Privacy and confidentiality

Version: 7
Published: 4 Oct 2023, 12:48 PM
Last edited: 4 Oct 2023, 12:47 PM
Approved: 4 Oct 2023, Sarah Tilley
Next review: 4 Oct 2024

Context

Connect Allied Health (CAH) 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, full time workers, part time workers, casual workers, contractors and the director.

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.

Policy Statement

CAH collects, holds, uses and discloses personal information from a range of individuals through services and organisational activities. This Policy outlines CAH's commitment to upholding participant privacy when managing personal information. As required by the Privacy Act 1988 (Cth), CAH manages personal information in accordance with the 13 Australian Privacy Principles which govern standards, rights and obligations around:

- The collection, use and disclosure of personal information.
- An organisation or agency’s governance and accountability.
- Integrity and correction of personal information.
- The rights of individuals to access their personal information.

Principles

Why We Collect and Use Personal and Sensitive Information:

CAH collects and uses personal information when it is necessary for service delivery and organisational activities, or otherwise required by law. The personal information provided by participants, representatives and key stakeholders involved as per the participant/representative's preferences, is our primary source data collection.

Privacy and confidentiality guidelines

- We protect the personal information of the people we support.
- We only collect personal information for purposes directly related to CAH services, e.g., allied health supports, from the participant, their representative, or other key stakeholders as per the participant/representative's preferences.
- We always obtain consent to collect personal information. The people we support may choose to remain anonymous although this may limit the services then available to support them.
- We obtain consent from the participant/representative before referring to other service providers.
- We only use personal information for the purpose for which it was provided to us, for related purposes or as required or permitted by law.
- 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.
- Each participant is advised of confidentiality policies using the language, mode of communication and terms that the participant is most likely to understand.

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.
- We have put in place a range of security mechanisms including (but not limited to) user authentication, access controls, firewalls and security monitoring.
- 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.

Disclosing Your Personal Information

CAH will not disclose personal or sensitive information unless:

- You have provided written consent to do so.
- The use or disclosure of the personal information is required by law, a court/tribunal order, police or other enforcement body.
- There is suspicion of an offence(s) being committed and the information is needed to act.
- The information is required to lessen or prevent a serious threat to an individual's life, health or safety or to public health or safety.

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 which may result in termination of employment.

Legislation

The National Disability Insurance Scheme Act 2013 (NDIS Act)

The Privacy Act 1988 (Privacy Act)