Privacy and Information Management Policy and Procedures

Policy
Doctoroo will comply with:

- the Privacy Act 1988 and the Privacy Amendment Act 2012 to protect the privacy of individuals' personal information
- add any additional legislation for the relevant state / territory as listed in the OAIC - additional legislative requirements.

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 Doctoroo participants 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 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.

Additional legislation for the relevant state / territory (as listed in the OAIC: additional legislative requirement) 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 Doctoroo Staff Understand Privacy and Confidentiality Requirements

1. The Director of Doctoroo 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 Participant Information Storage

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

4. Security related procedures such as user access passwords, multi-factorial authentication 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 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.

Managing Privacy and Confidentiality Requirements of Participants

1. Doctoroo refers to their Privacy Policy on the participant'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 Participant Satisfaction Surveys
    V. 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 Doctoroo with an enquiry do not need to provide personal details. However, once a decision is made to progress to utilising Doctoroo's services, personal and sensitive information will need to be collected.
4. Doctoroo may need to share pertinent participant 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 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 Doctoroo, 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 Doctoroo 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.

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

AHP staff at Doctoroo 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 Doctoroo 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 Doctoroo holds about them. To do this, participants must contact the Director of Doctoroo.

Management of a Privacy Complaint
1. If a person has a complaint regarding the way in which their personal information is being handled by Doctoroo, 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. Doctoroo 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.