COLLEGE OF
PHYSIOTHERAPISTS
OF ALBERTA

HIA Policies and Procedures for Alberta Physiotherapist Custodians Manual

June 2026

COLLEGE OF
PHYSIOTHERAPISTS
OF ALBERTA

The College of Physiotherapists of Alberta regulates the practice of physiotherapy in Alberta. This guide has been developed to provide general information and practical advice for physiotherapists regarding privacy legislation.

The guide is not intended to provide or be a substitute for legal advice. Physiotherapists are advised to consult their own legal advisors for specific advice on privacy matters.

The information and advice in this guide is based on current legislation and is subject to change.

College of Physiotherapists of Alberta
300, 10357 - 109 Street, Edmonton, Alberta T5J 1N3
T 780.438.0338 | TF 1.800.291.2782 | F 780.436.1908
info@cpta.ab.ca | www.cpta.ab.ca

Contents

Background

Purpose

Registrants of the College of Physiotherapists of Alberta are custodians under the *Health Information Act* (HIA).

Individually identifying health information collected, used, stored, and disclosed by physiotherapists is governed by the HIA, with few exceptions. All physiotherapists are required to be familiar with and are individually responsible to comply with the requirements established by the Act.

Physiotherapists fulfill the role and responsibilities of custodian unless they have been formally designated as an affiliate to a custodian designated under the Act. See the Privacy Guide for Alberta Physiotherapists (2026) for more information about the roles of custodians and affiliates and requirements for designation as an affiliate to a custodian.

Physiotherapists who are custodians are required to develop, implement, and maintain HIA compliant policies and procedures for the management of health information as part of a broader Privacy Management Program that addresses training, oversight, risk management, and ongoing monitoring of the program and emerging privacy risks (HIA, Section 63).

The purpose of this document is to outline the policy and procedure requirements of the HIA and to provide guidance to physiotherapists as they review, revise, or establish HIA compliant privacy policies and procedures.

This is a companion document to the Privacy Guide for Alberta Physiotherapists (2026). Readers are advised to review the Privacy Guide prior to this document.

What About Netcare?

Being a custodian under the HIA is one precondition for physiotherapist eligibility to apply for access to the Alberta Netcare Portal.

Before gaining access to Netcare, physiotherapists must complete several additional steps, including the creation of HIA compliant policies and procedures. HIA compliant policies and procedures are required, even if a physiotherapist does not wish to pursue access to Alberta Netcare Portal.

This document is not a substitute for legal advice and is provided as a guide only.

Physiotherapists choosing to adopt the language in this guide in their own policies and procedures must understand what the policy says and how it applies to their practice. Physiotherapists are expected to adapt the wording to address their specific practice needs. In case of any doubt as to the proper application of the Act or when modifying the sample language provided in this document, physiotherapists are advised to consult with legal counsel or their organization's Privacy Officer to ensure that compliance with the requirements of the Act is maintained.

Definitions

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 as custodians.

Custodians are accountable to ensure that policies, procedures, and practices which comply with the requirements of the HIA are in place to protect individually identifying health information.

Custodians are responsible for ensuring that their affiliates comply with the requirements of the HIA and the HIA compliant policies and procedures the custodian has put in place to protect health information.

Sharing Custodians: when a group of custodians share custody of electronic health information (e.g., in the form of a shared electronic medical record), they are referred to as "sharing custodians". Sharing custodians must submit a PIA and must share common policies and procedures that address the requirements of the HIA and address shared custody of health information, including defining roles and responsibilities of the sharing custodians. See HIA Division 2- Shared Health Information for more information.

Affiliate: in relation to a custodian, means an individual employed by the custodian; a person who performs a service for a custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian; an information manager, or a person who is designated under the regulations to be an affiliate.

An affiliate is granted authority to collect, use, and disclose individually identifying health information by virtue of their relationship with the custodian and may only collect, access, use, or disclose health information in accordance with their role and relationship to the custodian.

The affiliate's actions are considered an action of the custodian.

The custodian retains ultimate responsibility for the protection of individually identifying health information.

Although the HIA identifies regulated members of the College of Physiotherapists of Alberta as custodians under the Act, there are times when the physiotherapist may work as an affiliate to a custodian. In such situations, the relationship between affiliate and custodian and their respective responsibilities and accountabilities must be clearly identified within the employment contract, job description, or other formal document. In cases where a physiotherapist employs support personnel, the support personnel must be designated as affiliates to the physiotherapist custodian.

Health Information: means one or both of the following:

- Diagnostic, treatment, and care information
- Registration information

Individually Identifying: when used to describe health information, means that the identity of the individual who is the subject of the information can be readily ascertained from the information.

Transitory record: a record that does not have long-term value. Contains individually identifying health information that is not required to meet legal, financial, or other obligations, and has no historical value. Examples include notes kept to prepare official documentation, duplicate documents, and working materials that are used to create a master record.

Roles and Responsibilities

Custodians must designate an individual to be responsible for compliance with the provisions of the HIA (i.e., to serve as the custodian's privacy officer).

Regardless of the appointment of the Privacy Officer, the custodian remains responsible for compliance with the HIA and remains a custodian under the Act with all the responsibilities of a custodian. If a group of health professionals designated as custodians under the HIA share custody of electronic health information, they must fulfill the requirements pertaining to shared health information and their designation as sharing custodians. Each custodian retains their responsibilities and accountabilities as a custodian.

Roles and authorities of the custodians, affiliates, and privacy officers must be defined in the position descriptions, employment contracts, and policies of the organization. Similarly, the routine practices the affiliate must follow must be defined in position descriptions, employment contracts, and operational policies and procedures.

See the Privacy Guide for Alberta Physiotherapists (2026) for more information about the roles of custodians, affiliates, and privacy officers, and requirements for designation as an affiliate to a custodian.

Policy and Procedure Requirements

Requirements

The HIA establishes the requirement that "A custodian must establish a privacy management program consisting of the policies and procedures the custodian establishes or incorporates to facilitate the implementation of this Act and the regulations." The purpose of the privacy management program is to ensure that custodians not only adopt privacy policies but also put them into practice through training, oversight, risk management, and ongoing monitoring.

The Privacy and Record Retention Standard of Practice requires that physiotherapists ensure that there are policies and procedures in place that address the requirements of the HIA.

A physiotherapist's individual responsibility for the creation and implementation of the privacy management program and related policies and procedures will depend on the setting in which the physiotherapist practices and the contents of employment agreements or other formal documentation in place between the physiotherapist and the practice setting owner.

For physiotherapists working for health organizations identified as custodians under the HIA (such as hospitals) HIA compliant policies and procedures should already exist. The physiotherapist's responsibility is to be familiar with and comply with the organization's policies and procedures and participate in privacy training that is part of the organization's privacy management program.

For physiotherapists working in private physiotherapy businesses, such as private practice clinics and mobile practices, a formal privacy management program and policies and procedures may or may not already exist. Existing programs and policies may not address the specific requirements of the HIA. Physiotherapists need to be aware of the HIA's requirements and are responsible to ensure policies and procedures are in place that address the requirements of the HIA.

How to use this document

This document is divided into sections consistent with the requirements of the HIA. Each section includes a brief description of the requirements of the legislation related to a given topic, followed by sample language that the physiotherapist custodian can use as a guide when developing their HIA policies and procedures. Several form templates are also provided.

Privacy Charter

A custodian must create a privacy charter which broadly defines its commitment to privacy and outlines, at a high level, the responsibilities of the custodian and their affiliates. The privacy charter serves to communicate the custodian's dedication to maintaining the privacy of health information to both affiliates and service users.

Key points to include in the charter are:

- The applicable privacy legislation (the HIA).
- The respective roles and responsibilities of the custodian, their affiliates, and the individual the custodian has designated to be responsible for compliance with the provisions of the HIA (e.g. the Privacy Officer).
- That privacy policies and procedures apply to the custodian and their affiliates.
- That privacy training is required for all custodians and affiliates who have access to individually identifying health information.
- The client's right to access and amendment of their client health records.

As part of developing a privacy charter, custodians are expected to identify their affiliates. Access to information by affiliates is based on whether the affiliate requires access to health information to fulfill their duties, and the extent of access to health information required (blanket access or access to a more limited set of health information).

Sample Policy and Procedure Content: Privacy Charter

Employees, volunteers, and students working at < XYZ Clinic > value the privacy of our clients. As designated custodians or affiliates subject to the *Health Information Act* (HIA), we take seriously our duties to protect health information and take all reasonable measures to safeguard the information in our custody and control or to which we have access.

Policies and procedures established by < Name of Custodian(s) > to protect health information apply to <XYZ Clinic> affiliates, including personnel affiliated with or subcontracted to <XYZ Clinic> and third-party contractors providing services on our behalf.

<XYZ Clinic>'s Privacy Officer, <first name, last name>, routinely assesses the risks to individually identifying health information, implements safeguards, conducts staff training to mitigate risks, and regularly reviews and updates privacy safeguards, policies and procedures in accordance with < Name of Custodian(s) >'s Privacy Management Program.

All <XYZ Clinic> custodians and affiliates have the responsibility to protect individually identifying health information during its collection, use, storage, and disclosure. We will collect and use the least amount of individually identifying health information necessary to fulfill the purpose for which the health information is collected and will employ physical, technical, and administrative measures to maintain its accuracy and security. Collection, access, use, and disclosure of individually identifying health information will only be completed by custodians and affiliates in the context of and within the limits of the individual's job responsibilities and duties.

<XYZ Clinic > custodians and affiliates will engage in routine training to ensure they are aware of policies, procedures, and safeguards in place to protect the privacy and accuracy of health information. Staff must comply with the requirements outlined in <Name of Custodian>'s policies and procedures and may be subject to sanction up to and including termination of employment if they do not comply with these requirements.

Clients have the right to request access to or correction of their health information. They also have the right to question how their individually identifying health information is protected. Clients with questions, concerns, or complaints regarding the <Name of Custodian> privacy practices at <XYZ Clinic>, or wishing to access or amend their health information are directed to the Privacy Officer, <name, address and business telephone number>.

Training

Custodians are required to train all individuals who collect, access, use or disclose health information in the custodian's custody and control in the privacy safeguards, policies, and procedures in place to manage and protect health information.

The custodian must identify the following components in their privacy training and awareness policy:

- Who will receive training?
- What content will be included?
- How frequently will training occur?
- How frequently will training be reviewed and updated to ensure currency?
- How is training tracked to ensure completion?
- The sanctions that apply to affiliates who do not comply with the custodian's policies and procedures or fail to employ the measures put in place to protect health information.

The training program must include the completion of confidentiality agreements by affiliates which include statements that:

- They will uphold to the best of their ability their duties under the *Health Information Act* and Regulations and the custodian's policies and procedures.
- They will not disclose or make known any individually identifying health information except as authorized by the Act, the Regulations and the custodian's policies and procedures.

The agreement must be signed and dated by both the employee and a witness. See Form 01 for a sample Employee Confidentiality Agreement.

For additional guidance about the content to include in training programs, see Appendix 3 of the Health Information Act Guidelines and Practices Manual.

Sample Policy and Procedure Content: Training

Prior to receiving access to individually identifying health information, <Name of Custodian> and their affiliates at <XYZ Clinic> will complete privacy training. Training will include instruction in the following topics:

- The *Health Information Act*.
- <Name of Custodian>'s policies and procedures regarding collection, use, disclosure, and disposition of individually identifying health information.
- Security of individually identifying health information including:
    - Physical, technical, and administrative safeguards in use.
    - Mandatory compliance with safeguards to prevent privacy breaches.
    - Policies regarding routine auditing and monitoring of access, use, disclosure, and disposition of individually identifying health information.
- Authorized purposes for collection and use of individually identifying health information.
- Processes for access and amendment of individually identifying health information.
- Fees for access to copies of individually identifying health information.
- Privacy requirements for third party providers including information technology system providers and information managers.
- Policies and procedures related to responding to and reporting privacy breaches, including roles and duties of affiliates, custodians, and <Name of Custodian>'s Privacy Officer.

Training will occur at the time of hire, and annually or any time <Name of Custodian> implements new, or significantly changes existing information handling practices or systems, or adopts new safeguards.

<Name of Custodian>'s Privacy Officer is accountable to monitor emerging risks to health information, implement reasonable safeguards to mitigate those risks and train staff in their implementation. The Privacy Officer will retain training records, including lists of attendees and content of training sessions.

<XYZ Clinic> custodians and affiliates will be granted access to individually identifying health information according to their employment role, to the extent necessary to fulfill their job-related duties. Role-based access controls, policies, and procedures are in place to prevent unauthorized access or use of individually identifying health information. Sanctions for failure to comply with privacy policy and procedures, up to and including termination of employment, are enforced by <Name of Custodian> and are reviewed during privacy training.

Privacy and confidentiality agreements will be completed or updated during privacy training.

Collection

Collection notices inform clients why the custodian is collecting health information.

The custodian is required to identify and make available a collection notice that indicates the authority under which health information is collected and the purposes for which that health information will be used. Custodians must collect health information from the individual who is the subject of the health information unless specific circumstances apply to the situation (HIA, Section 22(2)).

Custodians must identify their legislated authority to collect health information and the authorized purposes for which health information is being collected, at the time of collection. Consent is not required for the collection of health information for purposes that are authorized under the Act. However, custodians must have clearly defined and defensible reasons for collecting individually identifying health information.

Organizational policies and procedures must include the following content:

- The statutory authority to collect individually identifying health information (HIA, Section 20).
- The HIA authorized purposes for which individually identifying health information is collected, specific to the organization's operational activities (HIA, Section 27).
- That individually identifying health information will be collected from the client who is the subject of the health information or the specific circumstances when health information may be collected from someone other than the client (consistent with HIA Section 22(2)).
- That the least necessary information will be collected to fulfill the identified purpose(s).
- Samples of the collection notice and other notification methods that will be employed to inform clients about the collection of individually identifying health information.

The organization's collection notice must include the following content:

- Why individually identifying health information is collected.
- The specific legal authority to do so.
- The contact information of the individual (i.e., custodian or Privacy Officer) the client can speak to if they have questions.
- How the confidentiality of collected information and the client's privacy is protected.
- Whether the client's health information will be entered into an automated system (e.g., AI scribe tool, AI decision support tool).

Sample Policy and Procedure Content: Collection

Note: This sample collection statement includes a list of all purposes authorized under Section 27 of the Act. A custodian may choose not to collect and use individually identifying health information for all the purposes authorized under the Act.

However, the custodian must identify the purposes for which health information is collected in the collection statement. If the collection statement does not identify an authorized purpose as a reason for which individually identifying health information is collected, at the time of collection, the custodian may not later use individually identifying health information for this purpose without gaining client consent to do so.

<Name of Custodian> and their affiliates at <XYZ Clinic> collect individually identifying health information in compliance with and under the authority of Section 20(2) of the *Health Information Act* and consistent with the purposes identified in Section 27 of the Act and identified in <Name of Custodian>'s Collection Notice.

When collecting individually identifying health information, <Name of Custodian> and their affiliates at <XYZ Clinic> will collect information from the individual who is the subject of the information unless the individual is unable to provide information or authorizes collection from a different source. <Name of Custodian> and their affiliates at <XYZ Clinic> will collect the least amount of individually identifying health information necessary to fulfill the purposes identified.

Sample Collection Notice

Your health information is collected through <form name, website, program, service> by <Name of Custodian> and their affiliates at <XYZ Clinic> under the authority of Section 20(2) of the *Health Information Act* and for purposes identified in Section 27 of the Act, including:

- Providing health services
- Determining or verifying eligibility to receive a health service
- Conducting investigations, discipline proceedings, practice visits or inspections relating to the members of a health profession or health discipline
- Conducting research or performing data matching or other services to facilitate another person's research
- Providing for health services provider education
- Carrying out any purpose authorized by an enactment of Alberta or Canada
- For internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management

[Note: modify the above list according to current and anticipated uses of health information within the practice setting.]

The health information collected by <Name of Custodian> and their affiliates at <XYZ Clinic> through <form name, website, program, service> is entered into and processed by <Name of automated system> for the purpose of <specify purpose>.

The confidentiality and privacy of the health information collected by <Name of Custodian> and their affiliates at <XYZ Clinic> is protected by the provisions of the *Health Information Act* and measures put in place by <XYZ Clinic>'s custodian, <Name of Custodian>. If you have any questions about the collection, use, and security of individually identifying health information, please contact <XYZ Clinic>'s Privacy Officer, <name, address and business telephone number>.

Consent and Disclosure

Note: For the purpose of this document, the term consent refers to permission to collect, use, or disclose individually identifying health information and does not refer to clinical consent, such as consent for assessment or treatment of a health condition.

Consent is not required for collection, use or disclosure of health information for purposes authorized under Section 27 of the Act and identified at the time of collection of the health information.

The *Health Information Act* allows for disclosures of individually identifying health information to other custodians under the Act, for purposes identified in the Act without the consent of the individual who is the subject of the information. When disclosing health information to other custodians for purposes authorized under the Act, the custodian making the disclosure must consider any expressed wishes of the client who is the subject of the health information regarding disclosure of that information.

Disclosures not authorized by the Act require consent of the individual who is the subject of the information, in the format specified in Section 34 of the Act.

Custodians are required to retain records of all disclosures of individually identifying health information, whether authorized under the Act or disclosed with the subject's consent. Subjects of individually identifying health information in the custody and control of a custodian have the right to access these disclosure records.

Excluded Services and Consent

Section 3.1 of the HIR identifies services which are excluded from the definition of a health service under the HIA. If health information is collected, used, or disclosed for the provision of an excluded service, the information is subject to the requirements of other privacy legislation applicable to the organization or practice setting (e.g., PIPA, POPA), including applicable consent requirements. For more information see Appendix 1 of the Privacy Guide for Alberta Physiotherapists (2026).

Express Consent Requirements

Section 34 of the Act specifies that consent for disclosures not authorized by the Act must include:

- Authorization for the custodian to disclose the individually identifying health information
- Specification of which information is included in the consent (what information will be disclosed)
- The purpose for which the individually identifying health information may be disclosed
- The identity of the person to whom the information may be disclosed
- Acknowledgement that the individual providing consent has been made aware of the reasons for the disclosure and the risks and benefits of consenting or refusing to consent
- The date the consent is effective, and the date consent expires (if any)
- A statement that the consent may be revoked at any time by the person providing it

See Form 02 Consent for Disclosure of Health Information.

Consent may be obtained in writing, electronically, or verbally. If consent is provided electronically, it is only valid if there is a reliable method to verify the individual providing consent.

Verbal Consent for Disclosure of Health Information

When obtaining verbal consent for disclosure of health information, the consent is only valid if:

- The custodian's privacy management program includes:
  - Provisions for verbal consent for disclosure,
  - The purpose for which verbal consent for disclosure may be sought, and
  - The process of obtaining verbal consent.
- Verbal consent is obtained for a purpose identified in the privacy management program
- The custodian verified the identity of the person providing consent using a reliable method

A record of the verbal consent for disclosure must be retained for 10 years.

Consent for Marketing Purposes

Telecommunications information, such as telephone numbers and email addresses, is classified as registration information and is protected under the HIA. The HIA explicitly prohibits the use of health information for marketing purposes,

"No person may knowingly use individually identifying health information to market any service for a commercial purpose or to solicit money unless the individual who is the subject of the health information has specifically consented to its use for that purpose." (HIA, Section 107(2)(f))

As such, custodians who engage in marketing activities must have express consent to use individually identifying health information (registration information) for marketing purposes.

Disclosure Policy and Procedure Content Requirements

A custodian's policies and procedures related to disclosure must include the following content:

- The statutory authority under which individually identifying health information is disclosed.
- That aggregate or de-identified information will be disclosed, if such disclosure is sufficient to fulfill the identified purpose.

- That the least necessary information will be disclosed to fulfill the identified purpose.
- That the custodian will make a reasonable effort to ensure that disclosures of health information are made to the person intended and authorized to receive the information.
- That disclosure without consent from the individual who is the subject of the information is authorized under the Act when:
  - The disclosure is to another custodian under the Act, for purposes authorized in Section 27 of the Act
  - The disclosure is for another authorized purpose identified in Section 35 of the Act
- In deciding how much information to disclose, the custodian will take into consideration any expressed wishes of the client in relation to the disclosure of the client's health information when disclosure is authorized by the Act.
- That consent will be obtained from the subject of the individually identifying health information for disclosures that are not authorized under the Act.
- That the custodian will maintain detailed records of disclosures.
- That the custodian will notify recipients of individually identifying health information of the purpose of the disclosure and the authority under which the disclosure was made when the recipient is not a custodian under the Act.
- That the custodian will notify recipients of individually identifying health information that they must not use the health information for direct commercial marketing or fundraising purposes, or for a purpose that differs from the purposes identified at the time the disclosure was made, without the specific consent of the subject of the health information.

Consent Policy and Procedure Content Requirements

When disclosure of individually identifying health information is not authorized under the Act, express consent from the person who is the subject of the information is required.

Consent policies and procedures must include a description of:

- Any services which are excluded from the definition of a health service under the HIA, and the legislation and consent requirements applicable to those services.
- The process for obtaining consent for disclosure of health information (when disclosure is not authorized by the HIA) and the custodian's format and content requirements for that consent.
- Conditions related to verbal consent for disclosure of information (e.g., when the custodian will accept verbal consent for disclosure), required content of verbal consent discussions, and documentation requirements.
- The process by which consent for use of registry information for marketing purposes will be sought (if applicable).

Sample Policy and Procedure Content: Consent and Disclosure of Health Information

<Name of Custodian> and their affiliates at <XYZ Clinic> collect, use and disclose individually identifying health information in compliance with and under the authority of the *Health Information Act* (HIA). <Name of Custodian> and their affiliates will disclose the least amount of information possible to fulfill the identified purpose for the disclosure, disclosing aggregate or de-identified health information whenever possible.

<Name of Custodian> and their affiliates at <XYZ Clinic > will make every effort to transparently communicate the authorized purposes for which health information is collected, used and disclosed by the clinic, and for which consent is not required under the HIA.

As authorized by the Act, individually identifying health information will be disclosed without the subject's consent to other custodians, for the authorized purposes identified by Section 27 of the Act, which include:

- Providing health services
- Determining or verifying the eligibility of an individual to receive a health service
- Conducting investigations, discipline proceedings, practice visits or inspections relating to the members of a health profession or health discipline
- Conducting research or performing data matching or other services to facilitate another person's research
- Providing for health services provider education
- Carrying out any purpose authorized by an enactment of Alberta or Canada
- For internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management

[NOTE: Edit the list of authorized purposes to be consistent with those engaged in by the organization.]

When disclosing health information in accordance with Section 27 of the Act, <Name of Custodian> and their affiliates at <XYZ Clinic > will take into consideration the expressed wishes of the client regarding disclosure of their health information and will balance the expressed wishes of the client (when applicable) and the need for disclosure for an authorized purpose.

<Name of Custodian> and their affiliates at <XYZ Clinic > will make a reasonable effort to ensure that a disclosure of health information is made to the person intended and authorized to receive the information.

Disclosure for a purpose not authorized under the Act, or for a purpose that was not identified at the time of collection will only occur with the consent of the individual who is the subject of the information. Consent will be obtained in in accordance with the requirements of Section 34(2) of the Act, using <Name of Custodian>'s Consent for Disclosure of Health Information Form.

<Name of Custodian> and their affiliates will verify the identity of the individual providing consent.

If consent cannot reasonably be obtained using written or electronic methods, <Name of Custodian> and their affiliates will accept verbal consent for disclosure of health information for <identified purpose> provided that:

- The procedure for obtaining verbal consent outlined in this policy and in privacy training is followed
- The identity of the individual providing consent is verified using a reliable method
- The consent discussion includes the required elements:
  - Authorization for the custodian to disclose the individually identifying health information
  - Specification of which information is included in the consent (what information will be disclosed)
  - The purpose for which the individually identifying health information may be disclosed
  - The identity of the person to whom the information may be disclosed
  - Acknowledgement that the individual providing consent has been made aware of the reasons for the disclosure and the risks and benefits of consenting or refusing to consent
  - The date the consent is effective, and the date consent expires (if any)
  - That the consent may be revoked at any time by the person providing it

<Name of Custodian> and their affiliates at <XYZ Clinic > will maintain detailed records of disclosures of individually identifying health information, including the name of the individual to whom the information was disclosed, the date of disclosure, and a description of the information disclosed, as required by Section 41(1) of the Act. <Name of Custodian> and their affiliates, will retain a record of the verbal consent for disclosure for 10 years. The subject of the individually identifying health information may request access to these disclosure records by completing <Name of Custodian>'s Access Form.

When <Name of Custodian> and their affiliates at <XYZ Clinic > disclose individually identifying diagnostic, treatment and care information to another party who is not a custodian under the Act, they will inform the recipient in writing of the purpose of the disclosure, and that the disclosure was made under the authority of the *Health Information Act*. In accordance with Section 107(2), recipients will be informed that they must not use the health information for direct commercial marketing or fundraising purposes, or for a purpose that differs from the purposes identified at the time the disclosure was made without the specific consent of the subject of the health information.

Consent for Marketing Purposes

Express, written consent will be obtained prior to the use of individually identifying health information (including registration information) for marketing activities.

Consent for Services Excluded from the HIA Definition of a Health Service

If <Name of Custodian> and their affiliates at <XYZ Clinic > provide services identified in Section 3.1 of the HIR, such as <identify service>, prior to engaging in the collection of health information or provision of the excluded service, <Name of Custodian> and their affiliates at <XYZ Clinic > will identify the privacy legislation applicable to the information and obtain consent consistent with the requirements of the applicable legislation.

Use

Under the HIA, "use" of information encompasses the application of health information (diagnostic treatment and care information and registration information) for any purpose authorized in Section 27 of the Act, including reproduction of information. Use also includes appropriate and controlled access to and application of individually identifying health information by affiliates of a custodian for purposes authorized by the Act and in accordance with the affiliate's duties to the custodian. When one custodian shares health information with another custodian for the purpose of providing care and treatment to the individual who is the subject of the health information, the action is considered disclosure, not use.

Custodians may use non-identifying health information for any purpose.

Consent is not required for use of individually identifying health information for purposes that are authorized under the Act. However, custodians and their affiliates must have clearly defined and defensible reasons for how individually identifying health information is used.

Privacy policies and procedures must include the following content:

- The statutory authority under which individually identifying health information is used (HIA Section 27).
- The authorized uses of individually identifying health information, consistent with the provisions of the Act and specific to the custodian's intended use(s) of the information and collection notice.
- That the least necessary information will be used to fulfill the identified purpose.
- That consent will be obtained from the subject of individually identifying health information for uses that are not authorized under the Act, identifying the legislation that applies to the identified use.

Sample Policy and Procedure Content: Use

<Name of Custodian> and their affiliates at <XYZ Clinic > use individually identifying health information in accordance with the provisions of Section 27 of the *Health Information Act*.

<Name of Custodian> and their affiliates at <XYZ Clinic > use individually identifying health information for the purposes of:

- Providing health services
- Determining or verifying the eligibility of an individual to receive a health service
- Conducting investigations, discipline proceedings, practice visits or inspections relating to the members of a health profession or health discipline
- Conducting research or performing data matching or other services to facilitate another person's research
- Providing for health services provider education
- Carrying out any purpose authorized by an enactment of Alberta or Canada
- For internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management

[NOTE: Edit the list of authorized uses to be consistent with those engaged in by the custodian.]

<Name of Custodian> and their affiliates at <XYZ Clinic > will identify all anticipated and authorized uses of individually identifying health information at the time of collection and will use the least amount of information necessary to fulfill the purposes identified.

<Name of Custodian> and their affiliates at <XYZ Clinic > will access and use individually identifying health information solely for the purpose of fulfilling their work-related responsibilities and for uses identified above which are applicable to their employment role. <Name of Custodian> employs role-based access controls, policies and procedures to prevent unauthorized access and use of individually identifying health information.

<Name of Custodian> and their affiliates at <XYZ Clinic > will obtain express consent if seeking to use individually identifying health information for purposes not identified at the time of collection. <Name of Custodian> and their affiliates at <XYZ Clinic >will also obtain written client consent prior to using individually identifying health information for marketing activities or for other uses not authorized by the *Health Information Act*.

If seeking consent for use of individually identifying health information, such consent will adhere to the requirements identified in the *Health Information Act*.

Non-identifying health information may be used for any purpose, without client consent, as authorized by the *Health Information Act*.

Access or Amendment

An individual who is the subject of individually identifying health information (e.g., the client) "has a right of access to any record containing health information about the individual that is in the custody or under the control of a custodian." (HIA, Section 7(1))

The Act also provides individuals with the authority to request a correction or amendment to the individually identifying health information in a custodian's custody and control (HIA, Section 13(1)).

Custodians must have policies and procedures in place to respond to requests for access, correction, or amendment of individually identifying health information.

Custodian policies regarding access to an individual's own health information must include:

- The identity and contact information of the individual to whom requests are to be made (e.g., the organization's Privacy Officer).
- Any forms individuals are required to use to request access to individually identifying health information (see Form 3).
- Timelines for responding to a request, consistent with the provisions of the HIA.
- Any fees for access to copies of records of individually identifying health information.
- How access to health information is to be documented; including documentation of the access request, date of the request, whether access was granted.

Custodian policies regarding correction or amendment to an individual's own health information must include:

- How requests for routine, informal amendments will be managed (e.g., address updates).
- Any forms individuals are required to use to formally request an amendment of individually identifying health information (see Form 4).
- The identity and contact information of the individual to whom formal requests for amendments are to be made (e.g., the custodian's Privacy Officer).
- Timelines for responding to a request.
- Options available to the individual requesting the amendment, if the custodian declines the request.
- How requests for correction or amendment are to be documented; including documentation of the request, date of the request, whether the correction or amendment was made.
- That requests for amendment of a professional opinion will be declined.

Sample Policy and Procedure Content: Access

<Name of Custodian> and their affiliates at <XYZ Clinic > collect, use and disclose individually identifying health information in accordance with the provisions of the *Health Information Act*. <Name of Custodian> and their affiliates at <XYZ Clinic > also generate and retain records regarding the disclosure of individually identifying health information in <Name of Custodian>'s custody and control. Individuals who are the subject of information that is in the custody and control of <Name of Custodian> have the legislated right to access their individually identifying health information, and records regarding the disclosure of that information.

Requests for access must be made in writing, using <Name of Custodian>'s Access Application Form, and forwarded to <Name of Custodian>'s Privacy Officer, <First Name, Last Name, contact information>.

<Name of Custodian> and their affiliates at <XYZ Clinic> will make every reasonable effort to assist individuals requesting access to individually identifying health information or records related to disclosure of individually identifying health information in the custody and control of <Name of Custodian> and to respond to each applicant openly, accurately and completely, within 30 days of receiving the request in writing.

<Name of Custodian> will provide applicants with the opportunity to examine the record, in the presence of the Privacy Officer or their appointee, with no charge.

Applicants requesting a copy of their health record will be charged a fee, consistent with the fees specified in the Health Information Regulation (Section 9 and Schedule). Estimates of the applicable fees will be provided to the applicant before the record is prepared.

Sample Policy and Procedure Content: Correction or Amendment

<Name of Custodian> ensures that the individually identifying health information in their custody and control is as accurate, complete, and current as reasonably possible. Individuals who are the subject of information that is in the custody and control of <Name of Custodian> have the legislated right to request correction or amendment of that information.

Amendment to registration information (e.g., street address, telephone number, email address) will be managed informally. <Name of Custodian> and their affiliates at <XYZ Clinic > will amend registration information, upon receipt of a verbal request and confirmation of the identification of the individual making the request.

Individuals who are the subject of individually identifying health information may make a formal request for correction or amendment of their individually identifying health information in the custody and control of <Name of Custodian>. Requests must be made in writing, using <Name of Custodian>'s Amendment of Health Information Form. The request must specify the information in the custody of control of <Name of Custodian> and the requested amendment. Requests must be submitted to <Name of Custodian>'s Privacy Officer, <First Name, Last Name, Contact Information>.

All requests will be reviewed and a written response to the request will be provided to the individual requesting the correction or amendment within 30 days of receiving the request.

If <Name of Custodian> agrees to the amendment, it will be made within 30 days of receiving the request and <Name of Custodian>'s Privacy Officer will provide written notice of the amendment, in accordance with the requirements of the Health Information Act within this period.

If <Name of Custodian> refuses the request, they will:

- Notify the individual requesting the amendment within 30 days of receiving the request
- Provide written reasons for the refusal
- Notify the individual of their legislated options for further action as outlined in Section 14(1) the *Health Information Act*

<Name of Custodian> will not amend professional opinions or observations made by a health service provider regarding the individual who is the subject of the individually identifying health information in question.

When <Name of Custodian> amends individually identifying health information related to a diagnosis or treatment already rendered, they will do so in a manner that retains the information upon which that diagnosis or treatment was generated or provided.

Research

The *Health Information Act* includes provisions enabling the use of individually identifying health information in a custodian's custody and control for research purposes undertaken by the custodian or to facilitate another person's research. The HIA defines research as "academic, applied or scientific research that necessitates the use of individually identifying health information." When custodians employ health information for internal management purposes, such as quality improvement, monitoring, audit, or evaluation, it is considered use of health information, not research.

Any use or disclosure of health information for research purposes must be conducted in a manner consistent with the requirements of the HIA, Sections 27(d), and Division 3. These requirements include:

- Submitting a proposed research protocol to a research ethics board
- Obtaining approval from the research ethics board related to the matters referred to in Section 50(1)(b) of the HIA
- Compliance by the custodian or researcher with any conditions suggested by the research ethics board
- Obtaining consents from the individuals who are the subjects of the health information to be used in the research, if the research ethics board recommends that consents be obtained

Despite these provisions, custodians are not required to engage in research activity or grant access to health information for the purpose of research. In addition, a custodian may impose other conditions on a researcher as a condition of granting access to individually identifying health information in the custodian's custody and control.

If a custodian is engaging in research activities or supporting another person's research, they must identify this as a reason for their collection, use and disclosure of individually identifying health information at the time of collection.

Key points to consider:

- De-identified or aggregate health information may be used for any purpose identified under the Act.
- Prior to disclosing health information, the researcher must enter into an agreement with the custodian, consistent with the provisions of Section 54 of the HIA, which include:
  - That the researcher will comply with the HIA.
  - Outlining the custodian's conditions for use, protection, disclosure, return or disposal of the health information.
  - Specifying that the health information will ONLY be used for conducting the research described in the approved research protocol.
  - Granting the custodian access to the researcher's premises to confirm that the researcher is complying with the legislation and the conditions and requirements the custodian imposed.

The custodian's policies and procedures must identify:

- The process by which the custodian will consider and approve requests related to research activities.
- The requirement that the research protocol be submitted to and receive approval of a research ethics board.
- The requirement to comply with any directions or conditions of the research ethics board, including obtaining consent when deemed necessary by the research ethics board.
- The requirement that a formal research agreement between the custodian and the researcher be in place, consistent with the requirements outlined in Section 54 of the Act.

See Form 5 - Sample Research Disclosure Application and Form 6 - Research Agreement Checklist.

Sample Policy and Procedure Content: Research

Requests for access to health information for research purposes are to be sent to

<Name of Custodian>'s Privacy Officer <first name, last name, contact information> for consideration.

The request must be made in writing, using <Name of Custodian>'s Research Disclosure Form and accompanied by copies of the proposed research protocol and the research ethics board letter of approval, if the application involves use of individually identifying health information.

Research requests will be considered on a case-by-case basis.

<Name of Custodian> will only consider requests for disclosure of individually identifying health information for research purposes which have been reviewed by and have received approval from an appropriate health research ethics board.

Researchers are required to agree to and comply with the stipulations of <Name of Custodian>'s Research Agreement. No health information will be released without a countersigned research agreement in force.

If, in the opinion of the health research ethics board, the researchers are required to obtain consent from the subject of the individually identifying health information prior to its release, <Name of Custodian> will facilitate the consent process. The researcher will be required to compensate <Name of Custodian> for the costs of undertaking the consent process on behalf of the researcher. No individually identifying health information will be released without consent from the individuals who are the subject of the health information, if consent is deemed necessary by the health research ethics board.

Researchers must employ the physical, technical, and administrative safeguards specified by <Name of Custodian> when individually identifying health information is in the custody and control of the researcher.

Researchers are required to grant access to the researcher's premises to <Name of Custodian> or their Privacy Officer at any time and without notice so that <Name of Custodian> can confirm that the researcher is complying with the legislation, and the conditions of <Name of Custodian>.

If a researcher contravenes the Research Agreement or fails to comply with the Act or conditions established by the health research ethics board, the Research Agreement will be cancelled. Under this circumstance, the researcher is no longer authorized to use health information for any purpose and must destroy or return the health information to <Name of Custodian>.

Researchers are required to return individually identifying health information to <Name of Custodian> at the conclusion of the research or upon termination of the research agreement and must certify that any copies of individually identifying health information have been securely destroyed or de-identified.

Storage and Disposition

Custodians are required to prepare privacy impact assessments (PIAs) for administrative practices and information systems employed in relation to the collection, use and disclosure of individually identifying health information (HIA, Section 64). The purpose of the PIA is to identify risks to health information arising from the administrative practice or information system and the safeguards required to mitigate those risks.

Custodians are required to implement safeguards to protect the health information in their custody and control. Safeguards must include physical, technical and administrative safeguards which address foreseeable risks to privacy. Such risks may include:

- Unauthorized use of individually identifying health information by internal parties
- Unauthorized collection/use/disclosure of individually identifying health information by external parties
- Loss of integrity of individually identifying health information
- Loss, loss of use, or destruction of individually identifying health information
- Collection, use, or disclosure of individually identifying health information by a contractor or business partner in contravention of the HIA or the organization's policies

Succession Planning

Custodians are required to proactively plan for career transitions including moves from one practice setting to another and the end of their physiotherapy practice, including retirement and unforeseen illness or incapacity, by:

- Ensuring contractual agreements specify:
  - That the physiotherapist will remain custodian of health records upon their departure from a practice setting, and
  - Specifying the methods by which clients will be made aware of the location of their health information,

OR

- Identifying and entering into a formal, contractual agreement with an eligible successor custodian who agrees to take over custody of the health information when the need arises,

AND

- Arranging for secure storage and eventual disposal of client records.

In order to be eligible to be a successor custodian under the HIA, the individual or organization taking on the role must be designated as a custodian under the HIA, in accordance with Section 1(1)(f) of the HIA or Section 2 of the HIR.

Succession planning ensures that:

- Client records remain protected for the full retention period.
- Individuals can continue to request access to their health records.
- Individuals know who to contact to request access.

Physiotherapists are advised that if they cease to be a registrant of the College of Physiotherapists of Alberta, they are no longer a custodian of health information in accordance with Section 2(2) of the HIR, and must designate an eligible successor custodian to fulfill responsibilities under the HIA.

Third-Party Contractors

Custodians are required to ensure that any third-party contracted to provide information management or other services to the custodian has the required safeguards in place to maintain the security and integrity of individually identifying health information.

See Contracting with Service Providers on page 29 for more information about requirements.

The custodian's policies and procedures must include:

- The custodian's standard for documentation of individually identifying health information, including expectations regarding transitory records, if the organization employs transitory records
- How the custodian classifies and handles different types of information
- The safeguards used to protect information according to its classification, including physical, technical and administrative safeguards
- The frequency with which safeguards will be reviewed and updated according to new and emerging risks
- The duration for which individually identifying health information is retained, consistent with the requirements of the Standards of Practice
- How individually identifying health information will be securely destroyed at the end of the retention period
- That the custodian and their affiliates will create and retain logs of records destroyed
- How compliance with policies and procedures will be monitored, and what situations/triggers would result in a formal audit of records and review of effectiveness of safeguards
- The requirement to complete or amend a privacy impact assessment whenever the organization considers a significant change to how it collects, uses, stores or disposes of individually identifying health information (e.g., change in routine practices, implementation of a new electronic medical record system, or contract with a new information manager).
- The frequency with which privacy impact assessments will be reviewed and amended to reflect emerging risks and changes to routine practices.
- The identification of the custodian's successor custodian and the routine review of successor custodian arrangements.

Sample Policy and Procedure Content: Storage and Disposition

<Name of Custodian> and their affiliates at <XYZ Clinic > generate records of client health information that contain content consistent with their role and the expectations articulated in the Standards of Practice for Physiotherapists in Alberta (2026). The health information contained in records in <Name of Custodian>'s custody and control will be categorized as either:

- Diagnostic, treatment, and care information
- Registration information

<Name of Custodian> and their affiliates at <XYZ Clinic > will be granted access to individually identifying health information appropriate to their role and work duties and will be granted access to the least information necessary to fulfill their role.

<Name of Custodian> will complete and submit for review by the Office of the Information and Privacy Commissioner, a privacy impact assessment (PIA) for each administrative practice or information system used to collect, use, or disclose individually identifying health information prior to implementing the administrative practice or information system, or for any significant changes to the administrative practice or information system.

The purpose of the privacy impact assessment is to identify and address the privacy risks associated with the administrative practice or information system through the implementation of reasonable safeguards that address those risks.

Health information will be protected from unauthorized access, use, alteration or destruction through the use of physical, technical, and administrative safeguards. Custodians and affiliates will complete annual training in the privacy risks to health information and use of safeguards to protect health information.

<Name of Custodian> will enter into contracts with any party contracted to provide information management or information technology services to the custodian to ensure that the security and integrity of individually identifying health information is maintained. Formal agreements will:

- Specify that <Name of Custodian> retains control over the health information.
- Enable <Name of Custodian> to monitor compliance with the terms and conditions of the agreement.
- Identify the responsibilities of each party.
- Include the requirement that contract holders adhere to the requirements of the HIA and <Name of Custodian>'s policies and procedures.
- Contain remedies to address issues of non-compliance or breach of the terms and conditions of the agreement.

Risks to health information in the custody and control of <Name of Custodian> will be reviewed when emerging risks are identified or at a minimum annually, or when changes to administrative practices or information systems occur. Safeguards will be updated according to the risks identified through the review. A privacy impact assessment amendment will be submitted to the Office of the Information and Privacy Commissioner when required.

In accordance with the HIA and the requirements established by the College of Physiotherapists of Alberta, <Name of Custodian> will retain individually identifying health information for a minimum of 10 years from the last date of service, or 10 years from the 18th birthday in the case of a client who received physiotherapy services as a minor. Individually identifying health information may be retained for a longer period if there are regulatory, business, or legal reasons to do so.

At the conclusion of the retention period, <Name of Custodian> will destroy records in its custody and control using secure measures, ensuring that individually identifying health information stored electronically is both deleted and purged from digital storage media. <Name of Custodian> will retain logs of records destroyed which identify the unique identity of the individual who is the subject of the information, the nature of the information and the date range of the information destroyed.

<Name of Custodian>'s Privacy Officer <first name, last name> will monitor compliance with policies, procedures and safeguards designed to protect the privacy of individually identifying health information in<Name of Custodian>'s custody and control on an ongoing basis and will engage in random audits on no less than a quarterly basis. If a privacy breach is discovered through routine monitoring of compliance and auditing, the Privacy Officer will follow <Name of Custodian>'s breach reporting policies and procedures to investigate and determine what further action is required.

Succession Plans

<Name of Custodian> has arranged for <Name of Successor Custodian> to serve as successor custodian of client records, should the need for a successor custodian arise (e.g., transition to a new practice setting, leave of absence, retirement, in the event of an unforeseen illness or incapacity).

<Name of Successor Custodian> is eligible to fulfill the role of successor custodian by virtue of their designation in accordance with <Section ## of the Health Information [Act or Regulation]>.

Should <Name of Custodian> leave <Name of Practice Setting>, they will employ client registration information on file for the purpose of notifying clients of the location of their health information and arrangements made for the storage and disposition of that health information, including the name of the successor custodian and methods available to contact the successor custodian should the need arise (if applicable).

Breach Reporting

A loss of, unauthorized access to, or disclosure of individually identifying health information constitutes a privacy breach.

Affiliates of a custodian are required to notify the custodian of privacy breaches as soon as practicable. The custodian is required to assess risk of harm in the event of any privacy breach to determine if a report is required. When there is a risk of harm to the individual who is the subject of the health information, custodians are required to report privacy breaches as soon as practicable.

"As soon as practicable" means as soon as the affiliate or custodian becomes aware of the breach and has the information necessary to provide the report. Failure to report a breach and failure to employ appropriate measures (physical, technical and administrative) can both lead to penalties under the Act.

Breach reporting by the custodian is required when the following conditions are met:

- There has been a loss of, or any unauthorized access to or disclosure of individually identifying health information

AND

- There is a risk of harm to the individual who is the subject of the information as a result of the loss, unauthorized access or disclosure. Risk of harm is assessed using the criteria specified in Section 8.1(1) of the HIR.

Breach reporting by the custodian involves informing the subject of the information, the Information and Privacy Commissioner and the government minister responsible of the breach.

The custodian's policies and procedures must include:

- The format and process by which affiliates are to notify the Custodian (or Privacy Officer) of a breach
- The information to be provided in the affiliate's report
- The process by which the custodian (or Privacy Officer) will assess the risk of harm to the individual who is the subject of the information. (See Form 07 - Risk of Harm Checklist)
- How the custodian will respond to privacy breeches, including incident response protocols and reporting. (See Form 08 - Model ClientNotification Letter)

Sample Policy and Procedure Content: Breach Reporting

This policy applies to <Name of Custodian> and their affiliates at <XYZ Clinic >, including staff, volunteers, contractors, and any other party granted access to health information in the custody and control of the custodian.

Affiliates of <Name of Custodian> will notify <Name of Custodian>'s Privacy Officer <first name, last name, contact information> of a suspected or confirmed breach of health information as soon as practicable.

Upon discovery of a breach or suspected breach, affiliates shall take any immediate actions necessary to prevent further loss, unauthorized access or disclosure of individually identifying health information. This may include:

- Attempting to recall emails containing individually identifying health information sent to the incorrect recipient
- Requesting that individuals receiving email or fax transmissions containing individually identifying health information in error securely destroy the information
- Other actions appropriate to the situation

Once immediate actions have been completed, the affiliate will notify <Name of Custodian>'s Privacy Officer <first name, last name> via telephone and follow up email of the breach or suspected breach, providing the following details:

- The nature of the privacy breach or suspected breach (e.g., loss, unauthorized access, unauthorized disclosure)
- The record or records believed to be subject to the breach
- The nature of the individually identifying health information that was subject to the breach or suspected breach (i.e., registration information or diagnostic, treatment and care information)
- The date or period of time within which the breach is suspected to have occurred

If a suspected or confirmed privacy breach is discovered, whether through routine monitoring of compliance and auditing, or report from custodians, affiliates or other parties, <Name of Custodian>'s Privacy Officer, <first name, last name>, will investigate and determine:

- Whether individually identifying health information has been accessed, altered, used or destroyed without appropriate authorization
- The nature of the individually identifying health information that was subject to the breach
- The date of, or period of time within which the breach occurred
- The cause of the breach
- The extent of the privacy breach, (number of records or individuals effected)
- Immediate and future actions to reduce the risk of harm to the individual or individuals subject to the breach
- Immediate and future actions necessary to reduce the risk of a future breach of a similar nature
- Whether the breach constitutes a risk of harm to the individual(s) who is (are) the subject of the information, as defined by Section 8.1(1) of the Health Information Regulation
- Whether the breach is such that reporting to the subject of the information, the Information and Privacy Commissioner and government minister responsible is required
- Whether substitutional notification (e.g., television or newspaper advertisements) is required due to the number of affected individuals or currency of contact information of those affected

Upon completion of the investigation, <Name of Custodian>'s Privacy Officer will:

- Implement measures to reduce the risk of further harm to the individual(s) who is (are) subject to the breach.
- Report the breach to the Information and Privacy Commissioner and government minister responsible when the breach meets the requirements for such reporting, in the manner and format specified by Section 8.2 of the Health Information Regulation.

- Report the breach to the individual(s) whose individually identifying health information has been affected, in the manner and format specified by Section 8.2 of the Health Information Regulation, if the breach constitutes a risk of harm to the subject of the breach.

OR

- Apply to the Information and Privacy Commissioner for approval to employ substitutional notice if appropriate for the situation (e.g., large number of files affected) if the breach constitutes a risk of harm to the subject of the breach.

AND

- Review and update the custodian's policies and determine any additional safeguards or training required to address the source of the breach.
- Implement further actions necessary to reduce the risk of a future breach of a similar nature.
- Address the need for disciplinary or other action related to affiliates of <Name of Custodian> involved in the breach.
- Retain records of the privacy breach including the notification received from the affiliate; findings of the investigation; notifications sent to the subject of the breach, the Information and Privacy Commissioner, and the government minister responsible ; and documentation of additional actions taken to protect the privacy of the subject(s) of the privacy breach and to prevent a future breach of a similar nature.

Individuals with questions regarding this policy are directed to <Name of Custodian>'s Privacy Officer <first name, last name> for further information.

Contracting with Service Providers

Custodians may enter contracts with information technology providers (e.g., electronic medical record platform providers, AI Scribe services) or other third parties to provide services that include the processing, storage, and disposition of health information.

Individuals and organizations that process, store, retrieve, or dispose of health information as well as transform individually identifying health information into non-identifying health information, or provide information management or information technology services that require the use of health information are classified as "information managers" by the HIA.

When securing services from an information manager, custodians retain responsibility for the health information in their custody and control to which the information manager has been granted access.

Hiring an information manager does not alter the responsibilities and accountabilities of the custodian.

Custodians are required to ensure that any information manager contracted to provide services to the custodian has the administrative, physical, and technical safeguards specified by the custodian in place, to maintain the security and integrity of individually identifying health information.

Information Manager Agreements that fulfill the requirements of Section 7.2 of the HIR must be in place, including:

- Identifying the purposes of the agreement with the information manager
- Specifying that the custodian retains control over health information
- Identifying the responsibilities of each party, including whether and how the information manager may collect, use, disclose, or destroy health information
- Specifying the processes by which the information manager would address requests for access, correction, and amendment of health information
- Specifying the administrative, physical, and technical safeguards that the information manager will employ to protect health information
- Enabling the custodian to monitor compliance with the terms and conditions of the agreement
- The requirement that the information manager adhere to the requirements of the HIA, the College of Physiotherapists of Alberta's Standards of Practice, and the custodian's policies and procedures
- Containing remedies to address issues of non-compliance or breach of the terms and conditions of the agreement, and specifying how the agreement can be terminated

For information about what to include in an information manager agreement, see Form 09 - Information Manager Agreement Checklist.

Sample Policy and Procedure Content: Contracting with Service Providers

<Name of Custodian> engages third-party contractors to provide information management services including:

- Processing, storage, retrieval, or disposition of health information
- Transformation of individually identifying health information into non-identifying health information
- Providing information management or information technology services that require the use of health information in the form of electronic medical records, AI scribe tools, online booking portals.

Prior to providing health information to an information manager, <Name of Custodian> will confirm that:

- An Information Manager Agreement is in place that fulfills the requirements of Section 7.2 of the HIR.
- The information manager has in use physical, technical and administrative safeguards for health information, consistent with <Name of Custodian>'s policies.
- The information manager is aware of and in compliance with the requirements of the HIA.
- Confirms that the information manager's staff completes routine training to ensure they are aware of and in compliance with the requirements of <Name of Custodian> and the HIA.

All requests regarding access, correction or amendment, and disclosure of individually identifying health information must be directed to <Name of Custodian>'s Privacy Officer <name, contact information>.

The Privacy Officer will direct all actions of the information manager in relation to access, correction, amendment, collection, use, disclosure or destruction of health information.

Information managers are not authorized to release information directly to any other party at any time or under any circumstance.

Information managers are not authorized to collect or use health information for any purpose without the express written authorization of the custodian.

Forms

The sample forms provided in this section are intended to serve as a preliminary template for custodians.

However, the forms cannot contemplate the full range of needs and considerations that different custodians may face. As such, custodians are advised to carefully review the content of these documents, modifying and seeking legal advice as necessary to ensure the requirements of the *Health Information Act* and the custodian's unique needs are met.

Form 01: Employee Confidentiality Agreement

Employee Name: _____

Employee Role/Position:_____

1. I acknowledge that I am an employee/volunteer/contracted service provider for <XYZ Clinic>.
2. I acknowledge that I am an affiliate of <Name of Custodian>, who is a custodian subject to the provisions of the *Health Information Act*.
3. I will uphold to the best of my ability my duties as an affiliate under the *Health Information Act* and the Regulations, and the custodian's policies and procedures
4. I will observe and comply with all policies and procedures of <Name of Custodian> with respect to privacy, confidentiality, and security of health information.
5. I further acknowledge specific information handling and security practices which include:
    a. Health Information Policy & Procedure Manual
    b. Laptop security
    c. Wireless networking/remote access policies

[Note: Edit list according to organization's resources, policies, and information handling practices.]

6. I will not use or disclose health information that comes to my knowledge or possession by reason of my affiliation with <Name of Custodian>, including after I cease to be an affiliate of <Name of Custodian>, except as authorized by the HIA, the HIR, and the custodian's policies and procedures, and in the performance of my duties.
7. I understand that a breach of this agreement may be just cause for termination of my employment or affiliation with <Name of Custodian>.
8. I am aware that <Name of Custodian> has a Health Information Policy & Procedure Manual regarding the privacy, confidentiality, and security of health information. I understand that it is my responsibility to:
    a. Read and be familiar with the requirements outlined in these policies and procedures,
    b. To review the policies and procedures annually, and
    c. To seek clarification if I have questions about requirements and responsibilities or identify inconsistencies within the policies and procedures.
9. I am aware that my use of <Name of Custodian>'s EMR, Netcare, and other electronic applications that collect, use, or store health information may be monitored to ensure appropriate access, use and security of health information. Specifically, audit and access logs will be checked by the system administrator intermittently and in the event that a breach of security or privacy is suspected. <Name of Custodian> will work with the appropriate vendor to automatically generate audit logs that identify use of the system outside of office hours, same last name (of user and client record) look-up, and other relevant monitoring criteria.
10. I understand that I can contact <Name of Custodian>'s Privacy Officer regarding these policies and any other information I require in order to understand my obligations.

_____	_____	_____
Employee Signature	Name (Print)	Date

Form 02: Consent for the Disclosure of Individually Identifying Health Information

Name: _____

Date of Birth:_____

Address:_____

I authorize that my individually identifying health information related to_____

_____

may be disclosed by (name of custodian)_____ in accordance with

Section 34 of the *Health Information Act* to (name of recipient)_____

for the following purpose(s):_____

_____

I understand why I have been asked for consent to collect/use/disclose my individually identifying information and am aware of the risks and benefits of consenting or refusing to consent.

I understand that I may revoke this consent at any time.

Dated: . _____ Expiry date:_____

_____

Signature of client/authorized representative*

*If you are signing on behalf of the client, the following information must be provided:

_____ _____

Print Name of Authorized Representative Print Source of Representative's Authority

_____ _____

Witness Signature Witness Name [Print]

Form 03: Access

Name:_____

Date of Birth: _____

Address (city, province, postal code): _____

Telephone (business): _____ Telephone (home):_____

Fax: _____ Email: _____

About Your Request:

To which custodian are you making your request? (Please provide the name of the individual or the organization):

_____

Do you want to (check one): Receive a copy of the record? ___ OR Examine the record? ____

If you are requesting a copy of your health record, please attach the initial fee of $25.00.

About the Information You Want to Access:

What records do you want to access? Please give as much detail as possible. Indicate if you also want access to records about the disclosure of your information (be sure to give all your previous names). If you are requesting access to another individual's information, you must include information to identify the individual (in the box below) and attach proof that you can legally act for that individual (in accordance with section 104 of the Act). If you need more space, please attach a separate sheet of paper.

What is the time period of the records? Please give specific dates.

_____ I am aware that <Name of Custodian> may charge a fee for the provision of a chart copy. The fee will be in accordance with Section 10, and the Schedule of the Health Information Regulation. I will be provided with a written estimate of the fee before the chart copy is prepared.

_____ _____

Signature Date

****

OFFICE USE ONLY

Date Received Request number

Form 04: Amendment

Name: _____

Date of Birth: _____

Address (city, province, postal code): _____

Telephone (business): _____ Telephone (home): _____

Fax: _____ Email: _____

About Your Request:

Whose information do you want to correct?

_____ Your own health information.

_____Another person's health information. (Please include information to identify the other individual and attach proof that you can legally act for the individual (in accordance with Section 104 of the HIA.))

To which custodian are you making your request? (Please fill in the name of the individual or organization.)

What health information needs to be corrected or amended? Please give as much detail as possible. (Be sure to give the complete name that is in the records if it is different from the name given above. If you need more space, please attach a separate sheet of paper.)

What correction or amendment do you want to make and why? (Please attach any documents that support your request.)

Signature _____ Date _____

OFFICE USE ONLY

Date Received Request number

Form 05: Research Disclosure

Application for Disclosure of Health Information for Research Purposes

Principle Investigator: _____

Business Address (city, province, postal code): _____

Telephone (business): _____ Telephone (home): _____

Fax: _____ Email: _____

About Your Request:

This application is for disclosure of health information for research purposes.

To be disclosed by (Name of Custodian) _____, in accordance with Division 3 of the *Health Information Act* to (name of Principal Investigator) _____.

For the following purpose(s): _____
_____
_____
_____

The following documents are attached to this application:

_____ Description of the Research Project

_____ The response of the Research Ethics Board to the Proposed Research Protocol

_____ Other supporting documentation. Please specify: _____

_____ _____

Date: Expiry date:

_____ _____

Principal Investigator Signature Date

_____ _____

Witness Signature Witness Name (Print)

Form 06: Research Agreement Checklist

Seek independent legal assistance to develop research agreements that include contract terms that address the following considerations.

Pre-requisites

- Identifies that the Proposed Research Protocol has been submitted to the appropriate Research Ethics Board and that the Research Ethics Board is satisfied that the requirements of Section 50 of the HIA have been met.
- Appends copies of the Proposed Research Protocol, Research Ethics Board response, and custodian's Research Application to the agreement.
- IF the Research Ethics Board has recommended that consent be obtained from the subject(s) of health information, obtains consent before the disclosure of health information or provision of other research related services.

Definitions and Interpretation

- Identifies the parties entering into the agreement Identifies the *Health Information Act* (HIA) and *Health Information Regulation* (HIR) as the legislation that applies to the data and that the Researcher will comply with the HIA and HIR.
- States that the agreement is entered into in accordance with Section 54 of the HIA.
- Lists terms specific to the agreement and the research proposal and ensures that definitions are consistent with the HIA.
- Specifies that the agreement pertains to disclosure of data, performance of data matching, or performance of additional services to facilitate the research, and what those services entail.

Custodian's authority

- Includes provisions enabling the custodian to:
  - Decline to disclose data requested or perform services requested by the researcher.
  - Impose additional conditions on the use, protection, disclosure, return or disposal of data.
  - Disclose data in the form the custodian sees fit, including removing individually identifying information from the data before disclosure.

General Terms: Duration, Breach, and Termination of the Agreement

- Specifies the duration of the agreement.
- Acknowledges that the researcher has no claim to ownership of the data.
- Specifies costs for obtaining consents when required by the Research Ethics Board, preparing information, providing copies of data, performing data matching or other research related services that reflect the actual costs of providing the service.
- Requires that the researcher notify the custodian if the researcher becomes aware of a breach of the agreement.
- Includes clauses pertaining to termination of the agreement by either party.
- States that the researcher must, upon request of the custodian or termination of the agreement, cease activities related to the data, and return the data or destroy the data and provide proof of destruction.
- Cancels the agreement if the agreement is breached or if health information is disclosed or used in contravention with the agreement, the HIA, or the Health Information Regulation. Identifies any related penalties/consequences.
- Acknowledges the penalties established under Section 107 of the HIA for breach of a research agreement.

Collection, Use and Disclosure of Data for Research

- Includes terms imposing the conditions, restrictions, policies and guidelines suggested by Research Ethics Board.
- States that the researcher will comply with:
  - Policies and procedures of custodian (referred to in Section 63 of the Act) and any terms or conditions imposed by the custodian.
  - Requirements to safeguard against the identification of an individual who is subject of the data.
  - Applicable requirements, policies, guidelines under the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.
- States that the researcher will only collect, use, or disclose data for the purposes outlined in the research proposal or with written consent of the custodian.
- Requires that the researcher will refer any requests for access to data to the custodian.
- Specifies that the researcher will not attempt to contact individuals who are subject of the data without the custodian's approval and receipt of consent to contact from subject of the data (consistent with HIA Section 55) (in the alternative, bars the researcher from contacting the subject of the health information).
- Includes terms that allow the custodian to access and/or inspect the researcher's premises to confirm their compliance with the agreement, the custodian's conditions, and the HIA.

Security

- Requires the researcher to maintain confidentiality of data.
- Specifies the researcher's use of safeguards to protect confidentiality and guard against threats to data integrity or security, in accordance with the custodian's policies and procedures.
- Specifies that the researcher will not publish data in a format that could reasonably enable the identification of an individual who is subject of the data
- States that the researcher will be responsible for any unauthorized use or disclosure of data.
- Specifies that the researcher will report any breaches of confidentiality or security to the custodian, and will take steps to remedy the breach and prevent future similar occurrences.
- Requires that the researcher maintain a list of all research staff and associates who have access to the data, only sharing data with those engaged in the research project.
- Requires the researcher ensures staff and associates use data only for purposes described in the research proposal, and comply with the HIA and HIR.

Publication

- Requires that the researcher will provide the custodian with a copy of the results report or publication for the custodian's review.
- Provides that the publication must include a statement that some of the data used in the study was provided by the custodian and that the custodian expresses no opinion on the interpretations and conclusions in this publication.

See also Appendix 4 of the Health Information Act Guidelines and Practice Manual

Form 07: Risk of Harm Checklist

In accordance with section 60.1 of the *Health Information Act* (HIA) and section 8.1 of the *Health Information Regulation*, when any individually identifying health information under the custody or control of a custodian is lost, or there is unauthorized access to, or unauthorized disclosure of individually identifying health information, the custodian must evaluate the risk of harm to the individual who is the subject of that information in determining whether or not to proceed with notification to that individual, the Office of the Information and Privacy Commissioner, and the government minister responsible. When determining the risk of harm, the custodian must consider the following factors:

Section 1	**Yes**	**No**
Is there reason to believe that the information has been or may be accessed by or disclosed to a person?		
Is there reason to believe that the information has been misused or will be misused?		
Is there reason to believe that the information could be used for the purpose of identity theft or to commit fraud?		
Is there reason to believe that the information involved is of a type that could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual who is the subject of the information?		
Is there reason to believe that the loss, unauthorized access or disclosure has adversely affected, or will adversely affect, the provision of a health service to the individual who is the subject of the information?		
Are there any other factors that indicate a risk of harm to the individual who is the subject of the information?		
Section 2		
In the case of electronic information, can the custodian demonstrate that the information was encrypted or otherwise secured in a manner that would: • Prevent the information from being accessed by a person who is not authorized to access the information? OR • Render the information unintelligible by a person who is not authorized to access the information?		
If the information was lost, can the custodian demonstrate that the information was lost in circumstances in which the information was: • Destroyed? OR • Rendered inaccessible or unintelligible?		
If the information was lost, and subsequently recovered by the custodian, can the custodian demonstrate that the information was not accessed before it was recovered?		
In the case of an unauthorized access to or disclosure of information, can the custodian demonstrate that the only person who accessed the information (or to whom the information was disclosed) meets all of the following requirements: • Is a custodian or an affiliate? • Is subject to confidentiality policies and procedures that meet the requirements of section 60 of the HIA? • Accessed the information in a manner that is in accordance with the person's duties as a custodian or affiliate and not for an improper purpose? AND • Did not use (or disclose) the information except in determining that the information was accessed by (or disclosed to) the person in error and in taking any steps reasonably necessary to address the unauthorized access (or disclosure)? Are there any other factors that indicate that the risk may be mitigated?		

If you are able to demonstrate that factors from Section 2 are present, notification is not required.

As a custodian, you must consider if there are any other factors that are relevant which may indicate a risk of harm to the individual due to a loss of, unauthorized access to or disclosure of health information. Each situation is unique, and all factors should be considered. In some circumstances, the custodian may decide that notification is necessary even though factors from Section 2 are present.

Form 08: Model Client Notification Letter

Notice of Loss, Unauthorized Access, or Disclosure

<Custodian's file reference number>

<Date>

<Name and address of affected individual>

Dear <Title and name of affected individual>,

This notice is to advise you that your health information that was in the custody and control of <Name of Custodian> was <type of incident: lost/inappropriately accessed/disclosed inappropriately>.

The information involved in the <type of incident: loss, unauthorized access or disclosure> was (type(s) of health information involved) held by <Name of Custodian>.

The incident occurred on <date or time period of incident> when <describe the circumstances of the loss, unauthorized access or disclosure>.

This notice is being provided to you in accordance with the requirement to notify of a <type of incident: loss, unauthorized access or disclosure> under section 60.1 of the *Health Information Act* and as a precautionary measure to prevent or reduce possible risks of harm to you as a result of the <type of incident: loss, unauthorized access or disclosure>.

<Name of Custodian> has determined that, as a result of this incident, there may be a risk of <description of harm> to you because <how the risk of harm was assessed/Form 7 Section 1 harms identified>. We have taken the following steps to reduce the risk of harm to you: <description of steps taken to reduce the risk of harm>. We will be taking further steps to reduce the risk of harm, including <description of additional steps that will be taken>. To prevent this incident from occurring in the future, we are <description of steps that will be taken to prevent future occurrence>.

We strongly suggest that you <description of steps the individual may take to reduce the risk of harm>.

Please be advised that the Information and Privacy Commissioner of Alberta has the authority to investigate any contraventions of the *Health Information Act*. If you would like to report any concerns to the Commissioner, please contact the Office of the Information and Privacy Commissioner at 780-422-6860 (Toll-free at 1-888-878-4044) or generalinfo@oipc.ab.ca.

If you require further information or you have questions regarding this notice, please feel free to contact <name of Privacy Officer> at <phone number and/or email address>.

Sincerely,

[Name of Privacy Officer]

[Position title for Privacy Officer]

Form 09: Information Manager Agreement Checklist

Seek independent legal assistance to develop information manager agreements (IMAs) that include contract terms that address the following considerations.

Definitions and Interpretation

- Identifies the Health Information Act (HIA) and Health Information Regulation (HIR) as the legislation that applies to the agreement and the health information disclosed to the Information Manager.
- Identifies the parties to the agreement and their roles, and specifies the information manager as an affiliate of the custodian, consistent with Section 1(1)(a)(iv) and Section 66 of the HIA.
- States that the agreement is entered into in accordance with and to fulfill the requirements of Section 66 of the HIA, describing the services to be provided and any principles underlying the agreement.
- States that the Information Manager will comply with the HIA and HIR, the policies and procedures established or adopted by the custodian in accordance with Section 63 of the HIA, and the terms of the agreement.
- Identifies the services the Information Manager will provide and the health information to which the agreement applies.
- Defines any terms specific to the agreement, ensuring definitions are consistent with the HIA.

Custodian authority

- Identifies that the custodian remains responsible for compliance with the HIA and HIR, including in respect of the information disclosed to the Information Manager.
- Identifies that the information held by the Information Manager remains under the custody and control of the custodian for the purposes of the HIA.

General Terms: Duration, Breach, and Termination of the Agreement

- Specifies the duration of the agreement.
- Requires the Information Manager to provide services with reasonable care, skill and diligence, maintaining a high degree of data accuracy in handling health information.
- Specifies the fees charged by the Information Manager for services pursuant to the agreement.
- Acknowledges that the Information Manager has no claim to ownership of health information.
- Requires that the information manager notify the custodian in writing if the information manager becomes aware of a breach of health information, providing particulars of the breach.
- Requires that the information manager will take all reasonable steps to mitigate the breach.
- Requires that the information manager notify the custodian in writing if the information manager becomes aware of a breach of the conditions of the agreement or the custodian's policies and procedures.
- Terminates the agreement if the agreement is breached or if health information is disclosed or used in contravention with the agreement, the HIA, or the HIR. Includes other clauses pertaining to termination of the agreement as needed.
- Acknowledges the penalties established under Section 107(4) of the HIA for breach of an information manager agreement.
- Specifies that the information manager must, upon request of the custodian or termination of the agreement, cease activities related to the health information, and return the health information or destroy the health information and provide proof of destruction.
- Identifies that the information manager is responsible for the actions of its employees, contractors or agents in relation to the use and disclosure of health information and that this responsibility continues after termination or expiration of the agreement.

Collection, Use and Disclosure of Health Information

- Acknowledges that in providing services to the custodian described in the agreement, the Information Manager may need to have access to, or may need to use, disclose, retain or dispose of Health Information.
- Specifies that the custodian will provide access to health information to the Information Manager on a need-to-know basis.
- Requires the Information Manager to treat health information subject to the IMA as confidential, limiting access to health information to those employees or agents of the Information Manager who are engaged in the services described in the agreement and have a need to know.

- Requires that the information manager will inform the custodian of client access, amendment, and correction requests as soon as is reasonably possible.
- Describes the process for how the information manager will respond to requests to access, amend, or correct health information OR specifies that the information manager is not permitted to respond to such requests and describes the process for referring these requests to the custodian.
- Specifies whether the information manager is permitted to collect health information from another custodian or from a person and, if so, describing the health information and the purpose for which it may be collected, OR specifies that the information manager is not authorized to collect health information.
- Specifies that the information manager may only use or disclose health information provided by the custodian for the purposes authorized by the IMA and identifies those purposes in the IMA OR specifies that the information manager is not authorized to use or disclose health information provided by the custodian for any purpose.
- If permitted to use or disclose health information provided by the custodian, requires that the Information Manager limit its use and disclosure of health information to the minimum necessary to furnish services or resolve support issues on behalf of the custodian and specifying that the Information Manager must not retain, save, print, store, or otherwise maintain health information after a problem is resolved.
- Requires that the Information Manager only provide health information to other Information Managers used by the custodian with authorization of the custodian.
- Describes how the Information Manager is to address the expressed wish of the individual relating to the disclosure of that individual's health information, OR specifies that the Information Manager is not permitted to address such requests and describes the process for referring the individual to the custodian.
- Permits the custodian to audit the Information Manager's performance of this Agreement and conduct routine audits to verify that health information is only used in accordance with the IMA. Includes reasonable access to the applicable facilities of the Information Manager.
- Affirms the custodian's right to monitor and generate an audit trail of the Information Manager's access of health information.
- Requires that the Information Manager immediately, and before undertaking the activity, disclose all temporary or permanent storage of health information outside the province of Alberta.
- Specifies that health information stored outside of the province of Alberta remains in the custody and control of the custodian, is subject to the custodian's safeguards and compliance monitoring, and specifies that despite storage outside of Alberta, the provisions of the Alberta Health Information Act and the Alberta Health Information Regulation will be adhered to at all times.
- Requires the Information Manager to destroy all health information extractions or copies that are no longer required and provide the custodian with proof of destruction.

Security

- Requires the information manager to maintain confidentiality and security of health information and protect against risks of unauthorized access, use, disclosure, destruction or alteration.
- Specifies the safeguards to protect confidentiality and guard against threats to health information integrity or security that the information manager will use.
- Requires that the Information Manager will ensure that its employees, contractors, or agents who have access to health information are informed of their privacy obligations under the HIA.
- Requires that the Information Manager ensure its staff and associates use health information only for purposes described in the information manager agreement, and do not modify or alter the health information unless as required as part of the delivery of services outlined in the IMA or with written instruction from the custodian.
- Requires that the Information Manager maintain a list of all information manager staff and associates who have access to the health information.
- Specifies that the Information Manager will be responsible for unauthorized use or disclosure of health information by the information manager's staff.
- Describes how health information provided to the Information Manager is to be managed, returned or destroyed in accordance with the Act.

See also Appendix 4 of the Health Information Act Guidelines and Practice Manual

COLLEGE OF
PHYSIOTHERAPISTS
OF ALBERTA

www.cpta.ab.ca

300, 10357 - 109 Street, Edmonton, Alberta T5J 1N3
T 780.438.0338 | TF 1.800.291.2782 | 780.436.1908
info@cpta.ab.ca