Standards of Practice

Privacy and Record Retention

Standard

The physiotherapist maintains the privacy and confidentiality of health information and complies with the requirements of the *Health Information Act* (HIA), *Health Information Regulation* (HIR) and other privacy legislation relevant to their practice.

Expected outcomes

Clients can expect that:

- The physiotherapist will limit their collection of health information to that which is needed to provide physiotherapy services.
- Their health information is confidential and will be collected, used, and shared with the highest degree of anonymity possible.
- They will know when their health information is collected, who will have access to it, how it is used, how it is protected, and conditions for disclosure.
- Their consent for health information collection, access, use, and disclosure will be sought when required by the *Health Information Act*.

Performance expectations

The physiotherapist:

- Knows the privacy role they are assigned within their practice context, custodian or affiliate under the *Health Information Act*, and their role-related obligations and duties under the Act.
- Ensures that health information is under the custody and control of a custodian as defined in the *Health Information Act*.
- If serving as a custodian of health information under the *Health Information Act*
  - Retains responsibility and accountability for the actions of those whom they designate as their affiliates.
  - Establishes and enforces operating policies and procedures that adhere to the requirements of the *Act*.
- Retains full responsibility as a custodian of health information if they are employed by someone who is not a custodian, or if they have not been designated an affiliate of a custodian under the *Health Information Act*.

Confidentiality

- Protects the privacy of health information in all environments, regardless of the format of information collection.
- Is attentive to the physical environment during client assessment, treatment, and education and proactively addresses privacy risks including the risk of being overheard when discussing health information.

Collection

- Identifies the legal authority and authorized purpose(s) of health information collection at the time of collection.
- Collects only the relevant and necessary individually identifying health information required to provide physiotherapy services.

Consent

- Obtains client consent for the collection, access, use, and disclosure of health information when required by the *Health Information Act*, and in the format specified in the Act.

- Clearly discloses instances where audio or video recordings are generated in the practice setting.

Access and Amendment

- Accesses only relevant individually identifying health information when providing physiotherapy services for the client.
- Ensures processes for accessing or requesting corrections to health information are in place and are clearly communicated to clients.
- Provides or facilitates client access to a copy of the complete clinical and financial record upon request. If acting in the role of custodian, this includes
    - Providing the client's timely access to their health information
    - Disclosing health information to an individual acting on the client's behalf, with the client's written authorization.
    - Establishing fees for copies of health information that are consistent with the requirements of the *Health Information Act* and *Health Information Regulation*.
- If acting in the role of affiliate, follows the custodian's *Health Information Act* compliant procedures for access and disclosure.

Use and Disclosure

- Uses and discloses individually identifying health information for those purposes authorized by the *Health Information Act* which were identified at the time of collection, or with the client's consent.
- Discloses only the amount of individually identifying health information necessary to enable the recipient of the information to carry out the intended purpose. Provides aggregate or non-identifying health information when adequate for the identified purpose.
- Makes a reasonable effort to confirm that all correspondence with or regarding clients is sent to the intended recipient.
- Ensures that the use of individually identifying health information for research purposes complies with the requirements of the *Health Information Act*, including
    - the requirement for research ethics board approval and
    - adherence to any conditions imposed by the research ethics board.

Security

- Completes and submits a Privacy Impact Assessment before changing or implementing a health information management system or practice employed to collect, use or disclosure of individually identifiable health information.
- Employs appropriate administrative, physical, and technical safeguards to prevent unauthorized access, use, modification, disclosure, or destruction of health information throughout the health information lifecycle.
- Reports privacy breaches to the appropriate individual(s), and contributes to privacy breach investigation, mitigation, and remediation in accordance with organization policies, and role-based responsibilities.
- If acting as custodian of health information affected by a privacy breach,
    - performs a risk of harm assessment that considers all relevant factors,
    - notifies the privacy commissioner, the government minister responsible, and the individual when the risk of harm assessment confirms risk to the individual due to the privacy breach,
    - notifies the privacy commissioner immediately of a decision not to give notice to an individual in accordance with the provisions of the *Health Information Act*.
- Regularly assesses and modifies the safeguards in use to protect health information in their custody, addressing
    - the source of any privacy breaches that have occurred, and

- foreseeable threats or hazards to health information security

Retention

- Retains client clinical and financial records for ten (10) years after the last date of service.
    - Clinical and financial records for minors are retained for ten (10) years past the minor's 18th birthday.
- Retains health information in a manner that enables a complete copy or any component of the record to be retrieved and copied upon request, regardless of the media used to create or store the health information.
- Ensures contractual agreements are in place any time a third-party is engaged to process, store, retrieve, or dispose of health information or provide information technology services, and that the terms of the agreements comply with the requirements of the *Health Information Act* and regulations.
- Is responsible for compliance with the Act regardless of the contractual agreement with the third party.

Disposition

- Disposes of health information in a manner that maintains its privacy and confidentiality.
- Prevents abandonment of client records by designating a custodian or entering into a contract with an information manager to ensure the retention, accessibility, and security of client records in the event that the physiotherapist is unable to continue as custodian of client records.

If employed by someone who is not a custodian under the *Health Information Act*, the physiotherapist:

- Retains full responsibility as a custodian of health information if they are employed by someone who is not a custodian, or if they have not been designated an affiliate of a custodian under the *Health Information Act*.
- Informs the employer of the physiotherapist's legislated and regulatory obligations as a custodian of health information.
- Ensures that policies and procedures related to health information
    - comply with the requirements of the *Health Information Act* and regulations
    - are enacted in daily practice, and
    - that employer operational policies do not limit or interfere with the physiotherapist's ability to fulfill their legislated responsibilities.

Definitions

Abandonment of records: the act of leaving behind records without providing for their ongoing security and protection for the duration of the mandatory retention period. This occurs in instances where the physiotherapist fails to actively provide for the secure retention, ongoing access and appropriate destruction of records when leaving a practice or retiring, or fails to have contingency plans in place to address records management when faced with unexpected illness.

Health information: information related to a client's diagnostic, treatment, and care information or their registration information, as defined in the *Health Information Act*.

Health information lifecycle: refers to all stages of health information in the custody of control of the custodian from its collection, through use and storage, to its authorized destruction.

Individually identifying health information: health information related to an identifiable person