



Privacy: What Physical Therapists Need to Know

The Legislation

There are two privacy Acts in British Columbia: FOIPPA and PIPA.

Freedom of Information & Protection of Privacy Act (FOIPPA)

Governs public organizations (such as hospitals, health authorities, etc.)

FOIPPA guarantees the right of the public to gain access to, and request correction of, personal information collected about them by public organizations. It also prevents the unauthorized collection, use, or disclosure of personal information by public organizations. FOIPPA does not apply to personal information contained in private clinics.

Physical therapists working in public practice will not typically need to be involved in the creation of privacy policies – large healthcare organizations and institutions will have a Privacy Officer, privacy policies, technology infrastructure, and other resources already in place, and which must be followed by all staff.

Personal Information Protection Act (PIPA)

Governs private organizations (such as private physical therapy clinics, etc.)

PIPA applies to private clinics and the physical therapists within them. All clinics must comply with rules regarding the collection, use, and disclosure of personal information.

The core principle of PIPA is that personal information should not be collected, used, or disclosed without the prior knowledge and consent of the client. There are some exceptions (Section 18) and there are key privacy principles and policies that all clinics need to have in place in order to be in compliance with the legislature.

Physical therapists working in private practice need to be aware of PIPA and privacy requirements in their practice.

Below is what physical therapists in private practice need to know about PIPA.



You Need to Have a Privacy Officer

Put Someone in Charge: PIPA Requires This

A privacy officer is responsible to help clients understand how personal information is being managed and is responsible for ensuring compliance with PIPA.

If there is a breach of privacy – reported by a client, a clinic therapist, yourself, or someone outside of your clinic – an investigation may be conducted by the police and/or the Office of Information and Privacy Commissioner (OIPC) of British Columbia. One of the first questions you will be asked is to identify your privacy officer. Be sure you have designated someone!

What Does a Privacy Officer Do?

The privacy officer must understand what kind of information is covered under PIPA, how to collect information, what information is required from clients, what information to disclose, to whom it can be disclosed and why, when consent from the client will be required and when it is not, how clients can access their own records, how clients can request corrections to their records, and what fees can be charged for access. The privacy officer is responsible for ensuring that the clinic's privacy policy (see below) and procedures are fully implemented and working effectively.

Does this sound daunting? It shouldn't be. It's likely that you and your clinic have already put in place lots of privacy measures. A privacy officer just needs to collect all the strategies you are already doing and document them a bit more formally.

There are lots of resources available to help you and your privacy officer get things organized:

- College Privacy Toolkit
- The OIPC has very comprehensive guidance documents available on their site at <https://www.oipc.bc.ca/guidance-documents/1438>



- The BC government website has some clearly outlined privacy principles found at <https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information/principles>
 - [Request for Access to Personal Information](#)
 - [Correcting Personal Information](#)
-

You Need to Understand “Personal Information” & “Consent”

Personal Information

Personal information is any information about an identifiable individual, excluding contact information and work product information. It includes an individual's gender, age, ethnic origin, race, identification numbers, financial and credit information, personal health information, consumer preference information, religious affiliations, donation history, travel history, personal habits, and personal history.

Maintaining confidentiality is a fundamental responsibility of physical therapists, and is a central part of the therapist-client relationship. The client ultimately owns their personal information (including their health information), but you, as their physical therapist, act as an accountable custodian of the information that you collect. You must protect its disclosure. As stated earlier, **the core principle of PIPA is that personal information should not be collected, used, or disclosed without the prior knowledge and consent of the client.**

Consent

You always need **informed consent** from a client to collect, use, or disclose personal information. But there are many forms of consent – verbal or written consent, explicit consent, implicit consent, implied consent.... It's important to understand what is meant by each of these, and what is required by law according to PIPA.



To validly consent, clients must have a reasonable understanding of what information will be collected, who will have access to it, how it will be used, and to whom it may be disclosed.

Sometimes, it's enough to seek **implied informed consent**. An example of this might be when you provide a new client with a brochure or written / verbal information about how the clinic bills for services or for other administrative tasks. Providing the information means the client has been informed of your billing or invoicing policies and procedures. It is implied that they are informed and have consented unless they say otherwise. You can also provide them with information about your privacy policy and the strategies you use to protect their personal information in accordance with PIPA. But PIPA states that the information has to be in a form that the *individual can reasonably be considered to understand*. Consider how you will provide information to those whose first language is not English, or who are unable to read or understand English.

But implied informed consent is not always enough. For many situations during physical therapy care, you will want to seek **explicit consent** from your client. To provide explicit consent, the client needs to be informed about what personal information they are providing and for what purpose, and then actively agree to that information being collected and disclosed as described. Explicit consent can be given in writing or verbally – but if you rely on verbal consent, you might be asked later to prove that consent was given by the individual. Documenting the verbal consent in the client record is one way to prove this later.

Remember: Clients are able to withdraw consent at any time, subject to legal or contractual reasons and reasonable notice.

Which Consent is the Right One?

The answer is – it depends. You have to consider how sensitive the information is, what purpose it will be used for, what the client (or another individual) would reasonably consider to be appropriate, and the circumstances of the collection/disclosure. OIPC suggests that you should obtain explicit consent (verbally or in writing) whenever possible, especially when the personal information is sensitive.

Example: You have documented consent from your client to share information about his therapy goals and treatment plan with others involved in his recovery. You receive a request from his family physician for an update about his return to



work date; you likely would consider the consent already obtained adequate to cover this request and therefore you provide the physician with the information requested. The next day you receive a request from your client's employer to provide an update about his return to work date. **Would you share this information?** This information may be more sensitive from the client's perspective, and so it would be advised to seek explicit consent from the client before sharing information with his employer.

Example: You have worked with a family and their child for three years and the child is now transitioning into kindergarten. The family has provided consent for you to write a report for the school team, outlining the involvement you have had and to provide some of the child's history and progress to date. Because you have worked with the family for several years, you are aware that the mother has had some mental health challenges which you think are important for the school to be aware of, in order to best understand the child. **Would you share this information?** Again, while the family was comfortable providing consent for a report to be written, this particular piece of information is sensitive. You would be advised to get explicit consent from the family before including this information in the report to the school.

Remember: In general you should not rely on implied consent if the information you are sharing is particularly sensitive, or if you are sharing it outside of the immediate health care team.

The OIPC has resources on their website from the Office of the Privacy Commissioner of Canada called Obtaining meaningful consent found at <https://www.oipc.bc.ca/guidance-documents/2255>. The section of page 8 titled *Determining the Appropriate Form of Consent* is especially helpful.

There are some exceptions (Section 18 of PIPA). PIPA states that there some circumstances when consent does not need to be obtained prior to disclosing personal information. These are described in the Act and in the OIPC Guidance document above, and include situations such as when you receive a subpoena, or when an individual may be at risk of harm. Be sure to review the exceptions should a situation arise where you are unsure about whether or not you can disclose without consent.

You Should Conduct a “Privacy Review”

Review How Your Practice Handles Personal Information



- This could be something done by your newly-appointed privacy officer, or you could have the staff do this together. The first question to ask is “What personal information do we collect and how does our clinic currently manage it?”
- take an inventory of the personal information you currently have
- identify the information needs of the different functions within your clinic
- identify your current information practices (including how and why your clinic collects, uses, and discloses personal information)

Then consider whether your current practices meet the PIPA obligations.

Identify Gaps & Implement Changes

If you see practices that could be improved, document them, and then make a plan to fix them. Should there be an investigation after a breach, this documentation will help you demonstrate that you were aware of the PIPA requirements and were working towards policies and procedures to ensure you were in compliance. Be sure that you document the changes you’re making along the way in recognition of any gaps, also.

You Need to Have Privacy & Complaints Policies

Develop & Follow Privacy Policies: PIPA Requires This

Your policy needs to be available for review by clients and by staff, and should cover not only the collection, use and disclosure of personal information, but also:

- How information will be safeguarded by physical, technological, and organizational security measures
- How to ensure personal information is collected accurately and disposed of properly
- How to give clients notice of why you are collecting information about them and how to obtain and record consents and handle withdrawals of consent
- How you will maintain the privacy of your employee’s personal information

Remember that personal information is contained on much more than client charts or electronic medical records. Computer screens, conversations, phone calls,



emails, faxes, photocopiers, courier deliveries, and other media all need safeguarding.

Develop & Follow a Complaints Process (Related to Privacy)

PIPA requires you to create a process for handling privacy complaints. It is always more efficient for you to resolve complaints through your privacy officer than to involve an outside regulator (for complaints about privacy and confidentiality, the College of Physical Therapists of BC, and, failing a successful resolution, the Office of the BC Information and Privacy Commissioner). Your process should be easily accessible, simple to use, and quick to provide to individuals who inquire about your complaints process. Having an effective complaints-handling process is an important part of managing privacy risks within your clinic, and will be one of the first things asked for should an investigation be launched.

All Individuals Involved with Your Practice Need to Know Your Policies & Processes

There is no point having a privacy officer and policies in place if they are not followed. Be sure that your clinic's privacy plan includes a program to train staff about privacy procedures and policy. It is your staff members who will be responsible for consistently complying with the privacy principles on a client-by-client basis. Every one of your employees, associates, contractors, partners, or agents who collect, use, or disclose personal information will need to understand what they must do to comply with PIPA's privacy principles and your clinic's privacy policy. Consider having everyone sign a confidentiality agreement that confirms they are aware of, and have been trained in, PIPA and your clinic's privacy policy.

Questions?

You can always contact the Practice Advisors at the College to ask questions about privacy policies and PIPA requirements.



College of
**HEALTH AND CARE
PROFESSIONALS OF BC**

The Office of the Information and Privacy Commissioner for BC is very helpful regarding individual inquiries also – contact the office at info@oipcbc.ca or (250) 387-5629.