Physio Right*

Privacy and Information Management Policy and Procedures

*Physio Right refers to Owner/Principal Physiotherapist and 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 having in place systems governing the appropriate collection, use, storage and disclosure of personal information, access to and correction and disposal of that 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 only used for the intended purpose.

Background

The *Privacy Act 1988* (Privacy Act) provides regulations for 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 participants 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.

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

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 Physio Right Contractors Understand Privacy and Confidentiality Requirements

1. The Owner/Principal Physiotherapist of Physio Right will review their Privacy Policy annually and ensure all Contractors understand their responsibility to protect the privacy of individuals' personal information.
2. Physio Right Coordinator's will undergo an information session and instructional training when they commence and then annually that relate to Privacy and Confidentiality Requirements. This is recorded in the Human Resource Log.
3. Contractors, or those backfilling for leave or sickness will sign a *Contract* which includes *Confidentiality and Security Agreement* , as well as sign a *Contractor Checklist* to show they have reads this agreement. They are required to provide 100 points of ID and have a current police check. They will also sign off on reading all other Physio Right policies and procedures prior to commencing the service. As part of the Service Agreement, participants are aware at times Physio Right may need to backfill for leave and as such share participant information with this Contractor. The Contractor has an obligation to abide by Privacy and Confidentiality agreements and if any breach is shown will be dismissed immediately. The participant also has the option to request to cancel the service or not be contacted by the Contractor during this time.

Managing Privacy of Participant Information Storage

1. Participant information collected is kept in an individual participant record.
2. A participant record includes: personal information • clinical notes • investigations • correspondence from other healthcare providers • photographs • video footage.
3. Contractors permitted to access the computer case noting system to perform the service.
4. A password protected file is used by Contractors as a means of protecting information stored on the computer. Other security related procedures such as user access passwords, multi-factor authentication also assist with the protection of information.
5. Paper records are kept in locked cabinets.
6. Participant information is stored for seven years post the date of last discharge. In the case of participants aged under 18 years, information is kept until their 25th birthday and / or 7 years post discharge.
7. Participant related information, or any papers identifying a participant are destroyed by shredding and deleting from the computer and all databases.
8. User access to all computers and mobile devices holding participant information is managed by passwords and automatic inactive logouts.
9. Participant information is shared only with another Contractor of Turning point Support, if they are working directly with this participant. Contractors can only view participant information on Halaxy for those participant to whom they provide support.
10. Email accounts and Casenoting system is protected by two factor authentication for each user.

Physio Right record case-notes and store participant information on an online case-noting system- Halaxy. Physio Right use Halaxy as an accurate way to record the day and time spent support participants and to send a corresponding invoice. Halaxy have a Privacy Policy, which includes the Privacy Act 1988 (Cth) ("Privacy Act") (including the Australian Privacy Principles under that Act); health records legislation, including the Health Records Act 2001 (Vic), Health Records and Information Privacy Act 2002 (NSW), Health Records (Privacy and Access) Act 1997 (ACT); and marketing legislation, including the Spam Act 2003 (Cth) and the Do Not

Call Register Act 2006 (Cth). Halaxy operates from Melbourne, and store data within Australia in securely protected data centres with multiple back-ups in place. 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: Halaxys https://www.halaxy.com/article/security
Halaxy can be contacted on 1800 984 334 or via email: community@halaxy.com.

Managing Privacy and Confidentiality Requirements of Participants

1. Physio Right refers to their Privacy Policy on the participant's NDIS Service Agreement.
2. The NDIS Service Agreement includes 4 Consents plus other pertinent consents to your organisation :
    I. Consent for sharing and obtaining Information
    II. Consent for receiving services
    III. Consent to participate in Participant Satisfaction Surveys
    IV. 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 prior to the commencement of service.
3. Persons contacting Physio Right with an enquiry do not need to provide personal details. However, once a decision is made to progress to utilising Physio Right's services, personal and sensitive information will need to be collected.
4. Physio Right may need to share pertinent participant information with other support, care or therapy services. 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 participant 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 Physio Right, other than for a purpose made known to the participant and to which they have consented, or unless required by law.
6. Participants are informed there may be circumstances when the law requires Physio Right to share information without their consent.

Keeping Accurate Participant Information

Participants are informed of the need to provide us with up to date, accurate and complete information.
Physio Right update information on the participant record at the time of reviews or when they become aware of change in information.
Physio Right update the participant record as soon as practical after the delivery of services to ensure information is accurate and correct.

Using Participant Information for Other Purposes

Under no circumstances will Physio Right use personal details for purposes other than stated above, unless specific written consent is given 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 this, participants must contact the Owner/Principal Physiotherapist of Physio Right.

Management of a Privacy Complaint

1. If a person has a complaint regarding the way in which their personal information is being handled by Physio Right, in the first instance they are to contact the Contractor providing the service and then the Owner/Principal Physiotherapist. The complaint will be dealt with as per *the Feedback 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. Physio Right Coordination will provide every cooperation with this process.

Management of a Data Breach

If Physio Right suspects a data breach has occurred then the follow steps will take place:

1. Determine the likely cause of the data breach. Contractor will complete Date Breech form and send to Owner/Principal Physiotherapist.
2. The Owner/Principal Physiotherapist will make notes about what has occurred and who's information may have been shared.
3. Contractor will contact participant/s who's information may have been disclosed as part of the breach. Advise them of the type of breach, what information of theirs may have been shared and steps we are now taking.
4. Contact NDIS Fraud Line on 1800 650 717 and advise of the breach. Advise who's information may have been shared as part of the brach (provide participants name and NDIS no) and what information this in includes.
5. Report the data breach on the Office of the Australian Information Commissioner (OAIC) via their website. https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/
6. Inform any participants Plan Managers about the breach, and to be mindful of any suspicious emails from Physio Right.
7. Review what lead to the breach and create a plan for improvement and strategies to minimise the likelihood of this occurring again ie Contractor education about suspicious emails.

Steps Physio Right takes to minimise a data beach

1. Backing up files weekly to an external hard drive and to a password protected iCloud account
2. Keeping hard copies in a locked filing cabinet
3. Increased security on emails. Two factor log in and increased spam filter set up with Australian based email provider- VentraIP.
4. VPN and Anti Virus and Malware Protection on Contractors computers.

Website

Email addresses, names, phone numbers and any resumes and cover letters provided through Physio Right's website are sent directly to an email address, viewed by the Owner/Principal Physiotherapist. This
email address is protected by 2 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.