AUSTRALIAN
PHYSIOTHERAPY
ASSOCIATION

Is your privacy policy up to scratch?

australian.physio

Maintaining the privacy of your patients' personal information, including their health information, is not just a professional and ethical responsibility; it is legal one as well.

Privacy laws impose a range of responsibilities on you, many of which are quite demanding because of the sensitive nature of the information that you collect, use and sometimes disclose about your patients (the law says that **all** health information is, by definition, sensitive).

There are several different types of information-handling disclosure documents you might also routinely provide to your patients at, during or shortly after your first interaction with them.

In this document, we focus on the written privacy policy which every health professional in private practice, even a sole practitioner, is required to have. In it, we set out:

- a template (with commentaries) which you might want to use to check against your current policy (if you have one) in order to see whether you need to update or change it in any way
- links to resources to help you develop or update your written privacy policy.

The minimum information that a Privacy Policy must contain includes telling your patient:

- what information you collect about them, how you collect it and why you collect it
- how, and when, you propose to use (internally) and share/disclose (externally) that information
- what right they have to seek access to information you hold about them, and to seek correction of that information
- what right they have to complain about your information-handling practices, and to whom
- whether you are likely to disclose information about them to overseas recipients, and if so, more detail about when and why you do that, and where the recipients are based.

The level of detail in your policy will really depend on the size of your practice, how much and what type of information you collect, use and disclose, how you store and secure the information and whether you transfer information overseas.

For that reason, it's important to modify this resource to make sure it properly records your (lawful) information-handling practices and does not either over or understate them.

Once you've satisfied yourself that your privacy policy is up to scratch, you must then make it freely available to patients so that they know that you have one, and they know how and where to find it. You might want to display it at practice reception, refer to it in key documents eg. registration forms and other notices, or — if you have a website — on your website.

Remember though: complying with the law means more than creating the right paperwork. Every physiotherapist has an independent obligation to identify how the law requires them to behave, and to then comply with those requirements. Fortunately, privacy regulators have provided a lot of helpful material on the topic. We set out links to some of that material later.

A disclaimer from the APA – and a warning

This resource is intended for you to use as a guide only. It might not be relevant to your particular practices or your particular circumstances. If the resource describes a practice which you do not actually do, you either need to:

1. modify the document or (and maybe more importantly)
2. modify your practice to make sure it complies with the laws paraphrased in the resource.

In any event, you will need to exercise your own skill and judgement when seeking to adopt or adapt this resource. And you may want to seek appropriate professional advice as well.

As this is a general resource only, the APA disclaims any and all liability (including liability for negligence) to any users of this resource. That disclaimer extends to any loss or damage, cost or expense incurred or that arises by reason of relying on this resource in any manner.

Some preliminary thinking and some preliminary planning you might want to consider

Creating a privacy policy requires more than simply generating a nice-looking document; it needs to reflect the realities of your information handling practices, and to reflect what the law requires and permits you to do with information about your patients.

It is also part of a broader set of responsibilities you have to be proactive in establishing, implementing and maintaining privacy processes in your practice.

Recently, the Office of the Australian Information Commission (OAIC) released its 'Guide to Health Privacy', which describes the key practical steps you might want to take to embed privacy into your practice:

- develop and implement a privacy management plan
- develop clear lines of accountability for privacy management
- create a documented record of the types of personal information you handle
- understand your privacy obligations and implement processes to meet those obligations
- hold staff training sessions on privacy obligations
- create a privacy policy
- protect the information you hold
- develop a data breach response plan.

That's quite a lot of ground to cover. But at a minimum, and before finalising or updating your own privacy policy, you might want to think about doing the following things:

- **remind yourself about the law:** all physiotherapists in private practice must comply with the Commonwealth Privacy Act and the Australian Privacy Principles (APPs) contained within it (physiotherapists in some states and territories might also have to comply with state and territory legislation). The OAIC has provided lots of accessible information pitched at the health professions to help them through these issues, and we provide some useful links from them at the end of this document
- **check whether your current practices meet the requirements of the law – and if they don't, make sure they do:** once you've got a better feel for what the APPs say and require of you, consider how each of them is currently being handled within your practice. Are there any major gaps? Are you doing things wrong? You might need help to sort through some of these issues (eg, consulting with your liability insurer)
- **check with relevant people when developing/modifying your privacy policy (and other privacy – related practices):** it's always a good idea to check in with internal and external stakeholders to see what they think about your current practices. Internal stakeholders include staff and contractors. External ones include patients and other service providers. You might be surprised by what you find.

Privacy policy: a possible template

Privacy Policy of *[insert name of your practice; make it clear whether this policy covers just a sole practice or whether it extends to a larger entity or a group of practices]*

Our commitment to your privacy

We are committed to handling personal information about you, including health information about you, in accordance with the requirements of the Commonwealth Privacy Act 1988.

In this Policy, we explain:

- what kind of information we collect and hold about you
- how and why we collect it
- what we do with that information and who we share it with (and when)
- your right to seek access to, and if required correction of, the records we hold about you
- your right to make a privacy complaint, to us and others
- whether we are likely to disclose information about you to overseas recipients.

What kind of personal information do we collect about you?

We collect and hold the following kind of information about you:

- your name, address, date of birth, email and contact details
- information about your family or relatives
- information about other health professionals involved in your care
- any government identifiers such as Medicare number, DVA number. However, we do not use these for the purposes of identifying you in our practice
- other health information about you such as:
  - a record of your symptoms, your relevant medical history, the diagnosis made and the treatment we give you
  - specialist reports
  - test results
  - your appointment and billing details
  - your prescriptions
  - your healthcare identifier
  - your help fund details
  - other information about you collected for the purposes of providing care to you.

How do we collect and hold your personal information?

We will generally collect personal information about you in these ways:

- directly from you when you give us your details (eg, face-to-face, over the phone, via registration form or an online form)
- from a person responsible for you
- from a third party where we are permitted by law to do that (eg. other health care professionals involved in your care, from your health insurer, from the My Health Record system etc.).

Why do we collect and use information about you?

We primarily collect and use personal information about you to provide our physiotherapy services to you and to communicate with you and others involved in your care in relation to those services.

We also sometimes use that information for other purposes, including:

- to help us manage our accounts and administrative services, including billing, arrangements with health funds, pursuing unpaid accounts, management of our IT systems and
- to conduct accreditation, quality assurance or internal audits.

When and why might we share information about you with others?

We may disclose information about you to others outside of our practice as permitted or required under law. This will include situations where we disclose information about you in order:

- to comply with our legal obligations (eg. mandatory reporting under legislation, responding to a court order or subpoena)
- to consult with other health professionals involved in your healthcare
- to get test results from diagnostic and pathology services
- to claim on insurance
- to communicate with your health fund, with government and other regulatory bodies such as Medicare
- to help us manage our accounts and administrative services (eg. billing or debt recovery, arrangements with health funds, pursuing unpaid accounts etc.) *[note to physiotherapist: if you use the My Health Record, you might want to add a reference to it here eg, 'if you have My Health Record, to upload and to download personal information about you from it'.*
- to lessen or prevent a serious threat to a patient's life, health or safety or a serious threat to public health or safety
- to help in locating a missing person
- to establish, exercise or defend an equitable claim through the My Health Record
- to prepare the defence of anticipated or existing legal proceedings
- to discharge notification obligations to liability insurers.

Your right to seek access to and to seek correction of the information we hold about you

You have the right to seek access to and correction of the personal information we hold about you.

[Note to physiotherapist: if you propose to charge for giving access, you will need to mention this here eg, 'We will usually charge a small fee for giving access'.]

We will normally respond to your request within 30 days. To make the request, you should contact *[note to physiotherapist — insert details here, or direct the reader to the contact details which need to appear later in this document]* in writing *[note to physiotherapist: by law, an access request does not have to be in writing; a verbal request will often be enough. But it might be more efficient from a practice perspective to have a paper trail, particularly if there's going to be some sensitivity or controversy surrounding access issues].*

If you think that the information we hold about you is not correct, let us know in writing. We will take reasonable steps to correct your personal information where the information is not accurate or up-to-date. From time to time, we may also ask you to verify that the information we hold about you is correct and current. And please notify us if and when your contact details change (see 'how to contact us').

Security: how we hold your personal information

We take reasonable steps to protect the information we hold about you. These are designed to prevent unauthorised access, modification or disclosure and to prevent misuse and loss. This includes:

[Note to physiotherapist: provide some details here of how you hold information about your patients and what steps you take to hold it securely. Examples that might apply to your practice include:

- *holding information in a lockable cabinet*
- *holding information on an encrypted database*
- *holding information in secure cloud storage*
- *getting staff to sign confidentiality documents*
- *providing staff with training or induction etc. about confidentiality and (in particular) security issues*
- *access to information restricted on a 'need to know' basis and*
- *strong password protections when accessing the information on a computer.*

Your right to receive treatment from us anonymously (or by using a pseudonym)

Where it is lawful and practicable for us to do so, you can be treated anonymously or through use of a pseudonym (a name other than yours).

Disclosing information about you overseas

[Note to physiotherapist: if you will not be disclosing patient information overseas, or are unlikely to do so, use this text] We do not propose to disclose information about you to anyone overseas. If we want to transfer your personal information overseas, we will first seek your consent, unless we are required by law to do the transfer.

[Note to physiotherapist: if you do or might disclose information about the patient overseas, you need to let the patient know. For instance:] We may disclose your personal information to the following overseas recipients:

- any health professional who helps us to provide our physiotherapy services to you (eg. health professionals who treated you when you were overseas) or anyone else you authorise us to contact
- overseas cloud-based storage
- *[note to physiotherapist: add any other overseas recipients to whom you disclose information about the patient. Note, the routing of personal information in transit through an overseas-based server is not — of itself — 'disclosure' under privacy law. You therefore do not need to mention that. But if the patient information ultimately ends up with an overseas recipient, you need to mention that].*

If you have a privacy-related concern about us

If you have concerns about the way we've handled your privacy, let us know. You should do that in writing. We will then try to respond to you within 30 days.

If you are not satisfied with our response, you can refer your complaint to the Office of the Australian Information Commission, whose contact details are:

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Post: GPO Box 5218 Sydney New South Wales 2001

Website: https://www.oaic.gov.au/privacy/privacy-complaints/

Updating this policy

We will update this policy from time to time, to reflect any changes in our information-handling practices or the law or both.

We will notify you of changes to the policy by *[note to physiotherapist: think about the most efficient way to bring the policy changes to the attention of your patients, and then add in text to spell that out here. By displaying the updates at the reception desk? By posting it on your website, if you have one?].*

How to contact us

To contact us about any privacy related issues, please approach: *[note to physiotherapist: insert contact details for privacy contact officer here. Of course, that person's identity might change over time. If you can, think about creating a generic "privacy@…" email address to make sure that even after staff change, there is still some way for patients to get in touch easily, and without having to go beyond reading this document].*

AUSTRALIAN
PHYSIOTHERAPY
ASSOCIATION

australian.physio