December 2003

GUIDELINE
FOR THE RETENTION AND TRANSMISSION OF ELECTRONIC HEALTH INFORMATION FOR PHYSIOTHERAPISTS

Prepared by:
Canadian Alliance of Physiotherapy Regulators
November 2003

Modified and Adopted by:
Newfoundland and Labrador College of Physiotherapy
P.O. Box 21351
St. John's, NL.
A1A 5G6

Note to Readers

This guideline aims to define the appropriate method in which to retain and transmit a client's electronic health information.

The purpose of these guidelines is:

- to consolidate the present regulator perspective on the retention and transmission of electronic health information in physiotherapy practice,
- to emphasize the inherent privacy in a client's electronic record that contains confidential health information,
- to outline the abundance of legislation that regulates health information in Canada and
- to generally advise physiotherapists on how to ensure that a client's electronic health information is properly collected, appropriately maintained and securely transmitted.

It is the responsibility of all 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 regulator standards and compliance with other statutory requirements (e.g. hospital statutes, workers compensation statutes, and privacy of health information statutes).

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 on retention and transmission of electronic health information in Canada, physiotherapists can contact their provincial/territorial physiotherapy regulator

- College of Physiotherapists New Brunswick
- Prince Edward Island College of Physiotherapists
- Newfoundland and Labrador College of Physiotherapists
- Nova Scotia College of Physiotherapists

Introduction

In recent years advances in computer technology has enabled many physiotherapists to incorporate electronic record systems into their practice in order to facilitate document storage and retrieval. On November 28, 2002 the Romanow Report was released which 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 then paper records.

E-mail and the Internet have also evolved to a point where it enables 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:

- Reducing paperwork;
- Streamlining billing procedures;
- Identifying the most cost effective treatment; and
- Assessing the legitimacy of claims.

This guideline will address the following topics:

(a) Collecting Electronic Health Information:
   i. A Client's Consent;
   ii. Relevant Legislation.

(b) Maintaining an Integral Electronic Record System:
   i. Data Backup;
   ii. Termination Procedures;
   iii. Information Access Control;
   iv. Personnel Security;
   v. Security Configuration Management;
   vi. Security Incident Procedure;
   vii. Physical access controls;
   viii. Training.

(c) Transmitting Electronic Health Information
   i. Content of Transmission;
   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 risks that should, as best as 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 may 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 health information will not be collected indiscriminately nor will it be electronically stored unnecessarily.

ii. Relevant Legislation

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. An outline of the relevant legislation is appended as Schedule A to this guideline.

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.

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

A physiotherapist and the clinic or health care facility they work in 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 critical, how much storage capacity is available, and what their budget allows.

Physiotherapists must test your 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 a "best practice" to backup <u>all</u> the 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.

Unfortunately, implementing this technology tends to be expensive and may be impractical for some smaller physiotherapy practices.

ii. Termination Procedures

Physiotherapists must have established and documented policies and procedures in place with regards to paper record retention. 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 and existing policies and procedures should be modified to accommodate the removal of electronic health information from the electronic database once it has become obsolete.

iii. Information Access Control

Physiotherapists must determine who 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.

All access to electronic health information via computer terminal should be controlled through a 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 periodically.

Physiotherapists must periodically 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.

iv. Personnel 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 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. 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 in circumstances where the Internet is involved virus checking must be conducted. Viruses can compromise data as well as compromise security. As viruses develop and evolve over time, updating anti-viral software is crucial.

vi. Security Incident Procedure

Policies and procedures should be in place to track 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.

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. Further, computer terminals, specifically laptops, must be secured at all times in order to avoid property theft that includes theft of electronic health information. Policies 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.

[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].

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 in the process and is forced to rely on a third party to maintain the security and integrity of the electronic health information. A physiotherapist's duty does not end with the transmission of electronic health information to a recipient. A physiotherapist can be liable for breach in confidentiality if due diligence was not exercised in determining whether the recipient of the electronic health information has appropriate standards in place to ensure that confidentiality is maintained.

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.

The advances in e-mail and Internet security, 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 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.

An acceptable form of 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 as well as provides 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. Further, 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", http://www.cpri-host.org/toolkit/5_2.html

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 Disclosing Health Information

British Columbia
Freedom of Information and Protection of Privacy Act, RSBC 1996, c-165.

Alberta
Health Information Act, RSA 2000 c-H-5.

Saskatchewan
In 1999 the *Saskatchewan Health Information Protection Act* received royal assent; however, it is not yet proclaimed.

Manitoba
Freedom of Information and Protection of Privacy Act, CCSM c. F175 and the *Personal Health Information Act*, CCSM c. P33.5.

Ontario
The Ontario Legislature is about to table a Bill called the *Privacy of Personal Information Act*. It is a modified version of the Bill of the same name that died on the order paper in the last session.

Freedom of Information and Protection of Privacy Act, RSO 1990 c. F.31 and *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990 c. M.56.

Quebec
The *Act Respecting the Protection of Personal Information in the Private Sector* covers private health care providers and facilities. The *Act Respecting the Access to Documents held by Public Bodies and the Protection of Personal Information* covers the remainder of the health sector.

Nova Scotia
Freedom of Information and Protection of Privacy Act, 1993, c. 5.

New Brunswick
Protection of Personal Information Act, 1998, c. P19.1.

Newfoundland/Labrador
Privacy Act, RSNL 1990 c. P22 and *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1 [not yet proclaimed].

Prince Edward Island
Bill 47, the *Freedom of Information and Protection of Privacy Act* received royal assent on May 15, 2001 but has not yet been proclaimed.

Northwest Territories
Access to Information and Protection of Privacy Act, SNWT 1994, c. 20.

Yukon
Access to Information and Protection of Privacy Act, SY 1995, c. 1.

Nunavut
Access to Information and Protection of Privacy Act(Nunavut)

Federal
Personal Information Protection and Electronic Documents Act, RSC 2000 c. 5. This Act applies to personal health information that is collected, used or disclosed by federal works, undertakings and businesses. Further, it applies to personal health information that is conveyed over provincial or national borders for consideration or value.

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 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:

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