures **(Principle 2- Identifying purpose, Principle 4-Limiting Collection, Principle 8 –Openness, Principle 9-Individual Access, and Principle 10-Challenging Compliance.)**
7. Privacy Compliance **(Principle 10—see Resources, Section C-Privacy Assessments Tools and Privacy Breach checklists)**

Policy **templates** have been developed and the content taken from College and/or NLCHP existing policies. The following are examples that can be adopted by registrants and/ or organizations for their workplace, if not already established. Each example carries with it, the associated "Guiding Principle" to which it may be matched for assessment or audit purposes.

1. Privacy and Confidentiality –**Principle 1-Accountability**

Health professionals and/ or organizations are encouraged to review their practices with respect to privacy, confidentially and consent considerations. In reviewing you or your organizations current practices it is important to specifically identify the roles and responsibilities and clearly document these for the health professional, organization and the client.

Title:	**Privacy and Confidentiality (Policy template)**
Approval by:	
Date:	
Policy:	Personal and personal health information collected shall be limited to that which is necessary to carry out treatment/services for clients. Information should be accurate and complete. Health professionals, and other individuals who are engaged in providing or supporting the provision of services/treatment for clients (including clerical support, housekeeping and other staff and contractors) must ensure that information that they become aware of as a result of their interaction with or supporting the health professional is kept private and confidential. Health professionals, and other individuals who are engaged in providing or supporting the provision of services/treatment for clients (including clerical support, housekeeping and other staff and contractors) must sign an oath of confidentiality.
Procedure:	**1**.The health practitioner identifies the purpose for which information is to be used prior to the request for personal or personal health information. The information collected shall be limited to that which is necessary for the identified purpose. **2.** Consent is required of the client for the collection, use or disclosure of personal information. The consent can be written, verbal or implied. If the consent is verbal or implied this must be documented in the client file. **3.** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. 4. Personal information shall be accurate, complete and up to date as is necessary for the purpose for which it is to be used. **5**. Clients may access their file. A client can challenge the accuracy and completeness of the information in their file and have it amended as appropriate. **6**. Health professionals, and other individuals who are engaged in providing or supporting the provision of services/treatment for clients (including clerical support, housekeeping and other staff and contractors)

must sign an oath of confidentiality. See Schedule A. For health professionals in solo practice the practitioner is encouraged to sign the oath as an affirmation of their understanding of their responsibility for the maintenance of privacy of client information.

References: *Personal Health Information Act***,** Newfoundland and Labrador (2011) http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

Policy History: **<include date of policy approval and any revisions/updates>**

Schedule A

Oath of Confidentiality

I, the undersigned understand that I may have access to or inadvertently become aware as a result of my employment personal information and or personal health information (called "information") related to the provision of client treatments and or services. I acknowledge that access to, use of as well as security of such information are my responsibility and such obligations are outlined in the NL Personal Health Information Act (2011) and PIPEDA (2011, Canada).

I further acknowledge that I will not share this information except as required in the course of my duties and or as required by law.

I confirm that I have read and understood the policy on Privacy and Confidentiality.

Name _____

Date: _____

Witness: _____

Date: _____

2. Client File Management **(Principle 5-Limiting Use, Disclosure, and Retention)**

Title:	**Client File Management**
Developed by:	NLCHP QA Committee
Approval:	
Date:	May 2015

Overview:

Documentation related to client treatment/services, including assessments, consent to treatments/services as well as treatment/service outcomes are integral to the provision of client care and are usually contained in a client file.

The recommended timelines for retaining client files depends on a number of factors including: legislative requirements; third party payer requirements; standards set by accrediting bodies; statute of limitations for bringing medical malpractice claims or other legal actions against a health care provider. Where there is no documented legal obligation and/or published practices, organizations generally develop guidelines and policies based upon these factors above. A search of legislative requirements including policies and guidelines in the Newfoundland and Labrador context does not identify definitive statements on timelines for retention of client health files. The documents state in a general sense, that the custodian is expected to maintain files for as long as is necessary to meet the identified purpose. [11]

[11] Newfoundland and Labrador Centre for Health Information (NLCHI):emailed response from NLCHI representative March 5, 2015; *Reference IM00072105*

The responsibility to ensure policies and processes are in place and adhered to with respect to access to information is the role of the custodian* as identified in the *Personal Health Information Act*, NL, 2011 (PHIA). [12]

*A "custodian" by the PHIA legislation includes a list of entities accountable to personal health information in their care. These include but are not limited to health professionals, and health care providers, regional health authorities, government departments when engaged in health care, the public health laboratory, the Newfoundland and Labrador Centre for Health Information (NLCHI), Workplace Health and Safety Compensation Commission (WHSCC), as well as local schools and the university.

For health professionals working in publicly funded health care organizations or other publically funded organizations (i.e. school board) the organization, not the health professional is considered the custodian for the client file. For health professionals employed in the private sector, the employer is most often the custodian unless the health professional has entered into an arrangement where the health professional employee is the custodian. For health professionals who are self-employed, the health professional is the custodian of the client files.

Under the *Access to Information and Privacy Protection Act* (ATIPPA) and PHIA, client files must be kept confidential and only accessed for use within the circle of care**. Client files must be stored appropriately to avoid access by non-authorized parties.

**The "circle of care" refers to those individuals and authorities who may be involved in the provision of health care.

[12] *Personal Health Information Act,* Newfoundland and Labrador, 2008

Guidelines

Custodians of client files must have policies including but not limited to:

- Security of client files contained in paper and electronic formats ;
- Access, retention, transfer and destruction of client health files.

Clients must be informed of the custodians' policies including but not limited to:

- Security and safekeeping of client health files;
- Why information is collected;
- Who has access to the client health file;
- How long client health files will be kept;
- How to request a copy of their client health file;
- How to request a correction be made to their health file;
- Processes and safeguards used when client health files are transferred and /or destroyed.

Unless otherwise directed by the Regional Health Authority, another publicly funded organization, or specified in legislation, the <College> recommends that client files must be maintained for the minimum timeframes:

- For clients over 21 years old, a period of 10 years after the last treatment/service;
- For clients less than 21 years old, a period of 10 years after the age of 21;
- For clients who are deceased, a minimum of 6 years after a death.

Client health files maintained in a paper format may be transferred to an electronic format. Where client files are maintained in an electronic format they must be backed up on regular basis. A backup must be maintained on an encrypted storage device.

Documentation regarding the scheduled destruction of a client file must be maintained by the custodian and /or designate.

Access to client files will be only by those individuals who are within the circle of care of that client.

Procedure:

1. The custodian, or designate must inform the client of the office/organizational policies regarding access to, disclosure, retention and destruction of client files. Documentation of the discussion should be included in the client file. <To be developed>.

2. The custodian and /or designate will ensure that files are appropriately stored and secured.

   2.1 Paper files must be stored in areas not accessible to the public, or unauthorized users, and locked when staff are not in the work area.

   2.2 Electronic files and computer work stations must be password protected and locked when staff are not at their work station. Electronic files must be backed up on a regular based using an encrypted storage device. The storage device must not be stored at the office location.

3. If client files are to be transferred to another custodian the client must be notified in writing to the last known address of the transfer, why the transfer is being conducted and the client must be provided the opportunity to have their file transferred to an alternate care provider.

4. If client files are destroyed, documentation including the name of the client file, the initial and last date recorded for client service/treatment and the date of destruction including the method of destruction must be maintained by the custodian.

5. If destruction of records is carried out by an outside contractor, the contractor must sign an oath of confidentiality and certify that the records have been destroyed properly and agree to indemnify the custodian if patient confidentiality rights are breached.

6. Unauthorized access to client files by individuals not within the circle of care must be disclosed to the client unless disclosure to the client is contraindicated (PHIA: Section 37).

References:

Access to Information and Privacy Protection Act **(Newfoundland and Labrador, 2002)**
http://assembly.nl.ca/Legislation/sr/statutes/a01-1.htm

Personal Health Information Act **(Newfoundland and Labrador, 2008)**
http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

Canadian Institute for Health Information (CIHI): *Privacy policy on the collection, use, disclosure and retention of personal health information and de-identified data*, 2010.

http://www.cihi.ca/CIHI-ext-portal/pdf/internet/PRIVACY_POLICY_201005_EN

Newfoundland and Labrador Center for Health Information (NLCHI); email with M. Butler, March 5, 2015 Ref. IM00072105

Policy History: Original

3. Correction of Client File **(Principle 6- Accuracy)**

Clients have a right to review their file and make correction of information contained in the file.

Title: **Correction of Client file (Policy template)**
Approved by:
Date:

Policy:

Clients may make a request orally or in writing to the custodian (or health professional) for a correction to be made to their client file.

The custodian will respond within 30 days after receiving the request.

The custodian shall grant the request if the client demonstrates to the satisfaction of the custodian that the record is inaccurate or incomplete for the purposes for which the information was collected.

The custodian of the records may refuse to accept the correction under the following circumstances:

- the record was created by an individual other than the custodian and the custodian does not have sufficient knowledge , expertise or authority to correct the file
- 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 client
- the custodian believes on reasonable grounds that the request is frivolous, vexatious or made in bad faith

Where a client has been refused correction of the information and is dissatisfied, the client may submit a formal complaint to the Office of the Privacy Commissioner Newfoundland and Labrador, and /or the Trials Division of the Newfoundland Supreme Court.

Procedure for correction of inaccurate information:

1. Correction is made by striking out the information but ensuring that the information is still available and able to be read. If correction of the information cannot be made in the file an alert system needs to be established so that authorized users of the information contained in the file are aware of and how to access additional information.

2. Inform the client once the correction has been made.

3. Provide written notice of the correction of the information to the extent reasonably possible to any person to whom the information has been disclosed to within the 12 months immediately preceding the request for correction.

4. Where the custodian refuses to grant the request for correction:

4.1 The custodian will highlight the area to be corrected and indicate in a referenced note what was requested for correction and the following correction as requested by the client was not made.

4.2 The custodian will provide written notice to the client that the request for correction was refused, why the correction was refused and that the client has a right to appeal the refusal and submit a formal complaint to the Office of the Privacy Commissioner Newfoundland and Labrador, and /or the Trial Division of the Supreme Court of Newfoundland and Labrador.

References: *Personal Health Information Act* (Part V, Section 58-64; Part VII Section 83-86)

Supreme Court of Newfoundland and Labrador, Trial Division
http://www.court.nl.ca/supreme/general/Contact.html

Policy History: **<Include date of policy and any policy updates>**

4. Communication: Personal Information Via Facsimile **(Principle 7- Safeguards)**

Title: **Communication: Personal Information Via Facsimile (Policy template)**
Approved by:
Date:

Policy Overview: All means of communication, including the use of facsimile (fax) carry some level of risk. However, <**organization or health professional** > must take measures to ensure that established methods and guidelines are undertaken to protect the privacy and confidentiality of client personal and personal health information.

It is recognized that efficient and fluid communication is essential to the provision of quality care/service for clients, and that information that is forwarded requires appropriate security protocols.

Policy: Facsimile transmission should only be used where other more secure methods are not available and limited to necessary information for the purpose for which it is transferred.

When faxing personal or personal health information, it must be done in a manner that is safe and secure.

Sending Faxes

1. Where possible, contact the intended recipient for the faxed information to ensure that the information will be received securely.
2. Include a completed fax cover sheet with the name, address and phone number of the sender, and the name, address and phone number of the party receiving the faxed information. Also include the number of pages being transmitted and a notice that information contained in the fax is confidential.
3. Reconfirm the accuracy of the fax number before the number dialed.
4. Fax/copiers where possible, should be set up to deliver confirmation that a fax has been transmitted.
5. Retain a record of fax transmissions or confirmation sheet for a minimum of one month.

Receiving Faxes

1. When an expected fax fails to arrive, contact the originator immediately to advise that the fax was not received.
2. **<An individual should be designated to account for faxed information received and distribution to the correct individual and or client file.>**
3. If faxed information is received in error or is unclear, the sender where possible is contacted to acknowledge the received information and the information returned.
4. If the correct recipient cannot be determined, the faxed information is properly and securely destroyed.

5. Faxes with personal information must be securely filed with the clients file. If the fax is stored electronically, policy and procedures for records management must be followed

References:

Policy History:

5. Maintaining Client Files **(Principle 7-Safeguards)**

Title: **Maintaining Client files (Policy template)**
Approved by:
Date:
Policy: Clients or authorized agents can review their client files upon request unless it is deemed by the health professional that disclosure may have a significant likelihood of a substantial adverse effect on the physical, mental or emotional health of the client and or third party. Access must be provided within 60 days after the request.

No original document can be removed from a client file. Copies of the file may be made available to the client or authorized agent at cost.

Upon a client's death or termination services the file remains the property of the health professional and or custodian.

Measures are taken to protect personal and personal health information taken in confidence and restrict its use for which it was collected.

Responsibilities: It is the responsibility of the health professional and custodian to:

- Ensure that only one file exists for each client;
- Designate the location in which files (paper and electronic is required) will be held;
- Ensure that clients are aware of how files are maintained and secured;
- Ensure that client files are kept up to date;
- Ensure that clients have reasonable access to view their client file;

It is the responsibility of the client to:

- Ensure that all relevant information including contact information, next of kin as well as information for insurance purposes is up-to-date.

References: *Personal Health Information Act* (2011), NL
Access to Information and Protection of Privacy (2002), NL

Policy History:

To be developed: File Security: paper and electronic* **Principle 7-Safeguards**

6. Information for Clients (**Principle 2 –Identifying Purpose, Principle 4-Limiting Collection, Principle 8-Openness, Principle 9-Individual Access, and Principle 10-Challenging Compliance.**)

Ensuring that clients understand why the health professional collects health information and for how long the information is maintained. The following posters are available and can be printed for posting in the workplace and outline the responsibilities of the health profession and the client with respect to privacy and confidentiality. Additionally there are brochures that can be provided directly to clients regarding the Personal Health Information Act (NL) and the security measures maintained by the health professional to ensure that client files in there are maintained and secured.

We need to develop and additional public brochure with specifics to be communicated… on file retention, how to request your file, how to make correction for the file and who to make a complaint with…

- Poster for custodians (3.3 MB) **(Principle 2-Identifying Purpose, Principle 8- Openness)**
- Poster for general public (2.2 MB)
- Informational brochure (11 MB)

Section C:

Self-Assessment Tools

Privacy Assessment Checklist
Privacy Breach Checklist

Section C of the resource manual provide a number of self-assessment tools that can be utilized by health professionals to assess their compliance with the standards as set by the college.

1. Privacy Self-Assessment Tools

Health professionals due to the nature of their work have access to and collect client personal information. Health professionals also have a responsibility to ensure that the information collected is accurate, is kept confidential and is only shared within the circle of care. The PHIA outlines the role and responsibility of custodian. The custodian is the person within an organization, or if a health professional is self-employed the health professional themselves, who is responsible for:

1. ensuring compliance with the PHIA
2. for designating an individual within the organization to be responsible to ensure that the organization meets its obligations under the PHIA
3. ensuring that staff and contractors are aware of their duty to maintain privacy and confidentially
4. implementing policies /procedures for the collection, use, storage, transfer, copying, destruction and modification of client personal information
5. implementing procedures for responding to requests for information and or correction of personal information

Ensuring compliance with maintaining privacy and confidentiality of personal information is responsible and effective risk management. Self-assessment is often an effective way to identify if an organization or a health professional's practice is compliant with the standards for their profession and legislation within the province. Completion of a self-assessment tool can often identify for the health professional, issues of non-compliance and as a result of early identification the health professional and/ or the organization can develop a plan of action to address the identified issue.

In completing self-assessment tools compliance should be based on the evidence to support the criteria, such as formal policy and guidelines, evidence of education, knowledge on the policies and guidelines, and evidence of security of files etc. In order to complete the self-assessment the health professional must have familiarity with the policies, practices and guidelines that are available within their organization and workplace.

Given that a health professional may be the custodian for client files (i.e. is self-employed) or is the designate named by the employer, two (2) categories of assessments are established. One for all health professionals, and one for health professionals who are also the designated custodian in their organization. Please note that there are two (2) categories of assessments, but within each section for custodian or health professional, there is also a section designed to highlight the *resource* for each assessment statement, as well as the associated checklist that may be used to identify compliance.

The checklist asks the health professional to indicate if they are in compliance with the principles of privacy and to support the response by identifying the evidence (i.e. policy/guideline/practice etc.). If the health professional indicates non-compliance ("not met") they must develop an action plan to address the identified issue. The resource section of this manual contains additional information including draft templates, guidelines, and brochures based on the privacy principles and can be used by the health professional as a resource to address any deficiencies.

Example:

Checklist for <u>Principle 1-Accountability</u>	**Compliance**		**Evidence(policy, guideline, position statement, etc)**
Example:	Met	Not Met	
Assessment Statement (as below): **"You have clearly delineated who, within your organization is responsible for privacy governance and management."**	✓		*[Registrant] Organizational* Policy # 001, date
Assessment Statement (as below): **"Your policy and guidelines address the principle of limiting use, disclosure and retention of personal information."**		✓	

Privacy Assessment Resource- Custodian

CHECKLIST PRINIPLE 1-ACCOUNTABILITY	Resource
Assessment	
You have clearly delineated who, within your organization, is responsible for privacy governance and management.	**NLCHP Privacy Document.** pp 10; 1.1-1.4 **PHIA**: Part II, Section 18
You have directed staff through policy, procedure or training to provide the name, address and phone number of the **Privacy** contact person to clients when requested.	**NLCHP Privacy Document.** pp 11; 1.4; **PHIA**: Part II, Section 18
You have verified that third parties have implemented the privacy controls stated in any **contractual/consent** agreements.	**PHIA:** Section 32-35
Your **policy and guidelines** address the principle of "identifying purpose" regarding personal information.	**PHIA:** Section 33 **NLCHP Privacy Document.** pp. 11
Your **policy and guidelines** address the principle of "consent" regarding personal information.	**NLCHP Privacy Document.** pp. 12; **PHIA**: Part III
Your **policy and guidelines** address the principle of "limiting collection" of personal information.	**NLCHP Privacy Document.** pp. 13
Your **policy and guidelines** address the principle of "limiting use, disclosure and retention" of personal information.	**NLCHP Privacy Document.** pp. 13-14 Policy Template: Client File Management; pp. 25-31
Your **policy and guidelines** address the principle of "accuracy" regarding personal information.	**NLCHP Privacy Document.** pp 15**;** Policy Template: Correction of Client File. pp. 32 **PHIA:** Part V; Section 60
Your **policy and guidelines** address the principle of "safeguards" with respect to personal information.	**NLCHP Privacy Document.** pp. 15-16; Policy Template:
Your **policy and guidelines** address the principle of "openness" regarding personal information.	**NLCHP Privacy Document. pp. 16;**
Your **policy and guidelines** address the principle of "individual access" regarding personal information.	**PHIA: Part V ; Section 52-54** **NLCHP Privacy Document**
Your **policy and guidelines** address the principle of "challenging compliance" regarding personal information.	**PHIA**: Part VI; **NLCHP Privacy Document**
You have trained **staff/members** regarding the protection of personal information by informing them of organizational privacy policies, procedures and best practices.	**NLCHP Privacy Document;** pp. 22-24; 28-32
You have developed documentation to explain your personal information protection policies and procedures to customers and the general public.	**NLCHP Privacy Document.** pp. 38

CHECKLIST FOR PRINCIPLE 2 - IDENTIFYING PURPOSE	Resource
Assessment	
You have documented your purpose(s) for collecting personal information.	**NLCHP Privacy Document.** pp.11**; PHIA:** Part IV, Section 29-50
You seek the consent of clients and customers before using information for any new purpose if required.	**NLCHP Privacy Document.** pp. 12**; PHIA:** Part III

CHECKLIST FOR PRINCIPLE 3 – CONSENT	Resource
Assessment	
You obtain customer consent for any collection, use or disclosure of personal information.	
If you don't obtain customer consent for the collection, use and disclosure of personal information, you have determined that it is not required under (**s.37 of PHIA).**	
You allow a client or customer to withdraw consent at any time subject to legal or contractual restrictions and reasonable notice.	

CHECKLIST FOR PRINCIPLE 4 - LIMITING COLLECTION	Resource
Assessment	
You limit the amount and type of personal information you collect to what is necessary for the identified purpose.	

CHECKLIST 5 - FOR LIMITING USE, DISCLOSURE, AND RETENTION	Resource
Assessment	
You only retain personal information as long as necessary to allow for the fulfillment of identified purposes.	
You have policies/guideline regarding the destruction of personal information, including the role of contractors performing such services.	

CHECKLIST FOR PRINCIPLES 6- ACCURACY	Resource
Assessment	
Your policies/guidelines address the accuracy, completeness and currency of personal information which includes a process through which individuals can challenge the accuracy of information.	
You record when and where key information was collected, including dates of corrections or updates to such information.	

CHECKLIST FOR PRINCIPLES 7- SAFEGUARDS	Resource
Assessment	
You have adopted physical, technical and administrative safeguards to protect personal information against loss or theft as well as unauthorized access, disclosure, copying, use or modification.	
You have implemented processes to prevent unauthorized access to personal information during the disposal or destruction of information.	
You have established an information security breach policy and commit to investigating the root-cause of such breaches.	
You have developed and implemented policies and practices including appropriate safeguards for all uses of personal information outside the office.	

CHECKLIST FOR PRINCIPLES 8- OPENNESS	Resource
Assessment	
You explain to customers why you collect, how you use and when you will disclose their personal information.	
You describe to your clients how they can obtain access to or correct their personal information.	

CHECKLIST FOR PRINCIPLE 9- INDIVIDUAL ACCESS	Resource
Assessment	
You have advised staff of the need to direct requests for access to information to the staff member responsible for processing these requests.	
You limit refusal to provide access to information to exceptions described in **Section 58 of (PHIA).**	
You respond to a request for information in not more than 30 days unless you notify the requestor within that time period of your need to extend the time limit for response, indicate the extended time limit and inform the requester of his or her right to complain to the **OPC-NL**.	
You allow individuals to challenge the accuracy of personal information and amend information when an individual demonstrates that information is inaccurate or incomplete.	

CHECKLIST 10- CHALLENGING COMPLIANCE	Resource
Assessment	
You have policies and procedures in place for receiving and responding to complaints or inquiries about your personal information handling policies and practices.	
You advise individuals or complainants of the existence of all relevant complaint processes, including the right to make a complaint to a regulatory body.	

Privacy Assessment Checklist -Custodian

CHECKLIST FOR PRINCIPLE 1 -ACCOUNTABILITY	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You have clearly delineated who, within your organization, is responsible for privacy governance and management.			
You have directed staff through policy, procedure or training to provide the name, address and phone number of the **Privacy** contact person to clients when requested.			
You have verified that third parties have implemented the privacy controls stated in any **contractual/consent** agreements.			
Your **policy and guidelines** address the principle of "identifying purpose" regarding personal information.			
Your **policy and guidelines** address the principle of "consent" regarding personal information.			
Your **policy and guidelines** address the principle of "limiting collection" of personal information.			
Your **policy and guidelines** address the principle of "limiting use, disclosure and retention" of personal information.			
Your **policy and guidelines** address the principle of "accuracy" regarding personal information.			
Your **policy and guidelines** address the principle of "safeguards" with respect to personal information.			
Your **policy and guidelines** address the principle of "openness" regarding personal information.			
Your **policy and guidelines** address the principle of "individual access" regarding personal information.			
Your **policy and guidelines** address the principle of "challenging compliance" regarding personal information.			
You have trained **staff/members** regarding the protection of personal information by informing them of organizational privacy policies, procedures and best practices.			
You have developed documentation to explain your personal information protection policies and procedures to customers and the general public.			

CHECKLIST FOR PRINCIPLE 2 - IDENTIFYING PURPOSE	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You have documented your purpose(s) for collecting personal information.			
You seek the consent of clients and customers before using information for any new purpose if required.			

CHECKLIST FOR PRINCIPLE 3 – CONSENT	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You obtain customer consent for any collection, use or disclosure of personal information.			
If you don't obtain customer consent for the collection, use and disclosure of personal information, you have determined that it is not required under (s.37 of PHIA).			
You allow a client or customer to withdraw consent at any time subject to legal or contractual restrictions and reasonable notice.			

CHECKLIST FOR PRINCIPLE 4-LIMITING PURPOSE	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You have clearly delineated who, within your organization, is responsible for privacy governance and management.			

CHECKLIST 5 - FOR LIMITING USE, DISCLOSURE, AND RETENTION	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You only retain personal information as long as necessary to allow for the fulfillment of identified purposes.			
You have policies/guideline regarding the destruction of personal information, including the role of contractors performing such services.			

CHECKLIST FOR PRINCIPLES 6- ACCURACY	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
Your policies/guidelines address the accuracy, completeness and currency of personal information which includes a process through which individuals can challenge the accuracy of information.			
You record when and where key information was collected, including dates of corrections or updates to such information.			

CHECKLIST FOR PRINCIPLES 7- SAFEGUARDS	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You have adopted physical, technical and administrative safeguards to protect personal information against loss or theft as well as unauthorized access, disclosure, copying, use or modification.			
You have implemented processes to prevent unauthorized access to personal information during the disposal or destruction of information.			
You have established an information security breach policy and commit to investigating the root-cause of such breaches.			
You have developed and implemented policies and practices including appropriate safeguards for all uses of personal information outside the office.			

CHECKLIST FOR PRINCIPLES 8- OPENNESS	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You explain to customers why you collect, how you use and when you will disclose their personal information.			
You describe to your clients how they can obtain access to or correct their personal information.			

CHECKLIST FOR PRINCIPLE 9- INDIVIDUAL ACCESS	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You have advised staff of the need to direct requests for access to information to the staff member responsible for processing these requests.			
You limit refusal to provide access to information to exceptions described in **Section 58 of (PHIA).**			
You respond to a request for information in not more than 30 days unless you notify the requestor within that time period of your need to extend the time limit for response, indicate the extended time limit and inform the requester of his or her right to complain to the **OPC-NL**.			
You allow individuals to challenge the accuracy of personal information and amend information when an individual demonstrates that information is inaccurate or incomplete.			

CHECKLIST 10- CHALLENGING COMPLIANCE	Compliance		Evidence(policy, guideline, position statement, etc)
Assessment	Met	Not Met	
You have policies and procedures in place for receiving and responding to complaints or inquiries about your personal information handling policies and practices.			
You advise individuals or complainants of the existence of all relevant complaint processes, including the right to make a complaint to a regulatory body.			

The following section in blue is intended for those health professionals who are in direct contact with personal information but not necessarily the custodian of the client file. As in the above section, the assessment statements are indicated with the associated NLCHP referenced resource. Following the resource list is the self-assessment checklist aligned with the privacy principles.

Privacy Assessment Resource- Health Professional

CHECKLIST FOR PRINCIPLE 1 – ACCOUNTABILITY	Resource
Assessment	
You know who, within your organization, is responsible for privacy governance and management.	**NLCHP Privacy Document.** pp 10; 1.1-1.4 **PHIA**: Part II, Section 18
You have privacy policies and practices that apply to the personal information of your clients.	**NLCHP Privacy Document.** pp 11; 1.4; **PHIA**: Part II, Section 18
You are accountable for the protection of personal information.	**NLCHP Privacy Document.** pp.10; Template: pp. 26-27; **PHIA:** PART II, Section 13-20
You have been trained in privacy, as is new staff and there is refresher training for existing staff.	**NLCHP Privacy Document.** pp 26; **PHIA:** Part II
You have documentation to explain your personal information protection policies and procedures to customers and the general public.	

CHECKLIST FOR PRINCIPLE 2 - IDENTIFYING PURPOSES	Resource
Assessment	
You understand why you are collecting personal information at or before the time of collection.	**NLCHP Privacy Document pp. 11, 12; PHIA: Part IV; Sect 33(3)**
You ensure the consent of clients and customers is in place if required before using information for any new purpose.	**NLCHP Privacy Document pp. 12; PHIA; Part III ,Sect 23-28**

CHECKLIST FOR PRINCIPLE 3 - CONSENT	Resource
Assessment	
You obtain customer consent for any collection, use or disclosure of personal information.	NLCHP Privacy Document pp. 12; PHIA; Part III ,Sect 23-28
If you don't obtain customer consent for the collection, use and disclosure of personal information, you have determined that it is not required under (s.37 of PHIA).	
You make reasonable efforts to ensure that clients and customers are notified of the purposes for which personal information will be used or disclosed.	
You allow a client or customer to withdraw consent at any time subject to legal or contractual restrictions and reasonable notice.	
You inform clients and customers of the implication of the withdrawal of consent.	
You consider the sensitivity and intended use of personal information, and the reasonable expectations of clients and customers in determining which form of consent (implied or expressed) you will accept for the collection, use and disclosure of personal information.	

CHECKLIST FOR PRINCIPLES 4 - LIMITING COLLECTION	Resource
Assessment	
You limit the amount and type of personal information you collect to what is necessary for the identified purpose.	NLCHP Privacy Document pp. 11, 12; PHIA: Part IV; Sect 33(3)
You have documented the specific types of information you collect along with the purposes for collection.	

CHECKLIST FOR PRINCIPLES 5- LIMITING USE, DISCLOSURE, AND RETENTION	Resource
Assessment	
You do not use or disclose information for purposes beyond those for which it was collected, except with the consent of the individual or as required by law.	
You have policies on the destruction of personal information, including the role of contractors performing such services.	

CHECKLIST FOR PRINCIPLES 6- ACCURACY	Resource
Assessment	
You take reasonable measures to ensure that personal information is accurate, complete and up-to-date prior to using the information to make decisions.	
You have policy on the accuracy, completeness and currency of personal information which includes a process through which individuals can challenge the accuracy of information.	
You record when and where key information was collected, including dates of corrections or updates to such information.	

CHECKLIST FOR PRINCIPLES 7- SAFEGUARDS	Resource
Assessment	
You have physical, technical and administrative safeguards to protect personal information against loss or theft as well as unauthorized access, disclosure, copying, use or modification.	
You are aware of the importance of maintaining the confidentiality of personal information and have signed an oath of confidentiality.	
You understand the processes to prevent unauthorized access to personal information during the disposal or destruction of information.	
You adhere to information security policies and practices.	
You understand an information security breach policy and guidelines.	
You understand policies and practices including appropriate safeguards for all uses of personal information outside the office/practice area.	

CHECKLIST FOR PRINCIPLES 8- OPENNESS	Resource
Assessment	
You explain to customers why you collect, how you use and when you will disclose their personal information.	
You describe to your clients how they can obtain access to or correct their personal information.	

CHECKLIST FOR PRINCIPLE 9- INDIVIDUAL ACCESS	Resource
Assessment	
You have or are aware of policies and procedures for responding to requests for personal information under (PHIA).	
You are aware of policies and procedures to direct requests for access to personal information.	
You are aware and understand the principles and procedures regarding access and refusal to personal information as indicated in PHIA.	
You advise requestors of the reasons for refusal and recourse available to them when refusing to provide information.	
You allow individuals to challenge the accuracy of personal information and amend information when an individual demonstrates that information is inaccurate or incomplete.	

CHECKLIST 10- CHALLENGING COMPLIANCE	Resource
Assessment	
You have policies and procedures in place for receiving and responding to complaints or inquiries about your personal information handling policies and practices.	
You advise individuals or complainants of the existence of all relevant complaint processes, including the right to make a complaint to a regulatory body.	
You are cooperative to any assessment or investigation regarding personal information handling policies and practices.	

Privacy Assessment Checklist- Health Professional

CHECKLIST FOR PRINCIPLE 1 – ACCOUNTABILITY	Compliance		Evidence
Assessment	Met	Not Met	
You know who, within your organization, is responsible for privacy governance and management.			
You have privacy policies and practices that apply to the personal information of your clients.			
You are accountable for the protection of personal information.			
You have been trained in privacy, as is new staff and there is refresher training for existing staff.			
You have documentation to explain your personal information protection policies and procedures to customers and the general public.			

CHECKLIST FOR PRINCIPLE 2 - IDENTIFYING PURPOSES	Compliance		Evidence
Assessment	Met	Not Met	
You understand why you are collecting personal information at or before the time of collection.			
You ensure the consent of clients and customers is in place if required before using information for any new purpose.			

CHECKLIST FOR PRINCIPLE 3 - CONSENT	Compliance		Evidence
Assessment	**Met**	**Not Met**	
You obtain customer consent for any collection, use or disclosure of personal information.			
If you don't obtain customer consent for the collection, use and disclosure of personal information, you have determined that it is not required under (s.37 of PHIA).			
You make reasonable efforts to ensure that clients and customers are notified of the purposes for which personal information will be used or disclosed.			
You allow a client or customer to withdraw consent at any time subject to legal or contractual restrictions and reasonable notice.			
You inform clients and customers of the implication of the withdrawal of consent.			
You consider the sensitivity and intended use of personal information, and the reasonable expectations of clients and customers in determining which form of consent (implied or expressed) you will accept for the collection, use and disclosure of personal information.			

CHECKLIST FOR PRINCIPLES 4 - LIMITING COLLECTION	Compliance		Evidence
Assessment	Met	Not Met	
You limit the amount and type of personal information you collect to what is necessary for the identified purpose.			
You have documented the specific types of information you collect along with the purposes for collection.			

CHECKLIST FOR PRINCIPLES 5- LIMITING USE, DISCLOSURE, AND RETENTION	Compliance		Evidence
Assessment	Met	Not Met	
You do not use or disclose information for purposes beyond those for which it was collected, except with the consent of the individual or as required by law.			
You have policies on the destruction of personal information, including the role of contractors performing such services.			

CHECKLIST FOR PRINCIPLES 6- ACCURACY	Compliance		Evidence
Assessment	Met	Not Met	
You take reasonable measures to ensure that personal information is accurate, complete and up-to-date prior to using the information to make decisions.			
You have policy on the accuracy, completeness and currency of personal information which includes a process through which individuals can challenge the accuracy of information.			
You record when and where key information was collected, including dates of corrections or updates to such information.			

CHECKLIST FOR PRINCIPLES 7- SAFEGUARDS	Compliance		Evidence
Assessment	Met	Not Met	
You have physical, technical and administrative safeguards to protect personal information against loss or theft as well as unauthorized access, disclosure, copying, use or modification.			
You are aware of the importance of maintaining the confidentiality of personal information and have signed an oath of confidentiality.			
You understand the processes to prevent unauthorized access to personal information during the disposal or destruction of information.			
You adhere to information security policies and practices.			
You understand an information security breach policy and guidelines.			
You understand policies and practices including appropriate safeguards for all uses of personal information outside the office/practice area.			

CHECKLIST FOR PRINCIPLES 8- OPENNESS	Compliance		Evidence
Assessment	Met	Not Met	
You explain to customers why you collect, how you use and when you will disclose their personal information.			
You describe to your clients how they can obtain access to or correct their personal information.			

CHECKLIST FOR PRINCIPLE 9- INDIVIDUAL ACCESS	Compliance		Evidence
Assessment	Met	Not Met	
You have or are aware of policies and procedures for responding to requests for personal information under (PHIA).			
You are aware of policies and procedures to direct requests for access to personal information.			
You are aware and understand the principles and procedures regarding access and refusal to personal information as indicated in PHIA.			
You advise requestors of the reasons for refusal and recourse available to them when refusing to provide information.			
You allow individuals to challenge the accuracy of personal information and amend information when an individual demonstrates that information is inaccurate or incomplete.			

CHECKLIST 10- CHALLENGING COMPLIANCE	Compliance		Evidence
Assessment	Met	Not Met	
You have policies and procedures in place for receiving and responding to complaints or inquiries about your personal information handling policies and practices.			
You advise individuals or complainants of the existence of all relevant complaint processes, including the right to make a complaint to a regulatory body.			
You are cooperative to any assessment or investigation regarding personal information handling policies and practices.			

2. Privacy Breach Checklist

The Office of the Privacy Commissioner of Canada (OPC) outlines conditions where a breach of privacy may be identified and responded. "A privacy breach occurs when there is unauthorized access to or collection, use, or disclosure of personal information. Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation," [13]such as PHIA in Newfoundland and Labrador.

The Office of the Privacy Commissioner of Canada has a privacy breach check list that can be used by health professionals when a privacy breach occurs. Regardless of the nature of the breach organisations or health professionals should utilize the checklist when investigating and determining who to notify and the amount that type of information to be communicated as part of the notification process.

PRIVACY BREACH CHECKLIST

For more details, please see *Key Steps for Organizations in Responding to Privacy Breaches*.

Incident Description

- What was the date of the incident?
- When was the incident discovered?
- How was it discovered?
- What was the location of the incident?
- What was the cause of the incident?

Step 1: Breach Containment and Preliminary Assessment

- Have you contained the breach (recovery of information, computer system shut down, locks changed)?

- Have you designated an appropriate individual to lead the initial investigation?

- Is there a need to assemble a breach response team? If so, who should be included (e.g., privacy officer, security officer, communications, risk management, legal)?

- Have you determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?

[13] Office of the Privacy Commissioner of Canada (2012), Key Steps for Organizations in Responding to Privacy Breaches https://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf

• Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?

• Have you made sure that evidence that may be necessary to investigate the breach has not been destroyed?

Step 2: Evaluate the Risks Associated with the Breach

(i) What personal information was involved?

• What personal information was involved (name, address, SIN, financial, medical)?

• What form was it in (e.g., paper records, electronic database)?

• What physical or technical security measures were in place at the time of the incident (locks, alarm systems, encryption, passwords, etc.)?

(ii) What was the cause and extent of the breach?

• Is there a risk of ongoing breaches or further exposure of the information?

• Can the personal information be used for fraudulent or other purposes?

• Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?

• Has the personal information been recovered?

• Is this a systemic problem or an isolated incident?

(iii) How many individuals have been affected by the breach and who are they (e.g., employees, contractors, public, clients, service providers, other organizations)?

(iv) Is there any foreseeable harm from the breach?

• What harm to the individuals could result from the breach(e.g., security risk, identity theft, financial loss, loss of business or employment opportunities, physical harm, humiliation, damage to reputation, etc.)?

Do you know who has received the information and what is the risk of further access, use or disclosure?

• What harm to the organization could result from the breach (e.g., loss of trust, loss of assets, financial exposure, legal proceedings, etc.?

• What harm could come to the public as a result of notification of the breach (e.g., risk to public health or risk to public safety)?

Step 3: Notification

(i) Should affected individuals be notified?

- What are the reasonable expectations of the individuals concerned?
- What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?
- Is there a risk of physical harm? Is there a risk of humiliation or damage to the individual's reputation?
- What is the ability of the individual to avoid or mitigate possible harm?
- What are the legal and contractual obligations of the organization?

If you decide that affected individuals do not need to be notified, note your reasons.

(ii) If affected individuals are to be notified, when and, how will they be notified and who will notify them?

- What form of notification will you use (e.g., by phone, letter, email or in person, website, media, etc.)?
- Who will notify the affected individuals? Do you need to involve another party?
- If law enforcement authorities are involved, does notification need to be delayed to ensure that the investigation is not compromised?

(iii) What should be included in the notification?

Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal information disclosed in the notification to what is necessary:

- information about the incident and its timing in general terms;
- a description of the personal information involved in the breach;
- a general account of what your organization has done to control or reduce the harm;
- what your organization will do to assist individuals and steps individuals can take to reduce the risk of harm or further protect themselves;

• sources of information designed to assist individuals in protecting against identity theft;

• contact information of a department or individual within your organization who can answer questions or provide further information;

• whether your organization has notified a privacy commissioner's office;

• additional contact information to address any privacy concerns to your organization; and

• contact information for the appropriate privacy commissioner(s).

(iv) Are there others who should be informed about the breach?

• Should any privacy commissioners' office be informed?
http://www.oipc.nl.ca/

• Should the police or any other parties be informed?
This may include insurers; professional or other regulatory bodies; credit card companies, financial institutions or credit reporting agencies; other internal or external parties such as third party contractors, internal business units not previously advised of the privacy breach, union or other employee bargaining units).

Step 4: Prevention of Future Breaches

• What short or long-term steps do you need to take to correct the situation (e.g., staff training, policy review or development, audit)?