

Our Responsibilities

Privacy is a fundamental human right and legal right of all Canadians. As trustees under *Health Information Protection Act* of Saskatchewan and the *Personal Information Protection and Electronic Documents Act* of Canada it is our responsibility to ensure the confidentiality and security of client personal and personal health information. In order to maintain the trust and confidence of clients, employees, patients, the public, and colleagues it is essential that this facility ensure fair handling of personal and personal health information, at all times, throughout this facility and in dealings with third parties. This is a coordinated effort that requires the commitment, participation, and compliance of facility personnel and third parties associated with this facility.

Emerald Physiotherapy & Rehabilitation will continue to identify and limit the purposes for which information is collected and inform the public of our information handling practices in ways that are understandable and accessible. We must also continue to implement reasonable administrative safeguards to ensure the privacy and security of personal and personal health information. It is also essential that this facility remain open in its information handling practices, making related policy and practice information available to the public, in addition to granting access to personal information and providing avenues of recourse if necessary.

We are directly accountable to ourselves, the clients, Provincial and Federal Governments, and the Saskatchewan College of Physical Therapists for our handling of this information. This includes but is not limited to ongoing and regular reviews of our information handling practices, as well as, updating and expanding our Policies and Procedures to meet or exceed the current standards of practice and legislative requirements.

This facility is responsible for the protection of personal and personal health information and the fair handling of it at all times. Care in collecting, using, and disclosing this information is essential to continued customer confidence and goodwill.

To fulfil this obligation, this facility has adopted the 10 principles of information handling as outlined in the *Personal Information Protection and Electronic Documents Act of Canada* (2004).

Therefore, **our responsibilities** with regards to handling personal and personal health information as outlined in the Act are as follows:

1. Be Accountable

Comply with all 10 principles of information handling.

Appoint a Privacy Officer to be responsible for the facility's compliance.

- Provide the Privacy Officer with the necessary management support and authority to intervene on privacy issues relating to any of the facility's operations. Inform the public and facility personnel of the name, title, and responsibilities of the Privacy Officer.

Protect all personal information held by this facility or transferred to a third party.

- Analyze all personal information handling practices including ongoing activities and new initiatives. More specifically: what personal and personal health information is collected and what it is used for; why, how, and when it is collected; where it is stored and how it is secured; who has access to or uses the information; to whom it is disclosed; and when it is disposed of.

Develop and implement personal information policies and practices.

- Develop, review, and implement policies and procedures that cover information management issues such as: defining the purpose of collection; obtaining consent; limiting information collection, use, and disclosure; information accuracy; security; retention and destruction; access requests; complaints & inquiries.

2. Identify the Purpose

Identify what personal and personal health information is required and how it will be used.

- Review the personal information holdings of the facility to ensure they are all required for a specific purpose.
- Share and document this information with facility personnel and clients either orally, or in writing.

Document why the information is collected.

Inform the individual client from whom the information is collected why it is needed.

- Share this information with the client either orally, or in writing.

Identify any new purpose for the information and obtain the individual's consent before using it.

- Obtain consent either expressed or implied.

3. Obtain Consent

Inform the individual of the purposes for the collection, use or disclosure of personal information.

- Communicate in a manner that is clear and can be reasonably understood.
- Ensure that facility personnel are able to answer an individual's questions about information collected and management of the information.

Obtain the client's consent before or at the time of collection, as well as when a new use is identified.

- Record the consent received. (note in file, consent form, etc.)
- Obtain consent via ethical means...never obtain consent by deceptive means, or as a condition for supplying a product or service.
- Explain to individuals the implications of withdrawing their consent.

4. Limit Collection

Collect only information that is necessary for the identified purpose. Do not collect personal and personal health information indiscriminately.

- Identify in policies and practice the type of information the facility collects.

Inform individuals accurately about the reasons for collecting personal and personal health information. Do not deceive or mislead.

- Ensure that staff are adequately informed/trained in the information management issues of the facility so that they can accurately share this information with others in an understandable form.

5. Limit Use, Disclosure, and Retention

Use and disclose information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act (2004).

- Document any new purpose for the use of personal or personal health information.

Retain personal information only as long as necessary to satisfy the purposes and implement procedures to ensure that the information is current.

Develop and implement policies and procedures with respect to record retention and destruction that meet provincial and federal privacy requirements, and comply with professional regulatory standards.

- Institute maximum and minimum retention periods.
- Dispose of information that no longer has a specific purpose or that no longer fulfills its intended purpose.

Retain personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.

Destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

- Dispose of personal information in a way that prevents improper access.

6. Be Accurate

- Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.
- Keep personal information as accurate, complete and up to date as necessary, taking into account its use and the interests of the individual.
- Update personal information only when necessary to fulfil the specified purposes.
- Keep frequently used information accurate and up to date unless there are clearly set out limits to this requirement.

7. Use Appropriate Safeguards

Protect personal and personal health information against loss or theft.

- Develop and implement policies and procedures to protect personal information within the facility and with dealings with other parties/organizations.
- Educate facility personnel of the importance of maintaining security and confidentiality of personal and personal health information.

Safeguard the information from unauthorized access, disclosure, copying, use or modification.

- Use appropriate and effective physical safeguards (locked filing cabinets, restricting access to office, etc.), technological tools (passwords, firewalls, etc.), and organizational controls (confidentiality agreements, staff training, etc.) to provide necessary protection.
- Educate and train facility personnel on a regular basis with regards to facility information handling practices, policies, and security safeguards.

Protect personal information and select appropriate safeguards that take into account the sensitivity of the information, the amount of information, the extent of distribution, format of the information (electronic, paper, etc.), and type of storage.

8. Be Open

Inform customers, clients, and facility personnel of policies and procedures for the management of personal and personal health information.

- Educate and train facility personnel to enable them to respond to individual inquiries.

- Make available:

name and title of individual within the organization who is accountable for privacy policies and practices,

name and title of individual to whom access requests should be sent,

how an individual can gain access to his or her personal and personal health information,

how an individual can submit a complaint,

brochures or other information that explain policies, standards, or codes, and

a description of what personal information is made available to other organizations and why it is disclosed.

Ensure that policies and procedures are understandable and easily available.

- Make available, information about policies and practices, in person, in writing, or by telephone.

9. Give Individuals Access

Inform individuals (when requested), if you have any personal &/or personal information about them.

Explain how it is or has been used and provide a list of any organizations to which it has been disclosed.

Grant individuals access to their information.

- Assist individuals to prepare a request for access to personal or personal health information.
- Respond to requests no later than 30 days after receipt of the request. Response time may be extended if responding to the request within 30 days would unreasonably interfere with facility activities, if additional time is necessary to conduct consultations, if additional time is necessary to convert personal information to an alternate format.
- Notify the individual if facility extends the response time past the 30 days of receiving the request, and of his or her right to complain to the Privacy Commissioner.
- Give access at minimal or no cost to the individual and notify the individual of the costs before processing the request.
- Provide the requested information to the individual in an understandable format (including descriptions of abbreviations), and make available the information in alternate formats such as tape recordings or translated copies, if necessary.

Correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient.

- Send any information that has been amended, where appropriate, to any third parties that have access to the information.

Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in Section 9 of the Act (2004).

- Inform the individual in writing when refusing to give access, setting out the reasons and any recourse available.

10. Provide Recourse

Develop complaint procedures that are easily understood and accessible.

- Record the date a complaint is received and the nature of the complaint.

Inform complainants of available avenues of recourse.

Investigate all complaints received.

- Acknowledge receipt of the complaint promptly.
- Contact the individual to clarify the complaint, if necessary.
- Assign the investigation to a person with the skills necessary to conduct it fairly and impartially.
- Give the investigator access to all relevant records, employees or others who handled the information or access request.
- Notify individuals of the outcome of investigations clearly and promptly, informing them of any relevant steps taken.
- Correct any inaccurate information.

Correct/modify information handling practices and policies as necessary based on the outcome of complaints.

Note any disagreement on the file and advise third parties where appropriate.

References: The Office of the Privacy Commissioner of Canada (2004), *Personal Information Protection and Electronic Documents Act*, Section 1.