

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, the Act), Health Information Regulation (HIR, the Regulations), and other privacy legislation relevant to their practice.

Expected outcome

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 disclosed as authorized by the *Health Information Act* and 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 the disclosure of their health information will be sought when required by the *Health Information Act* or other applicable legislation.

Performance expectations

The physiotherapist:

- Knows that they are a **custodian** of health information and retains responsibility for health information in their custody or control unless they are acting as an **affiliate** in relation to a designated custodian.
- Knows and fulfills their role-related obligations and duties under the *Health Information Act*.
- Ensures that health information is always under the custody and control of a custodian as defined in the HIA.
- When in the role of custodian:
 - Retains responsibility and accountability for the actions of those who are their affiliates.
 - Establishes and enforces operating policies and procedures that adhere to the requirements of the Act.
 - Implements a Privacy Management Program consisting of privacy training and the custodian's policies and procedures, to facilitate adherence with the Act and its Regulations.

Confidentiality

The physiotherapist:

- 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

The physiotherapist:

- Provides clients with a collection notice that complies with the requirements specified in the *Health Information Act* when collecting health information directly from the client.
- Identifies the legal authority and authorized purpose(s) for health information collection, when collecting health information from another custodian.
- Collects only the relevant and necessary **individually identifying health information** required to provide physiotherapy services.

Consent

The physiotherapist:

- Obtains client informed consent for the disclosure of health information when required by the *Health Information Act*, in the format specified in the Act.
- Clearly discloses and obtains written consent for the use of devices used in the provision of physiotherapy services that may not be visible to the client to collect health information.

Access and amendment

The physiotherapist:

- Accesses only relevant individually identifying health information when providing physiotherapy services for the client.
- Ensures that processes for accessing or requesting corrections to health information are in place, comply with the requirements of the *Health Information Act*, and are clearly communicated to clients.

Continued on next page...

Continued from last page...

- Provides or facilitates client access to a copy of the complete clinical and financial record upon request, subject to provisions of the Act. If acting in the role of custodian, this includes:
 - Responding to requests for access within 30 days.
 - Providing access to health information to a duly authorized individual acting on the client's behalf, or with the client's written consent.
 - Establishing fees for copies of health information that are consistent with the requirements of the Act and Regulations.
- If acting in the role of affiliate, follows the custodian's HIA compliant procedures for access and disclosure.

Use and disclosure

The physiotherapist:

- Uses and discloses individually identifying health information for those purposes authorized by the *Health Information Act* and identified at the time of collection.
- When disclosure is not authorized by the Act, only discloses health information with the client's informed 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 Act, including:
 - The requirement for research ethics board approval,
 - Adherence to any conditions imposed by the research ethics board, and
 - Entering into a HIA-compliant research agreement.

Security

The physiotherapist:

- Completes and submits a Privacy Impact Assessment before changing or implementing a health information management system or practice employed to collect, use, or disclose individually identifiable health information, or when otherwise required by the *Health Information Act*.

- 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 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

The physiotherapist:

- 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 eighteenth (18) 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 Information Manager Agreements and Privacy Impact Assessments are in place any time a third-party is used 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.

Continued on next page...

Disposition

The physiotherapist:

- Disposes of health information in a manner that maintains the client's privacy and confidentiality.
- Prevents **abandonment of client records** by designating a successor custodian 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 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.

Related Standards

- Documentation

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.

Affiliate: as defined in Section 1(1)(a) of the *Health Information Act*, "affiliate", in relation to a custodian, means

- (i) an individual employed by the custodian,
- (ii) a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian,
- (iii) a health services provider who is exercising the right to admit and treat patients at an approved hospital under the *Provincial Health Agencies Act*,
- (iv) an information manager, and
- (v) a person who is designated under the regulations to be an affiliate,

An affiliate is granted access to the health information in the custody and control of a custodian by virtue of their status as the custodian's affiliate. They may only collect, use or disclose health information in accordance with their job-related duties to the custodian.

Custodian: a health services provider who is designated in the HIA or Health Information Regulation (HIR) as a custodian, or who is within a class of health services providers that is designated in the HIR. Custodians include health organizations such as hospitals and continuing care facilities, and regulated members of health professions designated custodians in the HIR.

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 or control of the custodian from its collection, through use and storage, to its authorized destruction.

Individually identifying health information: health information from which the identity of the individual who is the subject of the health information can be easily determined.