Physio Right*

Privacy and Information Management Policy and Procedures

*Physio Right refers to Owner/Principal Physiotherapist and all Contractors.

Policy

Physio Right will comply with:

- Disability Services Act (1993)
- NDIS Practise Standards Provider Governance and Operational Management Module (Information Management)
- Standard 1 of the National Standards for Disability Services.
- The South Australian privacy committee handles privacy complaints related to state government agencies' compliance with a set of Information Privacy Principles
- The Health and Community Services Complaints Commissioner also receives complaints about government, private and non-government health and community services.

Physio Right will manage and store information in accordance with the Privacy Act.

This includes implementing systems to govern the appropriate collection, use, storage, disclosure, access, correction, and disposal of personal information.

Outcome

- Compliance with legislative requirements governing privacy of personal information.
- All Physio Right participants are satisfied that their personal information is kept private and used only for the intended purpose.

Background

The Privacy Act 1988 (Privacy Act) sets out regulations for the handling of personal information about individuals by private sector organisations. In 2012, amendments were made to this legislation (the Privacy Amendment Act 2012), updating the Australian Privacy Principles (APP), which came into effect in March 2014. The amendment requires organisations to explicitly outline their adherence to the APP and inform their participants about how their privacy will be protected. The APP cover the collection, use, storage, and disclosure of personal information, as well as access to and correction of that information. The APP are summarised in Appendix 1 of this document.

The South Australian Privacy Committee and Health and Community Services Complaints Commissioner regulate how long personal health information must be retained.

Definitions

- *Personal information* refers to any information (or an opinion) held by us (whether written or not) from which an individual's identity is clear or can be reasonably determined.
- *Sensitive information* is a specific type of personal information, including health, race, sexual orientation, or religious data.

Procedure

Ensuring All Physio Right Contractors Understand Privacy and Confidentiality Requirements

The Owner/Principal Physiotherapist of Physio Right will review the Privacy Policy annually to ensure all Contractors understand their responsibility to protect the privacy of individuals' personal information.

Physio Right Contractors will undergo an information session and instructional training upon commencement and annually thereafter regarding Privacy and Confidentiality Requirements. This training is recorded in the Human Resource Log.
Contractors, or those backfilling for leave or sickness, will sign a contract that includes a Confidentiality and Security Agreement, along with a Contractor Checklist to confirm they have read this agreement. They will be required to provide 100 points of ID and a current police check. They must also sign off on reading all other Physio Right policies and procedures before commencing service. As part of the Service Agreement, participants are informed that Physio Right may need to backfill for leave, which may require sharing participant information with the backfill contractor. The contractor is obligated to comply with the Privacy and Confidentiality agreements and will be dismissed immediately if a breach is identified. Participants also have the option to cancel the service or request not to be contacted by the contractor during this time.

Managing Privacy of Participant Information Storage

Participant information collected is stored in an individual participant record.
A participant record includes:

- Personal information
- Clinical notes
- Investigations
- Correspondence from other healthcare providers
- Photographs
- Video footage

Contractors are permitted to access the computer case noting system to perform the service.

A password-protected file is used by Contractors to protect information stored on the

computer. Other security procedures, such as user access passwords and multi-factor authentication, further protect the information.
Paper records are stored in locked cabinets.
Participant information is retained for seven years after the last discharge. For participants under 18 years old, information is retained until their 25th birthday and/or 7 years post-discharge.

Participant-related information, or any papers identifying a participant, is destroyed through shredding and deleting from computers and all databases.
User access to all computers and mobile devices holding participant information is managed by passwords and automatic inactive logouts.
Participant information is shared only with another Physio Right Contractor if they are working directly with that participant. Contractors can only view participant information on Halaxy for those participants to whom they provide support.
Email accounts and case-noting systems are protected by two-factor authentication for each user.

Physio Right records case-notes and stores participant information on the online case-noting system, Halaxy. Physio Right uses Halaxy to accurately record the time spent supporting participants and send corresponding invoices. Halaxy has a Privacy Policy that complies with the Privacy Act 1988 (Cth), including the Australian Privacy Principles under the Act. Halaxy operates from Melbourne and stores data within Australia in securely protected data centres with multiple backups. This data is protected by 256-bit bank-grade security and encryption, meaning patient (participant) records, notes, and payment information are protected to the same level required by Australian banks. In accordance with their Data Security Policy, they do not have access to participant information.
Information on Halaxy's Security can be found at: Halaxy Security
Halaxy can be contacted on 1800 984 334 or via email: community@halaxy.com.

Managing Privacy and Confidentiality Requirements of Participants
Physio Right refers to their Privacy Policy within the participant's NDIS Service Agreement. The NDIS Service Agreement includes four consents, plus other pertinent consents to the organisation:

1. Consent for sharing and obtaining information
2. Consent for receiving services
3. Consent to participate in participant satisfaction surveys
4. Consent to participate in quality management activities

These consents are discussed with the participant and/or their decision-maker in a way they can understand before the commencement of service.
Individuals contacting Physio Right with an enquiry do not need to provide personal details. However, once they decide to proceed with Physio Right's services, personal and sensitive information will need to be collected.
Physio Right may need to share relevant participant information with other support, care, or

therapy services. Information is only shared to provide the best service possible and is only shared with professionals whose codes of ethics include privacy and confidentiality.
Permission to share information is sought from the participant before service delivery and as required at other points of intervention.
Personal information is not disclosed to third parties outside of Physio Right unless required by law or if consent has been given for a specific purpose.
Participants are informed that there may be situations when the law requires Physio Right to share information without their consent.

Keeping Accurate Participant Information
Participants are informed about the need to provide accurate, up-to-date, and complete information.

Physio Right updates participant records at the time of reviews or when they become aware of changes.

Physio Right updates participant records as soon as practicable after service delivery to ensure the information is accurate and correct.

Using Participant Information for Other Purposes
Under no circumstances will Physio Right use personal details for purposes other than those outlined above, unless specific written consent is provided by the participant or their representative.

Participant Access to Their Information
Participants have the right to access the personal information Physio Right holds about them. To do so, participants must contact the Owner/Principal Physiotherapist of Physio Right.

Management of a Privacy Complaint
If a person has a complaint regarding how their personal information is being handled by Physio Right, they should first contact the Contractor providing the service and then the Owner/Principal Physiotherapist. The complaint will be handled according to the Feedback Complaints Management Policy. If a satisfactory solution is not reached through negotiation, the individual may request an independent investigation by the Office of the Australian Privacy Commissioner or the NDIS Quality and Safeguards Commission. Physio Right Coordination will provide full cooperation with this process.

Management of a Data Breach
If Physio Right suspects a data breach has occurred, the following steps will take place:

1. Determine the likely cause of the breach. The Contractor will complete the Data Breach form and send it to the Owner/Principal Physiotherapist.

2. The Owner/Principal Physiotherapist will document what has occurred and which participant information may have been shared.
3. The Contractor will contact the participants whose information may have been disclosed, advising them of the breach, the information shared, and the steps being taken.
4. Contact the NDIS Fraud Line on 1800 650 717 and inform them of the breach, providing the participant's name and NDIS number, along with the type of information shared.
5. Report the data breach to the Office of the Australian Information Commissioner (OAIC) via their website: OAIC Data Breach Report.
6. Inform any participants' Plan Managers about the breach, advising them to be mindful of suspicious emails from Physio Right.
7. Review the cause of the breach and create a plan for improvement and strategies to reduce the likelihood of future occurrences (e.g., Contractor education about suspicious emails).

Steps Physio Right Takes to Minimise a Data Breach

- Backing up files weekly to an external hard drive and a password-protected iCloud account.
- Storing hard copies in a locked filing cabinet.
- Enhancing email security with two-factor login and increased spam filters via Australian-based email provider, VentraIP.
- Using VPN and anti-virus/malware protection on Contractors' computers.

Website

Email addresses, names, phone numbers, resumes, and cover letters submitted via Physio Right's website are sent directly to an email address viewed by the Owner/Principal Physiotherapist. This email address is protected by two-factor authentication with a webmail provider based in Australia—Venta IP.

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.