



## PhysiYoga Privacy and Information Management Policy and Procedures

### Policy

PHYSIYOGA will comply with:

- the Privacy Act 1988 and the Privacy Amendment Act 2012 to protect the privacy of individuals' personal information
- Note: South Australia does not have any specific [additional legislative requirements](#).

This policy outlines the systems in place governing the appropriate collection, use, storage and disclosure of personal information, access to and correction and disposal of that information. Physiotherapy students will have access to client files for training and research purposes.

### Outcome

Compliance with legislative requirements governing privacy of personal information.

All PHYSIYOGA Clients are satisfied that their personal information is kept private and only used for the intended purpose

### Background

The [Privacy Act 1988](#) (Privacy Act) is an Australian law which regulates the handling of personal information about individuals by private sector organisations. Amendments were made to this legislation in 2012 (the Privacy Amendment Act 2012) which updates the [Australian Privacy Principles](#) (APP) and came into effect in March 2014. The amendment requires an organisation to explicitly state how they will adhere to the APP and inform their Clients on how their privacy will be protected. The APP cover the collection, use, storage and disclosure of personal information, and access to and correction of that information. The APP are summarised in Appendix 1 of this document.

### Definitions

'Personal information' means information (or an opinion) we hold (whether written or not) from which a person's identity is either clear or can be reasonably determined.

'Sensitive information' is a particular type of personal information - such as health, race, sexual orientation or religious information.

### Procedure

*Ensuring all PHYSIYOGA Staff Understand Privacy and Confidentiality Requirements*

1. The Director of PHYSIYOGA will review their Privacy Policy annually and ensure they understand their responsibility to protect the privacy of individuals' personal information.
2. All Staff will undergo training related to Privacy and Confidentiality Requirements at the time of induction and then annually.

*Managing Privacy of Client Information Storage*

1. Client information collected is kept in an individual Client record.
2. Each Client record has a unique identification number
3. A Client record includes: personal information • clinical notes • investigations • correspondence from other healthcare providers • photographs • video footage.



4. Client details are managed through Nookal which uses compliant security measures. Details can be found here: <https://www.nookal.com/au/security> A Firewall is used in the software system as a means of protecting information stored on the computer. Other security related procedures such as user access passwords, multi-factorial authentication also assist with the protection of information.
5. Paper records are kept in locked, fireproof cabinets.
6. Client information is stored for seven years post the date of last discharge. In the case of Clients aged under 18 years, information is kept until their 25th birthday and 7 years post discharge.
7. Client related information, or any papers identifying a Client are destroyed by shredding and deleting from the computer and all databases.
8. User access to all computers and mobile devices holding Client information is managed by passwords and automatic inactive logouts.

#### *Managing Privacy and Confidentiality Requirements of Clients of the NDIS*

1. PHYSIYOGA refers to their Privacy Policy on the Client's NDIS Service Agreement.
2. The NDIS Service Agreement includes 5 Consents:
  - I. Consent for sharing and obtaining Information
  - II. Consent for receiving services
  - III. Consent for photography
  - IV. Consent to participate in Client Satisfaction Surveys
  - V. Consent to participate in Quality Management Activities

These consents are discussed with the Client and /or their decision maker in a way they can understand prior to the commencement of service.

#### *Managing Privacy and Confidentiality Requirements of all PHYSIYOGA Clients*

3. Persons contacting PHYSIYOGA with an enquiry do not need to provide personal details. However, once a decision is made to progress to utilising PHYSIYOGA's services, personal and sensitive information will need to be collected.
4. PHYSIYOGA may need to share pertinent Client information with other professional Allied Health Professional at the time of case conferencing or when determining support plans. Information is only shared in order to provide the best service possible and is only shared with those people whose Professional Codes of Ethics include privacy and confidentiality. Permission to share information is sought from the Client prior to the delivery of services and as required at other points of intervention as / if required.
5. Personal information is not disclosed to third parties outside of PHYSIYOGA, other than for a purpose made known to the Client and to which they have consented, or unless required by law.
6. Clients are informed there may be circumstances when the law requires PHYSIYOGA to share information without their consent.

#### *Keeping Accurate Client Information*

Clients are informed of the need to provide us with up to date, accurate and complete information.



PHYSIYOGA staff update information on the Client record at the time of reviews or when they become aware of change in information.

AHP staff at PHYSIYOGA update the Client record as soon as practical after the delivery of services to ensure information is accurate and correct.

#### *Using Client Information for Other Purposes*

Under no circumstances will PHYSIYOGA use personal details for purposes other than stated above, unless specific written consent is given by the Client or their representative, or as outlined through current state or federal government health mandates.

#### *Client Access to Their Information*

Clients have the right to access the personal information PHYSIYOGA holds about them. To do this, Clients must contact the Director of PHYSIYOGA.

#### *Management of a Privacy Complaint*

1. If a person has a complaint regarding the way in which their personal information is being handled by PHYSIYOGA, in the first instance they are to contact the Director. The complaint will be dealt with as per *the Complaints Management Policy*. If the parties are unable to reach a satisfactory solution through negotiation, the person may request an independent person (such as the [Office of the Australian Privacy Commissioner](#)) or the [NDIS Quality and Safeguards Commission](#) to investigate the complaint. PHYSIYOGA will provide every cooperation with this process.

#### **Reference**

- ['Guidelines on Privacy in the Private Health Sector', Office of the Australian Information Commissioner](#)

## Appendix 1: Summary of the 13 Australian Privacy Principles

### **APP 1 — Open and transparent management of personal information**

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

### **APP 2 — Anonymity and pseudonymity**

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

### **APP 3 — Collection of solicited personal information**

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

### **APP 4 — Dealing with unsolicited personal information**

Outlines how APP entities must deal with unsolicited personal information.

### **APP 5 — Notification of the collection of personal information**

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

### **APP 6 — Use or disclosure of personal information**

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

### **APP 7 — Direct marketing**

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

### **APP 8 — Cross-border disclosure of personal information**

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

### **APP 9 — Adoption, use or disclosure of government related identifiers**

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

### **APP 10 — Quality of personal information**

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

### **APP 11 — Security of personal information**

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

### **APP 12 — Access to personal information**

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

### **APP 13 — Correction of personal information**

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.