Guideline for the Collection, Maintenance, Transmission and Destruction of

Electronic Health Information

November 2009

Canadian Alliance of Physiotherapy Regulators
Alliance canadienne des organismes de réglementation de la physiothérapie

1243 Islington Avenue, Suite 501, Toronto ON M8X 1Y9 t:416-234-8800 f: 416-234-8820 www.alliancept.org

Contents

Acknowledgements

This document was developed with input from member regulators and other key partners from across Canada. The Canadian Alliance of Physiotherapy Regulators (The Alliance) gratefully acknowledges the following individuals and organizations:

- Physiotherapy regulators in the Atlantic region
- Mark Raven-Jackson and Jane Steblecki of Field LLP
- The Alliance member regulators
- Members of the Regulatory Workgroup on Funding System Issues (RWFSI)

  Annick deGooyer
  Jenneth Swinamer
  Moyra Holliday
  Dennis Desautels
  Carol Puri
  Pamela C. Fralick
  Joan Ross
  Margaret Butler
  Dianne Millette

Note to Readers

This document outlines key considerations for physiotherapy* regulators when advising their members on the collection, maintenance, transmission and destruction of electronic health information.

The principles associated with managing electronic health information are not new to physiotherapists in Canada. In their respective jurisdictions, physiotherapists have an obligation to properly collect, maintain, transmit and destroy records regardless of the medium in which they are kept. Yet, with dramatic advances in technology in recent years and the associated risks of transmitting information electronically, physiotherapists should take precautions to ensure that client consent and confidentiality is managed appropriately.

Physiotherapists should consider the links between their record keeping and emerging privacy legislation as well as initiatives such as the Canadian Institute for Health Information's NeCST project, which will inform the profession about acceptable transmission standards for electronic health information. Federal and provincial initiatives outlining legal obligations related to the protection of personal privacy have an impact on how electronic information is collected, maintained and transmitted. Federal legislation such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) has broad application to any commercial activity involving the collection, use and disclosure of personal information. Please see *Schedule A* of this document for a list of relevant legislation within each jurisdiction.

The field of electronic health information is growing and this document should be considered as a work in progress. As physiotherapists become more involved with electronic health information including electronic billing systems, this document will need to be updated.

In all jurisdictions, it is the responsibility of registered physiotherapists to be familiar with the content and implications of all laws applicable to their safe, effective and ethical practice. That includes, but is not limited to compliance with regulatory standards and compliance with other statutory requirements (e.g. hospital statutes, workers compensation statutes, privacy of health information statutes).

All physiotherapists, physiotherapy clinics, and organizations involved in the collection of health information should consult their own legal counsel in order to determine:

a. What legislative obligations apply to their role in the collection, storage, use and transmission electronic health information?
b. What fines or penalties can be levied if there is a breach of the legislative obligation?
c. What legislative developments are occurring at a provincial level which will impact on a physiotherapist's electronic health information practices?

For more information about the retention and transmission of electronic health information in Canada, physiotherapists should contact their provincial/territorial physiotherapy regulator.

* Physiotherapy and related words are official marks used with permission.

Introduction

In recent years, advances in computer technology have enabled many physiotherapists to incorporate electronic record systems into their practice in order to facilitate document storage and retrieval. The November 28, 2002 the Romanow Report advocated the development and maintenance of electronic health records amongst Canadian healthcare providers, which would, in part:

- Allow access to a client's entire medical history with relative ease;
- Clearly and succinctly document a client's response to treatment;
- Provide inherently accurate, legible and organized records; and
- Be potentially more secure than paper records.

E-mail and the Internet have also evolved to a point where they enable the transmission of electronic health information[1] from physiotherapists to funding agencies or organizations.

Currently there is a movement to expand communications between funding agencies or organizations and physiotherapists using electronic transmissions as a means to:

- Reduce paperwork;
- Streamline billing procedures;
- Identify the most cost effective treatment; and
- Assess the legitimacy of claims.

This guideline addresses the following topics:

A. Collecting Electronic Health Information:
    i. A Client's Consent;
    ii. Relevant Legislation and Enforcement Provisions; and
    iii. Relevant Transmission Standards.

B. Maintaining an Integral Electronic Record System:
    i. Data Back Up Plan;
    ii. Deleting Procedures;
    iii. Information Access Control;
    iv. Personnel Training and Security;
    v. Security Configuration Management;
    vi. Security Incident Procedure;
    vii. Physical access controls;
    viii. Training; and
    ix. Breach Reporting.

C. Transmitting Electronic Health Information
    i. Content of Transmission; and
    ii. Transmission Agreements.

[1] Health information, in its broadest sense, is a record that contains diagnostic or treatment information that would individually identify the recipient of physiotherapy treatment. A record would include electronic information contained on a database or server.

A. Collecting Electronic Health Information

i. A Client's Consent

Physiotherapists are accustomed to collecting sensitive health information from their clients and treating this confidential information with the utmost care. The electronic storage and transmission of health information does, however, raise some additional risks that should, to the extent possible, be disclosed to the client in order to acquire informed consent to treatment.

An informed discussion between a physiotherapist and client should:

- take place in which the method of creating and maintaining an electronic health record is discussed;
- occur when the client first presents for treatment;
- include a handout explaining the security precautions in place; and
- be documented and signed by the client.

Individual physiotherapists may consider including a section on electronic storage and transmission of health information in their standard form of consent as follows:

> "I understand and agree that my health information will be maintained by [physiotherapist] in an electronic form and may be electronically transmitted to [general categories or specific names of: funding agencies, organizations or other health care providers] as required in the course of my treatment. The risks and benefits of maintaining and transmitting my health information in electronic form have been discussed with me."

It is important to emphasize that a standard form of consent should never replace a detailed and meaningful discussion with the client. It should simply be used as a method of documenting the fact that the discussion took place.

It should be recognized that a client might have the right to withhold their consent to having their health information maintained on an electronic system or transmitted via the Internet. This possibility should be discussed with funding agencies or organizations in order to determine what contingencies are in place to accommodate such individuals.

Finally, reasonable expectations of the client are relevant when consent is obtained. One of those expectations is that electronic health information will not be collected indiscriminately or stored unnecessarily. The principle for collecting, using and disclosing health information is that only the amount of health information that is *essential* to enable the physiotherapists or the recipient, as the case may be, to carry out their intended purpose should be collected, used or disclosed.

ii. Relevant Legislation and Enforcement Provisions

Within the last few years many provinces have enacted health information laws largely as a response to a regulatory gap to accommodate the development of electronic health information networks in Canada. In an effort to introduce legislation on an expedited basis, provinces have utilized several different models of legislation.

As this is an evolving area, any collection, use and disclosure of electronic health information on a national basis will be managed with a degree of uncertainty in the short term. Currently, there is a movement to modify and harmonize health information legislation across Canada and the goal of a national electronic health information base [as espoused in Recommendation 12 of the Romanow Report] will push this mandate forward.

One common element in all health information legislation is that penalties and fines can be levied against health care providers who are in breach of the legislation. The fines can be substantial and the penalties could have a significant impact on a physiotherapist's practice.

iii. Relevant Transmission Standards

While the transmission of electronic health information is emerging within the physiotherapy profession, it has been part of the practice of other health care professionals for many years. Dentists and pharmacists have long-standing electronic billing systems that link with their collection of patient information. As a result, transmission standards have evolved and the physiotherapy profession is in the process of working with other providers to ensure that internationally accepted standards for transmission are adopted.

B. Maintaining an Integral Electronic Record System

An electronic health information system has the following features:

a. A hardware and operating system design which provides longitudinal and time links to other patient records or information systems; allows continuous authorized access; supports simultaneous user interfaces; and can provide access to local or remote information sources;

b. Health record software that can guarantee confidentiality and audit trails; provide problem lists; keep records of clinical reasoning and rationale; facilitate clinical problem solving; support direct health care provider entry and assist health care providers in measuring and managing costs to improve quality of care; and

c. Content that measures both the health status and functional levels of the client and is flexible enough to support the evolving needs of a practice.

Once an electronic health information system is in place, the primary concern is the integrity of the electronic health information and the safeguarding against potential corruption, unauthorized access and inadvertent purging. The following is a brief summary of the policies and procedures that should be kept in writing and implemented in order to ensure prudent practice.

i. Data Backup Plan

A physiotherapist and the clinic or health care facility in which they work must have continuous access to electronic health information in order to provide the requisite standard of care to clients. Should electronic health information become inaccessible due to data corruption or, for instance, a fire in the facility, it is imperative to routinely "backup" the electronic health information to ensure that this valuable information is not lost.

The policy pertaining to data backup should include the following:

a. Name of backup coordinator and record keeper;
b. Method(s) used for data backups, with a checklist of procedures;
c. Frequency of data backups;
d. Location of on-site data storage;
e. Location of off-site data storage; and
f. Types of data (generally) to be backed up.

Each individual physiotherapist will need to decide what electronic health information they will backup. This may vary depending on what electronic health information is deemed to be required to meet regulatory standards or other legislation.

Physiotherapists must test their data backup regularly in order to ensure that, should electronic health information become corrupted or purged, it can be easily replaced without compromising client care.

It is best practice to backup *all* electronic health information that is stored on the system's hard drive, as this approach:

a. Offers the greatest amount of data security;
b. Allows for one-step restoration of total memory loss; and
c. Can often be done automatically during off-hours.

In addition, consideration should be made to the technical requirements for reading data backup files in the longer term. Changes in software programs and their availability may make data retrieval difficult and potentially costly over longer retention periods.

Overall, implementing data backup technology tends to be expensive and may be impractical for some smaller physiotherapy practices. A practice should adopt an electronic health record keeping system only if it has the resources to provide the necessary support, including adequate backup procedures.

ii. Deleting Procedures

Physiotherapists must have established and documented policies and procedures in place with respect to paper record retention and safe, confidential destruction. These policies and procedures need to meet the minimal standards established by the physiotherapy regulator and other applicable legislation.

The same reasoning applies to electronic health records. Existing policies and procedures should be modified to accommodate the removal of electronic health information from the electronic database in accordance with relevant privacy legislation.

Physiotherapists should ensure that the database management system utilized actually deletes the electronic health information, rather then simply "marking" it as deleted. The distinction is that "marking" data as deleted does not mean the electronic health information has been purged from the system; it simply means that the database management system can overwrite the electronic health information if further space is required.

If a physiotherapist upgrades or replaces a database management system it is imperative that the hard-drive has been completely erased and reformatted. If the hard-drive has been replaced because it is damaged a physiotherapist should ensure that the hard-drive is physically destroyed. Computer recycling companies may provide this service.

iii. Information Access Control

Physiotherapists must determine who associated with their facility has the ability to access and modify electronic health information. The level of access should correspond with the confidential nature of the health information. It is imperative to recognize that a physiotherapist is responsible for those individuals/employees who are granted access to electronic health information. There should be explicit organizational policies that address issues including but not limited to data access, audits and, security clearance.

All access to electronic health information via computer terminal should be controlled through a protected, individual password or through physical security measures. Computer terminals should not be left unattended if a user has logged into the database as the electronic health information is left insecure. Identity should be authenticated through a unique token, such as a magnetic strip or an individual password. Each individual must be responsible for his or her own password and a policy should be implemented which requires the password to be changed routinely.

Physiotherapists must consistently review access privileges and remove passwords from the system if users no longer require access. Further, all unauthorized accesses or attempts to access electronic health information should form part of an audit record that can be reviewed by the physiotherapist and provide evidence of violations or system misuse. Inappropriate access to confidential information is considered by most employers to be grounds for immediate termination.

iv. Personnel Training and Security

A physiotherapist must ensure that authorized and knowledgeable staff maintains the electronic health information.

Depending on the size of the physiotherapy practice this may involve having a full-time information technology (IT) employee to maintain the database or it may involve a service contract with a local IT company, preferably the vendor that assisted with the system installation.

Every user on the system should be trained to ensure that the electronic health information remains secure. This includes ongoing training on the privacy policies and procedures of the physiotherapy practice. Further, all staff, including IT service providers should sign a Non-Disclosure Acknowledgement in a form similar to that contained in Schedule B.

v. Security Configuration Management

A physiotherapist must ensure that the electronic record system is kept current by updating the hardware, software and conducting maintenance reviews. Security features must be assessed on a regular basis and the following is an example of some features that may be utilized by a physiotherapist:

- Viruses can compromise data as well as compromise security. As viruses develop and evolve over time, routinely updating anti-viral software is crucial. An immediate update of anti-viral software is necessary when a new virus is identified and poses a threat to the system.
- If an electronic record system is permanently connected to the Internet the physiotherapist should have firewall protection. A firewall is essentially a software bouncer, blocking a computer's doorway to the Internet. The protection extends to both incoming and outgoing net traffic and nothing can bypass the firewall unless expressly permitted by the physiotherapist.
- If a physiotherapist uses a wireless network or a virtually private network ["VPN"] the electronic health information should be encrypted. Encryption is the conversion of electronic health information into a form, called a ciphertext, which cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

vi. Security Incident Procedure

Policies and procedures should be in place to audit the transmission and receipt of electronic health information. Should electronic health information be compromised during the transmission process a determination can be made as to the source of the compromise and risk management efforts can be undertaken to ensure that future compromises will not occur.

Physiotherapists can implement software that creates an audit trail, which is an electronic log used to track computer activity. For example, an employee might have access to a section of the electronic record system, such as billing. However, that same employee may be unauthorized to access electronic health information. If that employee attempts to access an unauthorized section by typing in passwords, this improper activity is recorded in the audit trail. Audit trails are also used to investigate cybercrimes. In order for investigators to expose a system intruder's identity, they can follow the trail the intruder left in cyberspace.

vii. Physical Access Control

Passwords and magnetic access cards are entirely undermined if computer workstation locations enable third parties to observe electronic health information on the computer screen. Computer terminals, specifically laptops, must be secured at all times (i.e., in locked rooms or locked down with security cables) in order to avoid property theft that includes theft of electronic health information. It is also important to ensure that employees do not utilize the "remember my password" option that are often found on computers and laptops and that workstations are "locked" when employees leave their desk for an extended period of time. Handheld devices (e.g. Blackberries and iPhones) attract similarly stringent safeguarding obligations. These devices should "lock" after a minimal period of inactivity (e.g. after 15 minutes or as suggested by information technology administrators) to minimize risk of unauthorized access after loss or misplacement. Further, ancillary hardware such as external or removable devices (e.g. memory sticks or keys) should only be loaded with the least amount of information necessary to serve the purpose and, where possible, password protected. After data is transferred or used for its intended purpose, the device should be cleared. At all times, including during transport, the safeguarding duties equally apply; devices must be not left unattended unless securely stowed.

Policies and procedures should be in place to provide a secure environment to operate and contain an electronic records system.[2]

viii. Training

Both physiotherapists and their staff must be educated in the importance of accurately inputting electronic health information; transmitting electronic health information and security reminders should be issued on a periodic basis. Electronic record system vendors are often willing to conduct seminars as part of a service contract or pursuant to a purchase agreement.

ix. Breach Reporting

The physiotherapist, staff and others working with health information should have in place, and be familiar with, a plan for reporting and managing privacy breaches. Some legislation makes such reporting mandatory. In any event, a process should be implemented to mitigate risk and help prevent reoccurrence.

C. Transmitting Electronic Health Information

With the transmission of electronic health information via e-mail or the Internet the individual physiotherapist loses an element of control. Physiotherapists share responsibility and accountability with third parties to maintain the security and integrity of the electronic health information. A physiotherapist should exercise due diligence in determining whether the recipient of the electronic health information has appropriate standards in place to ensure that confidentiality is maintained. As mentioned earlier, there are ongoing efforts being made on a national level to ensure that transmission standards are acceptable.

The primary concern with transmitting electronic health information is the inappropriate accessing of this information by third parties. Many institutions, with varying employment practices, may be the recipient of electronic health information and physiotherapists are advised to exercise caution when transferring or disclosing health information electronically.

The advances in e-mail, Internet security, VPN's, and encryption, which are often needed for financial transactions, are generally adequate to protect electronic health information during the transmission process. As it is only a copy of the electronic health information being sent, there is little concern with data corruption or inadvertent purging of electronic health information during the transmission process. The advances in e-mail, Internet security, VPN's, and encryption, which are often needed for financial transactions, are generally adequate to protect electronic health information during the transmission process. As it is only a copy of the electronic health information being sent, there is little concern with data corruption or inadvertent purging of electronic health information during the transmission process.

i. Content of Transmission

The basic tenet of health information disclosure is that a physiotherapist should only disclose the absolute minimum health information required to fulfill the stated purpose. Whether the

[2] In Alberta the Information and Privacy Commission has issued a decision involving the theft of computers containing electronic health information from a health care facility that did not have appropriate policies and procedures in place [Investigation Report #H0054 & H0056].

requestor of the electronic health information is a funding agency or another healthcare provider, this tenet remains the same. The less electronic health information provided ensures minimal harm should there be a breach in confidentiality.

Any transmission of electronic health information via Internet or e-mail should be accompanied with a statement in a form similar to *Schedule C*.

ii. Transmission Agreements

In an attempt to ensure that the recipient of electronic health information, i.e. a funding agency or another healthcare provider, is in compliance with the standards established by the physiotherapist a transmission agreement should be in place. A transmission agreement is a contract between the physiotherapist and the recipient of electronic health information that protects the physiotherapist in the event that there is a breach in confidentiality by the recipient.

A sound transmission agreement, an example of which is contained in *Schedule D*, ensures that the recipient of electronic health information (and their employees) institute and adhere to policies in place and provide the physiotherapist with indemnification should a breach of confidentiality occur. Transmission of electronic health information can often occur through a third party (i.e. server provider or data management) and a transmission agreement should extend a duty to the recipient.

Summary and Conclusions

A client's care and a physiotherapist's practice can benefit from the installation of an electronic record system. The transmission of electronic health information can streamline transactions between physiotherapists and funding agencies. This transition does require careful planning and the implementation of policies and procedures in order to protect the physiotherapist, who is ultimately responsible for ensuring that confidentiality is maintained.

References

1. Andrews G; Wilkins GE, “Privacy and the computerized medical record” Med J Aust 1992 Aug 17;157(4):223-5.

2. Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada* (November 2002) Commissioner R. Romanow, Q.C.

3. Computer-Based Patient Record Institute, Section 5.2 – “Complying with Consent, Inspection, and Disclosure Requirements”,

4. Lamberg, L., “Confidentiality and privacy of electronic medical records: Psychiatrists explore
risks of the “information age” JAMA 2001 Jun 27; 285(24):3075-6.

5. Lusk R, “Update on the electronic medical record” Otolaryngol Clin North Am 2002 Dec; 35(6):1223-36.

6. Meyers JS, “Electronic medical records: 10 Questions I Didn’t Know To Ask”
Fam Pract Manag 2001 Mar;8(3):29-32.

7. “Model Code for the Protection of Personal Information” http://laws.justice.gc.ca/en/P-8.6/91270.html#rid-91272

8. Roberts, J; Decter SR; Nagel D, “Confidentiality and Electronic Medical Records” Ann Intern Med 1998 March 15; 128(6):510-1.

9. Shoenberg, R; Safran C, “Internet based repository of medical records that retains patient confidentiality”
BMJ 2000 Nov 11; 321(7270): 1199-203.

Schedule A - Legislation Relevant to Health Information (as at November 2009)

PROVINCIAL/TERRITORY JURISDICTION & SCOPE	TYPE	TITLE	CITATION	LINK
Federal				
Certain public & private. Applies to federally-regulated private sector organizations and to personal and health information that is collected, used or disclosed in the course of commercial activity that takes place across the Canadian border, between provinces and within a Canadian province that has not enacted "substantially similar" legislation.	Act	*Personal Information Protection and Electronic Documents Act* ("PIPEDA")	RSC 2000 c. 5	http://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html
Alberta				
Mostly public sector soon to cover both public and private	Act	*Health Information Act*	R.S.A. 2000, c. H-5	http://www.canlii.org/en/ab/laws/stat/rsa-2000-c-h-5/latest/rsa-2000-c-h-5.html
Mostly public sector soon to cover both public and private	Regulation	*Designation Regulation* (under the *Health Information Act*)	Alta. Reg. 69/2001	http://www.canlii.org/en/ab/laws/regu/alta-reg-69-2001/latest/alta-reg-69-2001.html
Mostly public sector soon to cover both public and private	Regulation	*Health Information Regulation* (under the *Health Information Act*)	Alta. Reg. 70/2001	http://www.canlii.org/en/ab/laws/regu/alta-reg-70-2001/latest/alta-reg-70-2001.html
Private Note: Declared "substantially similar" to PIPEDA.	Act	*Personal Information Protection Act*	S.A. 2003, c. P-6.5	www.canlii.org/ab/laws/sta/p-6.5/20060718/whole.html
Private Note: Declared "substantially similar" to PIPEDA.	Regulation	*Personal Information Protection Act Regulation* (under the *Personal Information Protection Act*)	Alta. Reg. 366/2003	http://www.canlii.org/en/ab/laws/regu/alta-reg-366-2003/latest/alta-reg-366-2003.html
British Columbia				
Certain public & private	Act	*E-Health (Personal Health Information Access and Protection of Privacy) Act*	S.B.C. 2008, c. 38	http://www.canlii.org/en/bc/laws/stat/sbc-2008-c-38/latest/sbc-2008-c-38.html

Certain public & private	Regulation	*Disclosure Directive Regulation* (under *E-Health (Personal Health Information Access and Protection of Privacy) Act*)	B.C. Reg. 172/2009	http://www.canlii.org/en/bc/laws/regu/bc-reg-172-2009/latest/bc-reg-172-2009.html
Certain public & private Note: Declared "substantially similar" to PIPEDA.	Act	*Personal Information Protection Act*	S.B.C. 2003, c. 63	http://www.canlii.org/en/bc/laws/stat/sbc-2003-c-63/latest/sbc-2003-c-63.html
Certain public & private Note: Declared "substantially similar" to PIPEDA.	Regulation	*Personal Information Protection Act Regulations* (under *Personal Information Protection Act)*	B.C. Reg. 473/2003	http://www.canlii.org/en/bc/laws/regu/bc-reg-473-2003/latest/bc-reg-473-2003.html
Manitoba				
Certain public & private	Act	*Personal Health Information Act*	C.C.S.M. c. P33.5	http://www.canlii.org/en/mb/laws/stat/ccsm-c-p33.5/latest/ccsm-c-p33.5.html
Certain public & private	Regulation	*Personal Health Information Regulation* (under the *Personal Health Information Act*)	Man. Reg. 245/97	http://www.canlii.org/en/mb/laws/regu/man-reg-245-97/latest/man-reg-245-97.html
Public	Act	*Freedom of Information and Protection of Privacy Act*	C.C.S.M. c. F175	http://www.canlii.org/en/mb/laws/stat/ccsm-c-f175/latest/ccsm-c-f175.html
Public	Regulation	*Access and Privacy Regulation* (under the *Freedom of Information and Protection of Privacy Act*)	Man. Reg. 64/98	http://www.canlii.org/en/mb/laws/regu/man-reg-64-98/latest/man-reg-64-98.html
New Brunswick				
Public	Act	*Protection of Personal Information Act*	S.N.B. 1998, c. P-19.1	http://www.canlii.org/en/nb/laws/stat/snb-1998-c-p-19.1/latest/snb-1998-c-p-19.1.html
Public	Regulation	*General Regulation* (under the *Protection of Personal Information Act*)	N.B. Reg. 2001-14	http://www.canlii.org/en/nb/laws/regu/nb-reg-2001-14/latest/nb-reg-2001-14.html
Newfoundland and Labrador				
Certain public & private	Act (not yet in force)	*Personal Health Information Act*	S.N.L. 2008, c. P-7.01	http://www.canlii.org/en/nl/laws/stat/snl-2008-c-p-7.01/latest/snl-2008-c-p-7.01.html

Public	Act	*Access to Information and Protection of Privacy Act*	S.N.L. 2002, c. A-1.1	http://www.canlii.org/en/nl/laws/stat/snl-2002-c-a-1.1/latest/snl-2002-c-a-1.1.html
Public	Regulation	*Access to Information Regulations* (under the *Access to Information and Protection of Privacy Act*)	N.L.R. 11/07	http://www.canlii.org/en/nl/laws/regu/nlr-11-07/latest/nlr-11-07.html
Northwest Territories				
Public	Act	*Access to Information and Protection of Privacy Act*	S.N.W.T. 1994, c. 20	http://www.canlii.org/en/nt/laws/stat/snwt-1994-c-20/latest/snwt-1994-c-20.html
Public	Regulation	*Access to Information and Protection of Privacy Regulations* (under the *Access to Information and Protection of Privacy Act*)	N.W.T. Reg. 206-96	http://www.canlii.org/en/nt/laws/regu/nwt-reg-206-96/latest/nwt-reg-206-96.html
Nova Scotia				
Certain public & private	Bill	*Personal Health Information Act*	Bill 64, First Reading: November 4, 2009	http://www.gov.ns.ca/legislature/legc//bills/61st_1st/1st_read/b064.htm
Certain public & private	Act	*Freedom of Information and Protection of Privacy Act*	S.N.S. 1993, c. 5	http://www.canlii.org/en/ns/laws/stat/sns-1993-c-5/latest/sns-1993-c-5.html
Public	Regulation	*Freedom of Information and Protection of Privacy Regulations* (under *Freedom of Information and Protection of Privacy Act*)	N.S. Reg. 105/94	http://www.canlii.org/en/ns/laws/regu/ns-reg-105-94/latest/ns-reg-105-94.html
Public	Regulation	*Regulations Amending the Schedule to the Act Listing Public Bodies* (under *Freedom of Information and Protection of Privacy Act*)	N.S. Reg. 205/2009	http://www.canlii.org/en/ns/laws/regu/ns-reg-205-2009/latest/ns-reg-205-2009.html
Nunavut				
Public	Act	*Access to Information and Protection of Privacy Act*	S.N.W.T. (Nu.) 1994, c. 20	http://www.canlii.org/en/nu/laws/stat/snwt-nu-1994-c-20/latest/snwt-nu-1994-c-20.html
Public	Regulation	*Access to Information and Protection of Privacy Regulations* (under the *Access to Information and Protection of Privacy Act*)	N.W.T. Reg. (Nu.) 206-96	http://www.canlii.org/en/nu/laws/regu/nwt-reg-nu-206-96/latest/nwt-reg-nu-206-96.html
Ontario				

Certain public & private Note: Declared "substantially similar" to PIPEDA.	Act	*Personal Health Information Protection Act, 2004*	S.O. 2004, c. 3, Sch. A	http://www.canlii.org/en/on/laws/stat/so-2004-c-3-sch-a/latest/so-2004-c-3-sch-a.html
Certain public & private Note: Declared "substantially similar" to PIPEDA.	Regulation	*General Regulation* (under the *Personal Health Information Protection Act, 2004*)	O. Reg. 329/04	http://www.canlii.org/en/on/laws/regu/o-reg-329-04/latest/o-reg-329-04.html
Prince Edward Island				
Public	Act	*Freedom of Information and Protection of Privacy Act*	R.S.P.E.I. 1988, c. F-15.01	http://www.canlii.org/en/pe/laws/stat/rspei-1988-c-f-15.01/latest/rspei-1988-c-f-15.01.html
Public	Regulation	*General Regulations* (under the *Freedom of Information and Protection of Privacy Act*)	P.E.I. Reg. EC564/02	http://www.canlii.org/en/pe/laws/regu/pei-reg-ec564-02/latest/pei-reg-ec564-02.html
Quebec				
Private Note: Declared "substantially similar" to PIPEDA.	Act	*Act Respecting the Protection of Personal Information in the Private Sector*	R.S.Q. c. P-39.1	http://www.canlii.org/en/qc/laws/stat/rsq-c-p-39.1/latest/rsq-c-p-39.1.html
Public	Act	*Act Respecting the Access to Documents held by Public Bodies and the Protection of Personal Information*	R.S.Q. c. A-2.1	http://www.canlii.org/en/qc/laws/stat/rsq-c-a-2.1/latest/rsq-c-a-2.1.html
Saskatchewan				
Certain public & private	Act	*Health Information Protection Act*	S.S. 1999, c. H-0.021	http://www.canlii.org/en/sk/laws/stat/ss-1999-c-h-0.021/latest/ss-1999-c-h-0.021.html
Certain public & private	Regulation	*Health Information Protection Regulations* (under the *Health Information Protection Act*)	R.R.S. c. H-0.021 Reg. 1	http://www.canlii.org/en/sk/laws/regu/rrs-c-h-0.021-reg-1/latest/rrs-c-h-0.021-reg-1.html
Yukon				
Public	Act	*Access to Information and Protection of Privacy Act*	R.S.Y. 2002, c. 1, as amended by .Y. 2003, c. 20	http://www.gov.yk.ca/legislation/acts/atipp.pdf http://www.gov.yk.ca/legislation/acts/ataatipp.pdf
Public	Regulation	*Access to Information Regulation* (under the *Access to Information and Protection of Privacy Act*)	Y.O.I.C. 1996/53	http://www.canlii.org/en/yk/laws/regu/yoic-1996-53/latest/yoic-1996-53.html

Schedule B - Employee/Student/Volunteer Nondisclosure Acknowledgment

Note: This is a sample form of an agreement and is for discussion purposes only. It should not be used or relied on without it being reviewed by your own legal counsel to ensure compliance with provincial legislation.

I have been asked by [name of health care facility] to reaffirm my commitment made at the time of my employment/assignment to protect the confidentiality of health information. I understand that [name of health care facility] reminds its employees and volunteers of their confidentiality obligations on a periodic basis to help ensure compliance, due to the significance of this issue. By my signature below, I acknowledged that I made the commitment set forth below at the time of employment/assignment. I confirm my past compliance with it, and I reaffirm my continued obligation to it.

[Name of health care facility] has a legal and ethical responsibility to safeguard the privacy of all patients and protect the confidentiality of their health information. In the course of my employment/assignment at [name of health care facility], I may come into possession of confidential patient information, even though I may not be directly involved in providing patient services.

I understand that such information must be maintained in the strictest confidence. As a condition of my employment/assignment, I hereby agree that, unless directed by my supervisor, I will not at any time during or after my employment/assignment with [name of health care facility disclose any patient information to any person whatsoever or permit any person whatsoever to examine or make copies of any patient reports or other documents prepared by me, coming into my possession, or under my control, or use patient information, other than as necessary in the course of my employment/assignment.

When patient information must be discussed with other health care practitioners in the course of my work, I will use discretion to ensure that such conversations cannot be overhead by others who are not involved in the patient's care.

I understand that violation of this agreement may result in corrective action, up to and including discharge.

_____
Signature of Employee/Student/Volunteer

_____
Date

Schedule C - Statement Accompanying Electronic Transmission of Health Information

Note: This is a sample form and is for discussion purposes only. It should not be used or relied on without it being reviewed by your own legal counsel to ensure compliance with provincial legislation.

As the recipient of this electronic health information, you are prohibited from using the health information for any purpose other then the stated purpose. You may disclose the health information to another party only:

1. With the written authorization from the subject of the health information or his/her authorized representative; or

2. As required or authorized by provincial legislation.

You are required to destroy the Health Information after its stated need has been fulfilled.

Schedule D - Sample Electronic Record Transmission Agreement

Note: This is a sample form of an agreement and is for discussion purposes only. It should not be used or relied on without it being reviewed by your own legal counsel to ensure compliance with provincial legislation.

This agreement applies to all health information transmitted electronically between [name of the physiotherapist; Health care facility or Corporation] and [name of the other party, i.e. funding agency] ["Health Information"] in connection with its [business relationship]. In consideration of, and as a condition to, [business relationship], [name of other party] agrees to collect, use, disclose or otherwise handle the health information in accordance with all applicable privacy legislation and in accordance with the Privacy Policies of [name of the physiotherapist, healthcare facility or Corporation], including (without limitation) to:

1. Ensure that all the Health Information is secure and to prevent unauthorized access to its facilities and system in which the Health Information is maintained and through which the Health Information is transmitted; and
2. Ensure that the Health Information is, at all times, maintained in the strictest confidence and not disclosed to any unauthorized person/entity or used in any inappropriate manner.

In addition, [name of the other party] agrees:

1. To use the Health Information only for the purpose of providing services to [name of the physiotherapist; Health care facility or Corporation] for [purposes of the business relationship]; and
2. To disclose the Health Information only to those of its employees or agents who need to access the Health Information to provide services to [name of the physiotherapist; Health care facility or Corporation] for [purposes of the business relationship] and who have signed a confidentiality agreement providing substantially the same protection for the Health Information as this agreement.

If either party uses an intermediary third party to transmit, log, or process Health Information, that party shall, prior to the disclosure of the Health Information, obtain an agreement from that third party providing substantially the same protection for the Health Information as this agreement and shall be responsible for any acts, failures or omissions by that third party in its provision of services. For the purposes of this agreement, the third party shall be deemed to be an agent of that party.

Further, [name of the other party] agrees to indemnify and hold harmless [name of the physiotherapist; Health care facility or Corporation] from all damages, losses, costs, liabilities, and expenses resulting from any and all breaches of this agreement by [name of other party], its employees, or agents.

The obligations of [name of other party] under this agreement, including, without limitation to, its responsibility for maintaining the security and confidentiality of the Health Information, shall survive the termination of the [business relationship]. Upon termination of the [business relationship] or upon request of the [name of the physiotherapist; Health care facility or Corporation] all Health Information shall be returned to [name of the physiotherapist; Health care facility or Corporation] in a form acceptable to [name of the physiotherapist; Health care facility or Corporation] or electronically purged in a manner acceptable to [name of the physiotherapist; Health care facility or Corporation], and no copies thereof may be retained by [name of the other party].

_____
Signature of [name of the physiotherapist; Health care facility or Corporation]

_____
Date

_____
Signature of [name of the other party]

_____
Date