College of Physiotherapists of Manitoba

PRACTICE DIRECTION

Current and updated as of: June 2, 2005

4.19 Retention and Transmission of Electronic Health Information

Purpose:
The use of electronic health information can have many benefits for health professionals and the clients to whom they provide service. Adequate safeguards are necessary to ensure confidentiality of electronic health information. It is the responsibility of all registered physiotherapists to be familiar with the content and implications of all laws applicable to safe, effective and ethical practice.

Policy:

I. Informed Consent

Physiotherapists need to obtain informed consent for the collection, use and disclosure of personal health information. It can be obtained in writing, verbally or by implied consent. Electronic storage and transmission of health information incurs some risks that should be disclosed to the client.

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.

II. Transmitting Electronic Health Information

Physiotherapists share responsibility and accountability with third parties to maintain the security and integrity of the electronic health information.

Consider the following guidelines when transmitting electronic health information:

i. Confirm the address of the recipient
ii. Use encryption
iii. Send an accompanying disclosure statement with all transmissions
iv. Have a disclaimer in place to protect oneself in the event that there is a breach in confidentiality by the recipient (see schedule A)

The advances in e-mail, Internet security, VPN's (virtual private networks) and encryption, which are often needed for financial transactions, are 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.

III. Maintaining an Integral Electronic Record System

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 Back-up Plan

The physiotherapist should ensure that electronic information is routinely "backed up" so that valuable information would not be lost if it were to become inaccessible (for example, due to data corruption or a fire in a facility).

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; and
e. Location of off-site data storage.

Physiotherapy client records must be maintained for a minimum of seven years after the date of the last entry. Records made while a client is a minor must be maintained until the client reaches the age of 25 years.

ii. Deleting Procedures

The physiotherapist must have policies and procedures in place to ensure the complete deletion of electronic health information. Physiotherapists should ensure that the database management system utilized actually deletes the electronic health information, rather than 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.

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

iii. Information/Physical Access Control

The physiotherapist must determine who has the ability to access and modify electronic health information. Access may be controlled through a password or through physical security measures.

Computer terminals should not be accessible nor screens viewed by unauthorized personnel or the general public.

iv. **Personnel Training and Security**

The physiotherapist must ensure that authorized and knowledgeable staff maintains the electronic health information. All staff, including IT service providers, should sign a Confidentiality Agreement.

v. **Security Configuration Management**

The physiotherapist updates hardware, software, and conducts maintenance reviews, when deemed appropriate, to keep the health information system safeguarded. This includes, but is not limited to, firewalls and anti-viral software.

vi. **Security Incident Procedures**

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 cyber crimes. In order for investigators to expose a system intruder's identity, they can follow the trail the intruder left in cyberspace.

The use of electronic health record often extends beyond the borders of a physiotherapist's clinical setting. Appropriate procedures must be in place to ensure both proper transmission and maintenance of electronic health record.

Excerpted from: Guideline for the Collection, Maintenance, Transmission and Destruction of Electronic Health Information June 2004
Canadian Alliance of Physiotherapy Regulators

Schedule A- Statement Accompanying Electronic Transmission of Health Information

Note: This is a sample form and is for discussion purpose 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 than 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.