Privacy and confidentiality

Version: 2
Published: 20 Oct 2020, 7:29 PM
Last edited: 20 Oct 2020, 7:28 PM
Approved: 20 Oct 2020, Sarah Tilley
Next review: 3 Sep 2021

Context

Connect Allied Health are committed to handling and protecting personal information in accordance with the NDIS and relevant privacy legislation. In collecting, maintaining and storing information, CAH will uphold an individual's right to privacy whilst also ensuring relevant data is collected to maximise participant outcomes.

The information we collect is used to provide services to participants according to their individual needs, meet duty of care obligations, initiate appropriate referrals, and conduct business activities to support those services.

This policy applies to all personal information, including sensitive personal information, used and held by the organisation for participants and workers.

Applicability

When
• applies to all personal information and sensitive personal information including the personal information of employees and participants. • applies to all company confidential information - that is any information not publicly available.

Who
• applies to **all** representatives including key management personnel, directors, full time workers, part time workers, casual workers, contractors and volunteers.

What is personal information?

Personal information includes, but is not limited to (regardless of its accuracy):

- name
- address
- phone number
- email address
- date of birth
- recorded opinions or notes about someone
- any other information that could be used to identify someone.

What is sensitive personal information?

Sensitive personal information can include personal information that is normally private such as:

- health information
- ethnicity

- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexuality
- criminal record
- biometric information (such as finger prints).

What is a data breach?

A data breach is type of security incident where personal, sensitive or confidential information normally protected, is deliberately or mistakenly copied, sent, viewed, stolen or used by an unauthorised person or parties. A data breach where people affected by the data breach are at risk of serious harm as a result, is reportable to the Office of the Australian Information Commissioner.

Privacy and confidentiality guidelines

- we are fully committed to complying with the privacy requirements of the *Privacy Act*, the *Australian Privacy Principles* and for *Privacy Amendment (Notifiable Data Breaches)* as required by organisations providing disability services
- we are fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework and relevant state or territory requirements
- we provide all individuals with access to information about the privacy of their personal information
- individuals have the right to request access to their personal records by requesting this with their contact person
- where we are required to report to government funding bodies, information provided is non-identifiable and related to services and support hours provided, age, disability, language, and nationality
- personal information will only be used by us and will not be shared outside the organisation without your permission unless required by law (e.g. reporting assault, abuse, neglect, or where a court order is issued)
- images or video footage of participants will not be used without their consent
- participants have the option of being involved in external NDIS audits if they wish.

Privacy and Dignity

Outcome: Each participant accesses supports that respect and protect their dignity and right to privacy. To achieve this outcome, the following indicators should be demonstrated:

- Consistent processes and practices are in place that respect and protect the personal privacy and dignity of each participant.
- Each participant is advised of confidentiality policies using the language, mode of communication and terms that the participant is most likely to understand.
- Each participant understands and agrees to what personal information will be collected and why, including recorded material in audio and/or visual format.

Information management

Outcome: Management of each participant's information ensures that it is identifiable, accurately recorded, current and confidential. Each participant's information is easily accessible to the participant and appropriately utilised by relevant workers. To achieve this outcome, the following indicators should be demonstrated:

- Each participant's consent is obtained to collect, use and retain their information or to disclose their information (including assessments) to other parties, including details of the purpose of collection, use and disclosure. Each

participant is informed in what circumstances the information could be disclosed, including that the information could be provided without their consent if required or authorised by law.
- Each participant is informed of how their information is stored and used, and when and how each participant can access or correct their information, and withdraw or amend their prior consent.
- An information management system is maintained that is relevant and proportionate to the size and scale of the organisation and records each participant's information in an accurate and timely manner.
- Documents are stored with appropriate use, access, transfer, storage, security, retrieval, retention, destruction and disposal processes relevant and proportionate to the scope and complexity of supports delivered.

Security of information

- we take reasonable steps to protect the personal information we hold against misuse, interference, loss, unauthorised access, modification and disclosure.
- personal information is accessible to the participant and is able for use by relevant workers
- security for personal information includes password protection for IT systems, locked filing cabinets and physical access restrictions with only authorised personnel permitted access
- personal information no longer required is securely destroyed or de-identified.

Data breaches

- we will take reasonable steps to reduce the likelihood of a data breach occurring including storing personal information securely and accessible only by relevant workers
- if we know or suspect your personal information has been accessed by unauthorised parties, and we think this could cause you harm, we will take reasonable steps to reduce the chance of harm and advise you of the breach, and if necessary the Office of the Australian Information Commissioner.

Breach of privacy and confidentiality

- a breach of privacy and confidentiality is an incident—follow the Manage incident process to resolve
- a breach of privacy and confidentiality may require an investigation
- an intentional breach of privacy and confidentiality will result in disciplinary action up to and including termination of employment.

Legislation

The National Disability Insurance Scheme Act 2013 (NDIS Act)

The Privacy Act 1988 (Privacy Act)