COLLEGE OF
PHYSIOTHERAPISTS
OF ALBERTA

Privacy Guide

for Alberta Physiotherapists

March 2019

Privacy legislation is complex and keeping current with legislative changes and provincial and federal rulings can be challenging. This guide is designed to provide physiotherapists with both general and practical information on privacy legislation, policies and procedures.

COLLEGE OF
PHYSIOTHERAPISTS
OF ALBERTA

The College of Physiotherapists of Alberta regulates and leads the practice of physiotherapy in Alberta. This guide has been developed to provide both general information and practical advice for physiotherapists on privacy legislation, policies and procedures. The guide and its resources will also help physiotherapists formulate their own privacy policies. However, the sample privacy statement, consent form, and privacy agreement provided are generic documents. Therefore, they may not be suitable for all physiotherapy practices.

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. The content was originally developed in June 2004 by Field Law (Edmonton) in consultation with the College of Physiotherapists of Alberta. The guide was revised in January 2019.

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

College of Physiotherapists of Manitoba
1465A Pembina Hwy, Winnipeg, Manitoba R3T 2C5
T 204.287-8502 | F 204.474.2506
info@manitobaphysio.com | www.manitobaphysio.com

Contents

Executive Summary

This guide contains information and advice regarding current privacy legislation affecting Alberta physiotherapists and is intended to help physiotherapists comply with that legislation. Physiotherapists are required to comply with applicable privacy legislation regardless of their practice environment.

Privacy legislation governs the collection, use, storage and disclosure of personal information. This guide's reference to personal information includes, but is not limited to contact information, health information, financial information, and employee information.

The Personal Information Protection Act (PIPA) applies to most of the personal information and personal employee information collected, used and disclosed by physiotherapists practicing on their own or with other physiotherapists in private practice environments. The *Health Information Act* (HIA) governs the personal health information collected about patients treated by physiotherapists employed by Alberta Health Services (AHS) or any other "custodian" as that term is defined under the HIA. If you are not sure which legislation applies, please review Appendix I - Privacy Legislation Applicable to Physiotherapists for further clarification.

Please review this guide in its entirety as it contains important information that is difficult to summarize. That said the guide's key recommendations are as follows:

1. **Appoint a Privacy Officer**

   Appoint a person responsible for privacy legislation compliance and access to information requests. The officer should be familiar with the concepts in the legislation and in this guide and have the authority to exercise this role.

2. **Develop a privacy policy**

   If employed by or under contract with AHS, a hospital or nursing home, or another custodian under HIA or public body under FOIP, you may be required to follow a privacy policy already in place. If there is no applicable policy, develop one that addresses your information management strategies to ensure the adequate protection of personal information in your custody.

3. **Obtain consent**

   It is a fundamental rule of privacy legislation that consent is required for collecting, using and disclosing personal information. In most circumstances you can insert a consent clause related to the collection, use and disclosure of personal information into existing intake or consent forms. Such a clause will suffice in most circumstances, however, if you must comply with HIA, a more specific form of consent (written or electronic) is required when disclosing information to non-health professionals (e.g., a lawyer, a third-party insurer or the patient's employer). See Appendix IV for a sample consent form that can be used in these circumstances.

4. **Adopt physical, technical and administrative safeguards for personal information**

   Ensure you adequately protect the personal information in your possession. For example, keep records in places where only authorized individuals have access and securely dispose of records containing personal information and personal employee information. Ensure that devices used to store personal information or personal employee information are physically secured and that information is encrypted during storage and transmission.

5. **Institute processes to facilitate access to and correction of personal information**

   Legislation gives patients and employees the right to access their personal information and to request correction of personal information in appropriate circumstances. Communicate your access process to patients and employees.

Privacy legislation is complex and keeping up-to-date with legislative changes and provincial or federal rulings is challenging. In addition to this guide, there are several resources that can provide current information (see page 7).

Introduction

Different privacy legislation can apply to a physiotherapist's practice depending on the circumstances, including the nature of the record and whether the physiotherapy service is privately or publicly funded.

PIPA is the key privacy legislation affecting most physiotherapists. Other legislation that can also apply:

- HIA
- Freedom of Information and Protection of Privacy Act (FOIP)
- Federal Personal Information Protection and Electronic Documents Act (PIPEDA)

While physiotherapists should be aware of the different privacy legislation(s) that can apply, the College of Physiotherapists of Alberta recognizes that it is not practical for physiotherapists to design separate systems to address privacy concerns that fluctuate depending on the governing legislation.

Therefore, to help physiotherapists comply with privacy legislation, we have provided a summary of the 10 Key Privacy Principles which all provincial and federal privacy legislation are based on.

Note – this guide's reference to personal information includes, but is not limited to contact information, health information, financial information and employee information.

Ten Key Principles of Privacy Legislation

Privacy legislation's underlying assumption is that an organization may only collect, use or disclose personal information for a purpose that a reasonable person would consider appropriate in the circumstances. Privacy legislation incorporates the following 10 principles:

1. Accountability

Organizations are responsible for the protection of personal information under their control. An individual who is accountable for the organization's compliance with privacy principles should be designated.

2. Purpose

The purpose for which the information is being collected must be identified before or during the collection.

3. Consent

Personal information may only be collected, used or disclosed with the knowledge and consent of the individual, with limited exceptions as specified in the legislation.

4. Limiting collection

The information collected is limited to what is necessary for the identified purposes and will be collected by fair and lawful means.

5. Limiting personal information's use, disclosure and retention

Personal information must only be used and disclosed for the purpose for which it was collected, except with consent or as required by law. Information can be kept only as long as necessary to fulfill that purpose.

6. Accuracy

Personal information must be as accurate, complete and current as necessary.

7. Safeguards

Personal information must be protected by adequate administrative, physical and technical safeguards appropriate to the information's sensitivity.

8. Openness

Information about an organization's privacy policies and practices must be readily available upon request.

9. Access

Individuals have the right to access their personal information and have a right to seek a correction. Both rights are subject to some exceptions as specified in each statute.

10. Challenging compliance

Organizations must provide a way for individuals to challenge its compliance with the above principles. In Alberta, patients can complain to the Information and Privacy Commissioner if they believe an organization has contravened provincial access and privacy legislation.

Steps to Ensure Privacy Compliance

Step 1. Review governing legislation

To help enhance your understanding of privacy rules:

- Review legislation. See Appendix I to determine which legislation applies to your practice and then familiarize yourself with the legislative requirements.
- Review available resources. The Office of the Information and Privacy Commissioner of Alberta's website (www.oipc.ab.ca) contains comprehensive information about privacy legislation. Other online resources include:
  - Personal Information Protection Act (PIPA) - legislation, additional information and resources are available at www. servicealberta.ca/pipa
  - Freedom of Information and Protection of Privacy Act (FOIP) - legislation, FOIP guidelines and additional resources are available at www.servicealberta.ca/foip
  - Health Information Act (HIA) - legislation is available from Alberta Queen's Printer at www.qp.gov. ab.ca. The Health Information - A Personal Matter - A Practical Guide to the Health Information Act, the Health Information Act Guidelines and Practices Manual and Highlights from Alberta's Health Information Amendment Act provide additional information about the Act.
  - Personal Information Protection and Electronic Documents Act (PIPEDA) - legislation and awareness tools (questions and answers, glossary, poster and brochures) are available at www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda.
  - Other resources:
    - Service Alberta PIPA Help Desk 780.427.5848 (for toll-free dial 310.0000 first)
    - Service Alberta HIA Help Desk 780.427.8089 (for toll-free dial 310.0000 first)
    - Service Alberta FOIP Help Desk 780.427.5848 (for toll-free dial 310.0000 first)
    - Office of the Information and Privacy Commissioner of Alberta 780.422.6860 or 1.888.878.4044
    - Office of the Privacy Commissioner of Canada 1.800.282.1376

Step 2. Create inventory of personal information in your practice

Identify the personal information currently collected, used, stored and disclosed about patients, employees or third-party individuals to create the inventory. (See Appendix II for a worksheet to help with this exercise.) You can categorize collected personal information into four groups:

Contact information

- Name (may also be considered health information under HIA)
- Home address, home phone number, email address and other contact information (may also be considered health information under HIA)
- Family information
- Emergency contact person

Health information

- Age or date of birth
- Gender
- Health history
- Examination results
- Health services provided to/received by patient, including copies of charts prepared by other health providers
- Prognosis or other opinions formed during assessment or treatment
- Attendance records and adherence with treatment
- Reasons for discharge and discharge plan
- WCB and insurance reports (may also contain contact and financial information)

Financial information

- Alberta health-care information/insurance benefit coverage
- Employer name
- Section B motor vehicle insurance information
- WCB claim number
- Credit card number and expiry date
- Bank account number

Employee information – applies to employees, contractors, students or volunteers

- Name, address and personal contact information
- Application or resume
- Performance reviews/evaluations
- Reference letters
- Salary information
- Leave of absence information (e.g., disability or maternity)

These lists of personal information are not exhaustive as the type of information that may be categorized as "personal information" under privacy legislation is very broad. When completing an inventory, identifying the category of personal information will help you understand why the information is being collected, for what purposes it may be used and disclosed, and the level of sensitivity of the information.

Once an inventory has been completed, it is important to identify the privacy legislation that applies to a particular piece of personal information. This will help you determine what consent requirements must be met in relation to the handling of that information (including the form of consent and whether an exception to consent applies).

It is also important to identify any third-party consultants/contractors who may have access to the personal information because of their work with you. You may be responsible for ensuring that they comply with privacy legislation, and your expectations for them to do so should be outlined in writing and communicated to them.

If during the creation of your inventory, you find you are collecting personal information that is not required for your primary function as a physiotherapist or employer, consider revising your collection practices to prevent the collection of similar information in the future.

Step 3. Appoint a privacy officer

The privacy officer is accountable for the organization's overall compliance with applicable privacy legislation and must have the authority to exercise this role. The officer does not have to be a physiotherapist. They could be a support worker or member of your administrative team—you do not need to hire externally to fill this role.

Determine if there is someone suitable in your office and delegate authority to oversee the privacy plan and authority to resolve privacy issues/concerns. Your privacy officer's name must be clearly identified and made known to patients and employees.

The privacy officer:

- Oversees the development of privacy policies and procedures.
- Ensures that:
  - The privacy policy is made public to patients and employees.
  - Staff are adequately trained regarding privacy policy and procedures.
  - Appropriate forms are used to obtain consent for information collection, retention and disclosure.
  - Safeguards are in place to protect personal information.
  - Contracts are in place and third-party service providers protect the privacy of personal information.
- Responds to questions/concerns regarding the protection of personal information.
- Liaises with external groups.
- Processes privacy related complaints.

Step 4. Establish and publicly display your privacy policy

Create a written policy identifying your information management strategies once you have determined the rules regarding what information should be collected, used, stored, and disclosed.

If employed by AHS, a hospital or nursing home, or another custodian or public body, you may be required to follow a privacy policy already in place. If so, review the policy to ensure it covers the basic principles set out in this guide and that you are compliant.

If working independently/in private practice and no other privacy policy applies, develop one that addresses your information management strategies and ensures the adequate protection of personal information in your custody. Appendix II contains a worksheet to help ensure your policy adequately covers the information collected, used, stored, and disclosed. Also see Appendix III for a sample privacy statement (note that your privacy officer's name and contact information must be inserted. Your statement should then be displayed and made available to all patients).

Principles that should be communicated to patients and employees in a policy include that:

- Their privacy is valued.
- There is a commitment to protect their personal information.
- The collection, use, storage, and disclosure of their personal information is limited to that which is reasonable to achieve the purposes of providing physiotherapy treatment or relates to their employment.
- Information is only disclosed to third parties for the specific purposes identified, with their express consent or as otherwise permitted by law.

- Physical, technical and administrative safeguards are in place to secure their personal information.
- There is a mechanism to access their personal information and changes to inaccurate information will be considered.
- A privacy officer is available to address questions/ concerns regarding privacy policies and procedures (and include their business contact information in your policy).
- The organization is committed to adhering to all applicable provincial and federal privacy legislation. In the event the individual does not believe the organization has done so, a complaint or request for review may be made to the Privacy Commissioner's office.

Step 5. Limit information collection

Legislation requires you collect only the information needed to provide physiotherapy services to patients and facilitate the processes necessary to complete transactions (e.g., direct billing). Consider information currently collected and ensure it directly relates to the provision of physiotherapy. If not, stop collecting it.

Consider the sensitivity of the information collected and ensure the collection purpose is expressly stated on all your collection forms. Collect personal information directly from the individual in question unless they consent to you obtaining it from another source.

Step 6. Provide for express consent

The concept of obtaining informed consent before providing physiotherapy services is not new. However, the concept of obtaining consent for the collection, use and disclosure of information may be. The general rule of all privacy legislation is that consent is required for the collection, use, storage and disclosure of personal information. While the mandatory form of consent can vary (e.g., some legislation authorizes verbal consent while other legislation requires written), you can ensure compliance by obtaining written informed consent from patients.

There may be some exceptions to the general requirement of consent, meaning in certain circumstances personal information can be collected, used or disclosed without consent. A review of all the exceptions contained in the legislation is beyond this guide's scope. For advice on specific situations, please contact your legal advisor or review the documents referenced under Step 1 - Review Governing Legislation.

Forms of consent

The form of consent required varies by the applicable legislation. For example, in circumstances where consent is required and is being collected to enable disclosure of individually identifying health information under HIA, consent must be provided in writing or electronically and contain certain information like the purpose for which the health information may be disclosed. In contrast, consent under PIPA may be provided in writing or verbally. If accepting verbal consent for disclosure of information under PIPA, physiotherapists are advised to document in the patient or employee record that consent was sought and received.

The following are some consent form recommendations:

- Form of consent if governed by PIPA - Verbal consent for the collection, use, and disclosure of information is sufficient to ensure PIPA compliance. However, written consent is always prudent as it is difficult to prove verbal consent later. Consider including a provision on existing treatment consent forms that would satisfy this requirement. For example:

  I hereby consent to the collection, use, storage, and disclosure of my personal information in accordance with the XYZ Physiotherapy Clinic's privacy policy. I hereby acknowledge that a copy of the privacy policy was made available to me and I have been advised who I may contact if I have any questions about anything contained in the privacy policy.

  You can provide patients with a copy of your policy or a means of accessing it to help ensure they are aware of what information is being collected, how it is being used and stored, and to whom it is being disclosed.
- Form of consent if governed by HIA - HIA requirements are more onerous if information is being disclosed outside the "circle of care" (defined as health-care professionals who provide treatment to a patient receiving physiotherapy from you). Information can be provided to circle of care providers without specifically obtaining patient consent. Outside that circle, however (e.g., to a lawyer or third-party insurer), HIA requires specific written or electronic consent. Have your patient sign a consent form at the time disclosure is made—see Appendix IV for a sample consent form.

Step 7. Safeguard personal information

Contact, health, and financial information are considered sensitive by most individuals. Appropriate safeguards must be in place to prevent unintended or unauthorized access to or loss of this information. Safeguards include:

- Keeping records in places that only authorized individuals can access.
- Locking cabinets and offices containing personal information and not leaving them unattended during business hours.

- For computer files - using passwords, encryption, antivirus and firewalls, and keeping software current (i.e., updates and patches).
- Preventing unauthorized viewing of computer screens and using a password-protected screen saver.
- Not discussing confidential information over the phone or when it could be overheard.
- Shredding paper records and completely expunging files from computer hard drives.
- Confidentiality oaths for staff and/or confidentiality clauses in employment contracts.

Ensure service providers also follow your privacy policies

You are responsible to ensure the personal information in your custody is handled in accordance with the applicable privacy legislation. You may be asked to disclose personal information to a third-party, or you may choose to contract services out to third parties (e.g., electronic medical record software providers, information technology specialists, accountants, etc.).

When hiring/retaining third-party service providers, ensure they know the personal information in your custody is governed by privacy legislation and that they too must protect the information's confidentiality. You can do this via a written and signed privacy agreement (see Appendix V for a sample agreement) or by inserting provisions of the agreement into third-party contracts. Keep in mind that contracting out services to others does not alter your responsibility to maintain the privacy of personal information that is in your custody.

PIPA also requires notification of individuals when their personal information is stored or accessed outside of Canada. If PIPA applies in your practice, ensure that you have policies and procedures in place to deal with these obligations.

Breach Reporting

As of 2018, PIPA, HIA and PIPEDA all have mandatory breach reporting requirements in force. For PIPA and HIA, custodians are required to notify the Office of the Information and Privacy Commissioner of Alberta and the individual(s) affected in the event of a breach of personal information involving a "real risk of significant harm." If a breach of information governed by PIPEDA occurs, custodians are required to notify the Office of the Privacy Commissioner of Canada and the individual(s) affected if the breach of personal information involves a "real risk of significant harm."

Additional information about breach reporting under the HIA can be found in Chapter 14 of the *Health Information Act* Guidelines and Practices Manual.

Step 8. Train staff in privacy legislation intent and requirements

Ensure staff (both employees and contractors) are aware of your privacy policy and relevant legislation and that they have the knowledge and skills necessary to handle privacy concerns. It is advisable for all staff to review this guide.

Step 9. Ensure information on file is current, complete and accurate

Staff should make reasonable efforts to ensure the currency, completeness and accuracy of personal information being collected, used or disclosed. This includes information regarding the current medical status of patients.

Step 10. Identify processes to access and change information on file

Patients and those acting on the patient's behalf may request access to their records at any time. PIPA, HIA and FOIP all have established, legislated time limits for responding to access requests. HIA and FOIP have also established legislated fee schedules for charges that may be collected for providing access to copies of records. Ensure patients understand the processes and fees for accessing personal information in your custody.

When responding to access to information requests ensure that personal information about another person (provided in confidence by someone other than the person requesting access) is not inadvertently disclosed.

If patients request a change to their information, determine if the information on file is factually correct. While incorrect facts/details should be amended, changing a professional opinion because a patient disagrees is not required or appropriate.

Document the change request in the patient's file. If the request is unwarranted, consider seeking advice (from the College of Physiotherapists of Alberta, the Office of the Information and Privacy Commissioner, etc.) to ensure the appropriate processes are followed. If patients express concern or dissatisfaction regarding a failed change request explain that they can make a written complaint to your privacy officer or to the Office of the Information and Privacy Commissioner of Alberta (see contact information under Step 1).

Step 11. Establish and communicate process for handling privacy related concerns

To ensure an open process for handling privacy related concerns:

- Identify the privacy officer as the complaints investigator.
- Ensure a confidential complaints process.
- Consider concerns objectively.
- Respond to concerns in the manner they were expressed (e.g., if submitted in writing, respond in writing).
- Seek an informal resolution wherever reasonably possible. For example, if an individual believes too much of their personal information is being collected, determine whether the information is actually needed. If it is not needed it can be destroyed, and the individual can be reassured that this step has taken place. If a concern remains unresolved, the individual may be directed to the Office of the Information and Privacy Commissioner.

- Document steps taken to address concerns.
- Adjust privacy policies and practices to minimize future concerns.

Step 12. Review and update privacy policies and forms regularly

Privacy legislation continues to evolve. Review your policies and practices regularly to ensure compliance with any changes and determine if your systems and processes meet your policy objectives and legislative responsibilities.

Step 13. Implement systems for personal employee information

While steps one to 12 focus on information related to patients, PIPA also applies to employees' personal information. Therefore, physiotherapists employing staff (e.g., assistants, administrative personnel or other physiotherapists) must also ensure the collection, use and disclosure of personal employee information complies with legislation.

PIPA defines personal employee information as:

"… in respect of an individual who is a potential, current or former employee of an organization, personal information reasonably required by the organization for the purposes of

i. establishing, managing or terminating an employment or volunteer-work relationship, or

ii. managing a post-employment or post-volunteer-work relationship

between the organization and the individual, but does not include personal information about the individual that is unrelated to that relationship."

Collection, use and disclosure of personal employee information

The general rule is that the information can be collected, used or disclosed by an organization without the consent of an individual if the individual is or was an employee or volunteer of the organization and:

- The collection, use or disclosure is reasonable for the purpose for which it was collected, used or disclosed.
- For current employees or current volunteers, the personal employee information includes only personal information related to establishing, managing or terminating that individual's employment or volunteer relationship.
- For former employees or former volunteers, the personal employee information includes only information related to managing the post-employment or post-volunteer relationship.
- For current employees or current volunteers, before collecting, using or disclosing the information, employees and volunteers are notified of the collection, use and disclosure and its purpose.

Access to employees' personal information

The rules regarding access to information also apply to personal employee information. Therefore, advise employees that they can access their information in the practice's custody/control.

Frequently Asked Questions

1. Whose responsibility is it to report a privacy breach?

If a physiotherapist becomes aware of a privacy breach or situation which may constitute a privacy breach, they should notify their organization's Privacy Officer as soon as possible.

The College of Physiotherapists of Alberta recommends that patients speak to the organization's Privacy Officer first if they have concerns about how their personal information has been used or believe that their privacy has been breached. This allows the Privacy Officer to discuss the patient's concerns, investigate the matter, and take corrective action to address the underlying issue. Patients also have the right to contact the Privacy Commissioner's office directly if they have a complaint or concern.

It is the Privacy Officer's responsibility to report a privacy breach to the appropriate authority.

2. How does the Privacy Officer know if they need to report a breach?

A privacy breach is any breach of personal or personal employee information which poses a risk of harm to the individual affected by the breach.

PIPA and HIA differ slightly in their wording regarding what constitutes a breach that requires a report.

Under PIPA, an organization must, without reasonable delay, report a privacy breach where "a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure," to the Privacy Commissioner.

Under HIA, organizations must report privacy breaches involving individually identifying health information as soon as practicable "if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure."

3. How does the Privacy Officer know if a privacy breach poses a risk of harm?

According to the Office of the Information and Privacy Commissioner, examples of possible harms that would trigger a mandatory report include:

- Identity theft
- Financial fraud or loss
- Mental or bodily harm
- Embarrassment, hurt or humiliation
- Reputational or relationship harm
- Blackmail or extortion
- Email phishing attacks
- Loss of employment, business or professional opportunities

4. Who does the Privacy Officer report a privacy breach to?

For breaches of information governed by PIPA or HIA, contact the Office of the Information and Privacy Commissioner of Alberta. For breaches of information governed by PIPEDA, contact the Office of the Privacy Commissioner of Canada.

5. What are some common physical, technical and administrative safeguards I should employ to protect personal information?

The controls you employ will vary depending on what information you collect and store and the methods you use to do so. The lists below are not exhaustive, but provide some common examples.

Physical controls

- Locked offices and file cabinets
- Keyed or key card access to file rooms and office spaces
- Locking cables to secure electronic devices to work stations

Technical controls

- Unique user logins and strong passwords
- Encryption of personal information while in storage and when transmitted
- Data access rules based on defined user roles
- Routine updates to IT systems and software
- Auditing systems to monitor access and changes to information

Administrative controls

- Identifying a Privacy Officer
- Staff training on privacy-related issues, policies and practices.
- Privacy and confidentiality agreements.
- Organizational policies and practices such as requiring unique user logins and strong passwords for electronic systems.

- Organizational policies and practices that define if paper records can be removed from the business location, and how those files must be secured when in transit or out of the business office.
- Having defined employee termination procedures to ensure that access to records is rescinded when employment is terminated.

6. How can I ensure privacy and confidentiality when working in online platforms or using online booking systems?

This will also depend on the system used; however, some suggestions include:

- Ensuring contracts are in place that require service providers to protect the personal information in their control.
- Ensuring information is encrypted while electronically transmitted or stored.
- Requiring unique logins and passwords for all users.
- Employing data auditing systems to monitor for unauthorized access or changes to information.
- Gathering express patient consent for collection and use of data using these systems.
- Limiting the collection of data/sharing of data through these platforms to the minimum mandatory information required.

7. We collect patient email addresses as part of our new patient intake practices. Is there anything I can't send to a patient via email?

Physiotherapists are only allowed to use the personal information they collect for the purposes they identified when they collected the information. This includes the use of emails and other contact information. When you gather that information, you should get consent for how it will be used. Possible uses of an email address may include: sending appointment reminders, sending patient education materials and exercise programs, or sharing organization newsletters/ publications.

Before sending an email to a patient, check to see what they consented to and if necessary get consent before sending the information.

Keep in mind that emailing information creates privacy risks due to the potential for misdirection or unauthorized access to personal information. If you are sending patient-specific information via email, it is recommended that you confirm you have the correct email address, re-confirm you have patient consent to send the information via email, and encrypt sensitive information.

8. We have recently had some thefts at our clinic and are considering installing a surveillance camera. Are there any rules I need to comply with?

In the private sector, video surveillance is subject to PIPA. If you implement a surveillance camera, you need to inform those accessing your premises that video surveillance is occurring. You also need to limit the use and viewing range of cameras. Some areas within a physiotherapy practice must not be filmed (i.e., change rooms and treatment spaces).

Visit the Office of the Information and Privacy Commissioner's website for more guidelines on video surveillance in the private sector.

Appendix A
Privacy Legislation Applicable to Physiotherapists

There are four different legislative Acts relevant to physiotherapy practice in Alberta that establish rules regarding the collection, use, disclosure of, and access to information. Because there are differences between the Acts, it is important to determine which governs your physiotherapy practice/environment. It is possible that more than one act can apply.

1. Personal Information Protection Act (PIPA)

PIPA applies to the personal and employee information collected, used and disclosed by physiotherapists working in an "organization," which can include a clinic or sole practice.

When does PIPA apply?

PIPA applies to personal information and personal employee information collected, used and disclosed by physiotherapists:

- Who operate their own physiotherapy practice or work in partnership with other physiotherapists.
- Whose services are contracted by the Alberta Workers' Compensation Board (WCB).*

Consent under PIPA

PIPA requires that consent be obtained for the collection, use and disclosure of personal information unless a specific exception applies; however, the Act does not specify the form of consent required (verbal versus written). Under PIPA, you must have reasonable purposes for the collection, use or disclosure of personal information, and you must limit the amount of information to what is reasonable to meet the intended purposes. One exception is to collect a debt the individual owes you/your practice.

PIPA also includes specific rules for the collection, use and disclosure of personal employee information.

2. The Health Information Act (HIA)

This provincial legislation governs the collection, use, disclosure, and access to health information collected, used and disclosed in conjunction with the provision of health services by custodians. Prior to 2010, the HIA applied to the management of health information by custodians in the publicly-funded health system.

In 2010, the HIA was amended to include additional custodians, including regulated members of some health professions (such as physicians, dentists, and registered nurses), regardless of source of payment for health services. Physiotherapists are not designated as custodians under the HIA; however, if employed by a custodian, a physiotherapist may be considered an "affiliate" under HIA.

When does HIA apply?

HIA applies to health information including registration information (such as name, personal health number, gender, and date of birth) and diagnostic, treatment and care information. It governs health information collected in connection to the provision of a health service (defined under the HIA) by a physiotherapist if/when the physiotherapist is employed by, or contracting services to, AHS, a hospital or nursing home, or another custodian. Aspects of the HIA, related to access to records and fees for copies, are also applicable to patient records for treatment provided under the Diagnostic and Treatment Protocols Regulation.

Consent under HIA

Under HIA, consent is not required before a custodian or affiliate can disclose health information to another health-care provider "within the circle of care." Consent is generally required to disclose information to a third-party (e.g., service providers, private businesses, or insurers). HIA requires that health information collected, used and disclosed be limited to only the amount essential to carry out the intended purposes.

3. Personal Information Protection and Electronic Documents Act (PIPEDA)

This legislation establishes the rules for the collection, use, disclosure of, and access to personal information during the course of "commercial activities." Personal information is broadly defined as "information about an identifiable individual" but does not include the name, title or business address or telephone number of an employee of an organization.

* Physiotherapists/clinics with WCB contracts also governed by the Workers' Compensation Act, which gives the WCB a right of access to information in a patient's file. FOIP may also apply to records related to WCB claims, depending on the circumstances.

When does PIPEDA apply?

PIPEDA can apply to Alberta physiotherapists in limited circumstances where personal information is being transferred across provincial boundaries (e.g., when delivering cross-border physiotherapy services, communicating with a third-party insurer in another province).

Consent under PIPEDA

PIPEDA requires consent to be obtained for the collection, use and disclosure of personal information, unless a specific exception applies such as relating to the collection of a debt. As under PIPA, the collection, use or disclosure of personal information should be limited to purposes that a reasonable person would consider are appropriate in the circumstances.

4. Freedom of Information and Protection of Privacy Act (FOIP)

FOIP establishes the rules for collecting, using, disclosing and accessing information/records in the possession of a "public body" defined as:

- Alberta government department, branch or office.
- Agency, board, commission, corporation, office or other body designated as a public body in the regulations (e.g., WCB).
- Local public body (e.g., educational body, health-care body, or local government such as a municipality or a municipal board).

FOIP applies to all records in the public body's custody/control and is broadly defined to include "information in any form," and can include information stored in any manner.

When does FOIP apply?

FOIP may apply to information collected, used and disclosed when a physiotherapist is employed by, or contracting services to, a school or school board. FOIP can also apply to physiotherapists working in public health-care settings like those employed by AHS (which would be defined as a "health-care body" under FOIP). In such a situation, the handling of health information will generally be governed by HIA as AHS is a custodian under that Act, but the handling of information that does not fall under the definition of health information (like a manager dealing with employment records of a staff member on their unit) will be subject to FOIP.

Appendix B
Inventory of Personal Information

	Information collected	Purpose of collection	Information disclosed to
Contact	□ Name □ Home contact information □ Emergency contact person □ Email address □ Other	□ Open/update patient files □ Invoice patients for services □ Send patient appointment reminders □ Send patient care information (e.g., home exercise program) □ Other	□ Other health-care providers □ WCB □ Third-party insurers □ Other
Health	□ Gender □ Birth date/age □ Health history □ Previous trauma/accidents □ Family health history □ Test/examination results □ Other health provider charts □ Prognosis or opinions □ Objective findings □ Subjective complaints □ Treatment history □ Discharge summary □ Other	□ Conduct assessments □ Provide physiotherapy treatment □ Prepare opinions □ Other	□ Other health-care providers □ WCB □ Alberta Health Services □ The College of Physiotherapists of Alberta (on request) □ Insurers or third-party health benefit providers □ Lawyers □ Other
Financial	□ Employer □ ID# (e.g., DL, APHN) □ Credit card □ Bank account details □ Third-party insurance □ WCB Claim Number □ Other	□ Facilitate payment for services □ Other	□ Third-party insurers □ Accountant □ Revenue Canada □ Credit card company □ Other

Appendix C
Sample Privacy Statement

Introduction

At XYZ Physiotherapy Clinic, we are committed to protecting the privacy of your personal information. We will not disclose your personal information without consent or reasonable and lawful notice except when required or permitted by law.

Our privacy commitment

At XYZ Physiotherapy Clinic, we protect patient privacy by:

- Collecting only the personal information required to provide physiotherapy services.
- Advising you how your information might be disclosed and obtaining your consent.
- Safeguarding your personal information.
- Sharing your personal information only for the purposes stated and agreed to in a signed consent form or otherwise permitted by law.
- Ensuring any contractors we hire who may have access to your information also protect the privacy of your information.
- Training staff and adapting the office space to ensure maximum protection of your privacy.
- Ensuring personal information is current, complete and accurate.
- Providing you access to your personal information and a mechanism for requesting corrections.
- Having our privacy officer available to answer your questions.
- Periodically reviewing our privacy policy to ensure it provides adequate protection for your personal information.

Information collected

The personal information collected is required to provide you with physiotherapy services and facilitate payment for services rendered.

- Contact information: your name, phone number, address, email address and an emergency contact person.
- Health information: your health history, treatment received, names of other health-care providers, family medical history, your subjective complaints, objective findings, diagnoses, reason for discharge, and discharge plan.
- Financial information: your insurance benefit coverage information, credit card information, employer's name, and other information to facilitate payment for services provided.

What do we use your information for?

We use contact information to open and update your patient file, invoice for services, remind you of appointments and/or the need for further treatment, and to provide informational materials about our clinic. We use health information to assess, diagnose, provide, and evaluate physiotherapy treatment. We use financial information to arrange payment for physiotherapy services rendered.

With whom do we share your information?

- Contact information - may be disclosed to third-party health benefit providers/insurers when reimbursement claims for all or part of the treatment cost have been submitted.

- Health information - may be disclosed to:
  - Third-party health benefit providers and insurance companies when a claim is submitted for reimbursement or payment of all or part of the cost of treatment or we have been asked to submit a claim on your behalf.
  - The WCB or your employer if you made a WCB claim.
  - Other health-care professionals also providing you with treatment.
  - Your lawyer, if you were injured in an accident.
  - Research teams in an anonymous form to facilitate outcome research.
- Financial information - may be disclosed to your insurer or credit card company as required to facilitate payment.

Note: Personal information can also be disclosed without your consent if we are required to do so by law.

Information stored outside of Canada

We contract with companies outside of Canada to provide services on our behalf, such as with companies located in [list country/countries] who provide [list services]. These companies and their affiliates may store personal information outside of Canada. For further information regarding storage of personal information outside of Canada or regarding the XYZ Physiotherapy Clinic policies and practices regarding storage of information outside of Canada, please contact our privacy officer, whose contact information is listed at the end of this Privacy Statement.

How we protect your personal information

- We store physical records containing your personal information in a secure place.
- We store electronic records on secured hardware, use antivirus software and passwords on all computers and take care to protect screen monitors from public viewing.
- We transfer physical records outside our office in sealed envelopes by secure methods.
- We conduct telephone discussions with sensitivity to ensure that your personal information is not inadvertently disclosed.
- Electronic information is transferred in secure files and made anonymous wherever possible.
- We do not share your personal information outside our office for any marketing, promotional, publicity, educational, or research purposes without your consent.
- We train staff to handle your information only through the protected measures outlined in our privacy procedures. If consultants or contractors are hired, we take steps to ensure the consultant or contractor also protects your privacy.

Accessing and correcting your personal information

You can get access to view your personal information by asking a staff member who may refer you to our privacy officer. We will attempt to help you understand the reasons we collect, store and use the information in your records.

You may request a change to your personal information if it is inaccurate, incomplete, no longer current, or if you believe there is a factual mistake.

You can also request a copy of your patient record. Requested copies will be provided in a reasonable period. If there is a charge for the cost of producing a copy, we will advise you of the cost in advance.

How long is information kept?

We are required by legislation to keep records containing personal information for 10 years from the last date of service. Or in the case of a minor, 10 years past the minor's eighteenth birthday. After that time, we shred paper records and delete electronic ones. When discarding hardware, we ensure the hard drive is destroyed.

More information

If you have a concern about your personal information, please feel free to ask the physiotherapist treating you or another staff member. If your question/concern is not resolved, please address it in writing to our privacy officer:

First and Last Name Privacy Officer
XYZ Physiotherapy Clinic Address
xxx-xxx-xxxx p.privacy@xyzphysio.com

Appendix D
Sample Health Information Disclosure Consent

I,_____, hereby authorize XYZ Physiotherapy Clinic to release the following information: full and complete disclosure of any medical information you may have or have had, or to which you may have or have had access, in any way related to the undersigned and including, but without restricting the generality of the foregoing, medical charts, medical history, diagnosis, treatment, symptoms, prognosis, opinions, the results or conclusions of any tests of any kind or x-rays and/or other knowledge and to furnish medical/legal reports, written or oral, both before and after the date of this consent, to (insert name and address of person to whom information is being released) for the purpose of (insert purpose for disclosure).

This consent is effective on [DATE] and will expire on [DATE}.

I acknowledge that I am aware of the reasons why my health information is required and have been advised of the benefits and risks of consenting to the release of my health information. I am also aware that I may revoke my consent at any time.

_____ _____

Name Witness

_____

Date

Appendix E
Sample Privacy Agreement

This Agreement made on [DATE] BETWEEN XYZ Physiotherapy Clinic ("the Clinic") and [BUSINESS NAME] (the "Contractor")

WHEREAS as a result of the work performed by the Contractor, the Contractor may receive or become aware of private and confidential information pertaining to clients receiving services at XYZ Physiotherapy Clinic;

AND WHEREAS the Clinic has an obligation to ensure that such information remains confidential, is properly secured and adequately protected, and is not improperly disclosed or destroyed by the Contractor;

The parties agree as follows:

1. The Contractor agrees to abide by and adhere to the Terms of this Agreement and all applicable privacy legislation with respect to personal information the Contractor becomes aware of or has access to in the course of their duties.
2. The Contractor agrees to use the personal information only to the extent that is reasonable for fulfilling the following purposes: (insert purposes for which personal information was disclosed to contractor).
3. The Contractor agrees, except as required by law, not to disclose any personal information without first obtaining written consent allowing for disclosure from the Clinic.
4. The Contractor agrees to protect the personal information by making reasonable security arrangements to protect against unauthorized access, collection, use, disclosure, copying, modification, or disposal.
5. The Contractor agrees to return any personal information to the Clinic:
    a. when the personal and health information is no longer required for fulfilling the purposes set out in paragraph 2 above; or
    b. upon the verbal or written request of the Clinic.
6. If a Contractor receives a request for access to personal information from a person or organization other than the Clinic, the Contractor must promptly advise the person to make the access request to the Clinic.

XYZ Physiotherapy Clinic

_____ _____

Signature Date

Contractor

_____ _____

Signature Date

Appendix F
Release of Information Flow Chart

Request Recieved

Public Practice
- HIA applies to hospital records.
- ***Freedom of Information and Protection of Privacy Act*** (FOIP) applies to school district and WCB internal records.
- Refer to the appropriate department: health records, privacy officer, department manager

DONE

Private Practice
- ***Personal Information Protection Act*** (PIPA) applies to most records.
- ***Health Information Act*** (HIA) applies to the release of DTPR records.
- Treatment record: includes everything related to the patient – chart notes, emails, financial documents, letters.

Who's Asking?

Patient
- Must release requested documents, with few exceptions.[1]
- No other "consent" required.
- Have the patient sign for the copy.
- Document release of information (and any information withheld) in the patient record.

The Patient's Lawyer (anyone acting on the patient's behalf)
- Signed patient consent required (either from the lawyer or the clinic's own form).
- Must release requested documents.
- Document release of information in the patient record.

Other Health-Care Provider
- Must release requested documents.
  - If PIPA legislation applies – signed consent is usually required.[2]
  - If HIA legislation applies – no consent required.
- Document release of information in the patient record.

Third Party Request
- Must release requested documents.
- Signed consent required in most cases.
- Signed Consent not required if requested by:
  - The College of Physiotherapists of Alberta or other Regulatory College (for the purpose of investigating a complaint).[3]
  - Insurance company paying for services under the DTPR.[4]
  - WCB.[4]
- Document release of information in the patient record.

1. In rare circumstances, physiotherapists may redact portions of records if the information would reveal personal information about another individual or could reasonably be expected to threaten the life or security of another individual (including the patient). PIPA Section 24(2). HIA 11(1)
2. PIPA includes provisions that allow for disclosure without consent if a reasonable person would consider the disclosure to be in the interests of the patient and consent cannot be obtained in a timely way, or if the individual would not be reasonably expected to withhold consent.
3. Subject to the *Health Professions Act*, Section 63(1)(a)(ii), a signed patient consent is not required for release of physiotherapy records to the College of Physiotherapists of Alberta.
4. PIPA and HIA both include provisions allowing disclosure of information when required by a statute or regulation of Alberta. This includes the Diagnostic and Treatment Protocols Regulation and the WCB Act.

It is a Best Practice that Consent be obtained prior to disclosure, whenever possible.

Appendix G
Applicable Legislation

Personal Information Protection Act (PIPA)

Applies to: Private practice patients (privately or third party paid), WCB chart notes

Fees allowed: "A reasonable fee for access to the applicant's personal information." The organization must provide a written estimate of the total fee.

Timelines: Must respond to the request within 45 days of receipt of the request.

Freedom of Information and Protection of Privacy (FOIP)

Applies to: Documents held by WCB (including physiotherapy-related WCB reports), and records maintained by public institutions (i.e., schools)

Fees:

- The public body may require the applicant to pay the cost of producing the copy.
- The public body may not charge other fees for services for access to the applicant's own personal information.

Timelines: The public body must make "every reasonable effort to respond not later than 30 days after receiving the request."

Health Information Act (HIA)

Applies to: Public practice patients (Hospitals), and patients treated under the DTPR.

Fees allowed: The custodian may only charge "for the cost of producing the copy." Per the Health Information Regulation, permitted fees include:

- Basic Fee: $25 for file preparation, clarifying the request, obtaining consent, retrieving the record, preparing the record, AND photocopying the record.
- Photocopies and computer printouts: $.25/page if the cost of photocopying the chart, when calculated at $.25/page exceeds $5 (chart greater than 20 pages long, $.25/page for pages 21 onwards).
- Producing a record from an electronic record:
  i. computer processing - actual costs
  ii. computer report generation - $10 per 1/4 hour

Timelines: Must respond to the request within 30 days of receipt of the request.

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