Privacy and Dignity Policy and Procedure

1.0 Purpose

CareAbility will manage and ensure that we provide the participant access to services and supports that respect and protect their dignity and right to privacy.

2.0 Scope

This policy applies to all Staff.

3.0 Policy

CareAbility is committed to protecting and upholding all stakeholders' rights to privacy and dignity, including participants, Staff, management and representatives of other service agencies.

CareAbility is committed to protecting and upholding the participants' rights to privacy and dignity as we collect, store and handle information about them, their needs and the services provided to them.

CareAbility requires Staff and management to be considered and consistent when writing documents regarding a participant and when deciding who has access to this information.

CareAbility is subject to NDIS Quality and Safeguards Commission rules and regulations. CareAbility will follow the guidelines of the Australian Privacy Principles in its information management practices.

CareAbility will ensure that each participant and/or the participant's representative understands, and agrees to, the type of personal information collected and the reasons for collection. If material is to be recorded in an audio or visual format the participant and/or the participant's representative must agree to their involvement, in writing, before any material can be collected. The participant and/or the participant's representative must also be informed at the time material is being recorded in an audio or visual format.

CareAbility will advise each participant and/or the participant's representative of our Privacy Policy using the language, mode of communication and terms that the participant is most likely to understand (Easy Read documents are made available to all participants).

CareAbility will ensure that:

- It meets its legal and ethical obligations as an employer and service provider, concerning protecting the privacy of participants and organisational personnel
- Participants and/or the participant's representative are provided with information about their rights regarding privacy and confidentiality
- Participants and/or the participant's representative and organisational personnel are provided with privacy and confidentiality is assured when they're being interviewed or discussing matters of a personal or sensitive nature
- All Staff, management and volunteers understand the necessary requirements to meet their obligations
- Participants and/or the participant's representative are informed of CareAbility's confidentiality policies using the language, mode of communications and terms they're most likely to understand
- CareAbility will attempt to locate interpreters and will use easy access materials.

Privacy and Dignity Policy and Procedure

This policy conforms to the Federal Privacy Act (1988) and the Australian Privacy Principles, which govern the collection, use and storage of personal information.

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals and to interviews or discussions of a sensitive personal nature.

4.0 Procedure

4.1 Dealing with personal information

In dealing with personal information, CareAbility Staff will:

- Ensure privacy for the participants, Staff, or management when they are being interviewed or discussing matters of a personal or sensitive nature
- Collect and store personal information that is only necessary for the functioning of the organisation and its activities
- Use fair and lawful ways to collect personal information
- Collect personal information only with consent from the individual
- Ensure that people know of the type of personal information collected; the purpose of keeping the information; the method used when information is collected, used
- Or disclosed; who'll have access to information
- Ensure that personal information collected or disclosed is accurate, complete, and up-to-date and provide access to the individual to review information or correct wrong information about themselves
- Take reasonable steps to protect all personal information from misuse, loss and unauthorised access, modification or disclosure
- Destroy or permanently de-identify personal information no longer needed or after legal requirements for retaining documents that have expired
- Ensure that participants understand and agree with the type of personal information being collected and the reason/s for collection
- Ensure participants are advised of any recordings in either audio or visual format. The participant's involvement in any recording format must be agreed to, in writing, before collection of material takes place.

4.2 Participant records

Participant records will be kept confidential and only handled by Staff directly engaged in the delivery of service to the participant. Information about a participant may only be made available to other parties with the consent of the participant, or their advocate, guardian or legal representative. A written agreement providing permission to keep a recording must be stored in the participant's file.

All hard copy files of participant records will be kept securely in a locked filing cabinet, in the office of Director.

4.3 Responsibilities for managing privacy

All Staff are responsible for the management of personal information to which they have access. The Director or their delegate is responsible for the content appearing in CareAbility publications, communications, and on our website, and must ensure the following:

- Appropriate consent is sought and obtained for the inclusion of any personal information about any individual, including CareAbility personnel (see 'Consent Policy and Procedure').
- Information provided by other agencies or external individuals conforms to our privacy principles.
- Our website contains a Privacy Statement that clearly outlines the conditions regarding any collection of personal information from the general public captured via their visit to the website

The Director or their delegate is responsible for safeguarding personal information relating to CareAbility's Staff, management and contractors. The Director or their delegate will be responsible for:

- Ensuring that all Staff are familiar with the Privacy Policy and administrative procedures for handling personal information
- Providing participants and other relevant individuals with information about their rights regarding privacy and dignity
- Handling any queries or complaints about a privacy issue

4.4 Privacy information for participants

During the first interview, participants and/or the participant's representative are notified of the information being collected about them, how their privacy will be protected, and their rights concerning this data. Information sharing is part of our legislative requirements. Participants and/or the participant's representative must provide consent to any information sharing between our organisation and government bodies. The participant is informed they can opt-out of any NDIS information sharing during audits.

4.5 Privacy for interviews and personal discussions

To ensure privacy for participants or Staff when discussing sensitive or personal matters, CareAbility will only collect personal information which is necessary for the provision of supports and services and which:

- Is given voluntarily
- Will be stored securely on the CareAbility database.

When in possession, or control, of a record containing personal information, CareAbility will ensure that the record shall be protected against loss, unauthorised access, modification or disclosure, by such steps as is reasonable in the circumstances. If a record must be provided to a person in connection with the provision of a service to CareAbility, everything reasonable will be done to prevent unauthorised use or disclosure of that record.
CareAbility will not disclose any personal information to a third party without an individual's consent, unless that disclosure is required or authorised by, or under, law.

5.0 Related documents

- Consent Policy and Procedure
- Participant Handbook (with Easy Read Supplement)
- Privacy & Confidentiality Agreement
- Service Agreement

6.0 References

- NDIS Practice Standards and Quality Indicators 2021
- Privacy Act (1988)

- Australian Privacy Principles (Commonwealth)

Management of Data Breach Policy and Procedure

1.0 Purpose

To meet legislative compliance requirements as a mandatory reporter of eligible data breaches to both the Office of the Australian Information Commissioner (OAIC) and any individuals who may be potentially affected by a data breach; to inform relevant authorities of any breach; and to limit and reduce risks to the business and ensure continuous improvement in maintenance of data held by our organisation.

2.0 Scope

All Staff are required to maintain the confidentiality of all data relating to participants and other Staff members.

This policy relates to all personal data regarding both participants and team members.

3.0 Definition

Terminology	Description
Data Breach (Eligible Data Breach)	• Unauthorised access to or unauthorised disclosure of personal information or personal information is lost in circumstances where unauthorised access to, or unauthorized disclosure of the information is likely to occur. • A reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.
Likely (likely to result in serious harm)	is to be interpreted to mean more probable than not
Reasonable Person	is to be taken to mean a person in CareAbility who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach. OAIC's guidance states that the reasonable person is not to be taken from the perspective of an individual whose personal information was part of the data breach or any other person, and, generally, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach.

Likely to result in serious harm/ potential forms of serious harm	An assessment as to whether an individual is likely to suffer 'serious harm' because of an eligible data breach depends on, among many other relevant matters: • The kind and sensitivity of the information subject to the breach; • whether the information is protected and the likelihood of overcoming that protection; • If a security technology or methodology is used in relation to the information to make it unintelligible or meaningless to persons not authorised to obtain it - the information or knowledge required to circumvent the security technology or methodology; • The persons, or the kinds of persons, who have obtained, or could obtain, the information; and • The nature of the harm that may result from the data breach. Could include physical, psychological, emotional, economic and financial harm as well as harm to reputation.
Remedial action	There are a number of exceptions to the notification obligation, including importantly where an entity is able to take effective remedial action to prevent unauthorised access to, or disclosure of, information when it is lost or to prevent any serious harm resulting from the data breach. Where such remedial action is taken by an entity, an eligible data breach will not be taken to have occurred, and therefore an entity will not be required to notify affected individuals or the OAIC.
Suspicion of an eligible data breach	If CareAbility merely suspects that an eligible data breach has occurred, but there are no reasonable grounds to conclude that the relevant circumstances amount to an eligible data breach, the entity must undertake a "reasonable and expeditious assessment" of whether there are in fact reasonable grounds to believe that an eligible data breach has occurred.
Assessment time frame	Within 30 days after the day, it became aware of the grounds that caused it to suspect an eligible data breach.

Personal Information	Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is identifiable in the circumstances. For example, personal information may include: • An individual's name, signature, address, phone number or date of birth • Sensitive information • Credit information • Staff member record information • Photographs • Internet protocol (IP) addresses • Voiceprint and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique) • Location information from a mobile device (because it can reveal user activity patterns and habits)

4.0 Policy

CareAbility views data breaches as having serious consequences, so the organisation must have robust systems and procedures in place to identify and respond effectively.

CareAbility will delegate relevant Staff members with the knowledge and skills required to become a Response Team member.

Staff are required to inform Director or their delegate of the potential, or suspected data breach immediately. Within forty eight (48) hours, the Director or their delegate is to complete a Data Breach Process Form and ensure that, as a regulated entity, they notify the particular individuals and the Commissioner about eligible data breaches as soon as practicable (no later than thirty (30) days after becoming aware of the breach or suspected breach).

If a Staff member becomes aware that there are reasonable grounds to believe that there has been an eligible data breach, CareAbility are required to promptly notify any individuals at risk of being affected by the data breach and the OAIC.

CareAbility will undertake the following when an eligible data breach has occurred:

1) Prepare a statement that, at a minimum, contains:
    a) CareAbility contact details:
        i) If relevant, the identity and contact details of any entity that jointly or simultaneously holds the same information, in respect of which the eligible data breach has occurred, e.g. due to outsourcing, joint venture or shared services arrangements. If information

of this sort is included in the statement, the other entity will not need to report the eligible data breach separately

b) A description of the data breach
c) The kinds of information concerned
d) The steps it recommends individuals take to mitigate the harm that may arise from the breach (while the entity is expected to make reasonable efforts to identify and include recommendations, it is not expected to identify every recommendation possible following a breach).

2) Provide a copy of the prepared statement to the OAIC using online Notifiable Data Breach Form.
3) Undertake such steps, as are reasonable in the circumstances, to notify affected or at-risk individuals of the contents of the statement. Individuals will be notified by email, telephone or post, depending on the situation; if direct notification is not practicable CareAbility will publish the statement on its website and take reasonable steps to publicise its contents.

5.0 Procedure

5.1 Stage 1. Assess and determine the potential impact

- Once notified of the potential data breach, the Director or their delegate must consider whether a privacy data breach has (or is likely to have) occurred and then make a preliminary judgement as to its possible severity. Advice on how to manage the data breach should be sought from appropriate managerial Staff.
- Criteria for determining whether a privacy data breach has occurred:
    - Is personal information involved?
    - Is the personal information of a sensitive nature?
    - Has there been unauthorised access to personal information, or unauthorised disclosure of personal information or loss of personal information, in circumstances where access to the information is likely to occur?
- Criteria for determining the severity of the breach:
    - Type and extent of personal information involved
    - Number of individuals that have been affected
    - If information is protected by any security measures (password protection or encryption)
    - Type of person/s who now have access
    - Whether there is (or could be) a real risk of serious harm to the affected individuals
    - If there could be media or stakeholder attention due to the breach/suspected breach.
- With respect to the above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in Section 26WG of the National Data Breach Act

Director or their delegate and relevant Staff will take a preliminary view as to whether the breach (or suspected breach) may constitute a Notifiable Data Breach. Accordingly, the Director will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team); this will depend on the nature and severity of the breach.

5.2 Stage 2. Select appropriate data breach management option

Option 1 - Data breach managed at a local level by managerial Staff

1. The Director or their delegate will ensure implementation of immediate corrective action, if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
2. A Data Breach Process Report is to be completed within 48 hours of receiving instructions. The report will contain the following:
    - Description of the breach or suspected breach
    - Summary of action taken
    - Summary of outcomes from the action taken
    - Outline of processes implemented to prevent a repeat situation
    - Recommendation outlining why no further action is necessary.
3. The Director or their delegate will sign-off, confirming that no further action is required.

Option 2 - Data breach managed by the Data Breach Response Team

1. When the Director instructs that the data breach be escalated to the Response Team, the Director will convene the Response Team and notify any relevant managerial Staff.
2. The Response Team will consist of:
    - Director or their delegate
    - Human Resources (or nominee)
    - Information Technology (or nominee)
    - Marketing and external relations (or nominee)
    - Other person/s nominated by the Director.

5.2.1 Primary role of the Data Breach Response Team

There is no single method of responding to a data breach. Each incident must be dealt with, on a case by case basis, by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team, as appropriate:

1. Immediately contain the breach, if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system
2. Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach, having regard for the information outlined above
3. Call upon the expertise of, or consult with, relevant Staff in specific circumstances
4. Engage independent cybersecurity or a forensic expert, as appropriate
5. Assess whether serious harm is likely (with reference above and to Section 26WG of the National Data Breach Act)
6. Make a recommendation to the Director whether this breach constitutes an NDB for mandatory reporting to the OAIC; and the practicality of notifying affected individuals
7. Consider developing a communication or media strategy including the timing, content and method of any announcements to participants, Staff or the media
8. The Response Team must undertake its assessment within 48 hours of being convened

5.2.2 Secondary role of the Data Breach Response Team

Once the data breach has been dealt with appropriately, the Response Team should turn its attention to the following steps:

1. Identify lessons learnt and remedial action that can be taken to reduce the likelihood of a recurrence; this may involve a review of policies, processes and refresher training.
2. Prepare a report for submission to senior management.
3. Consider conducting an audit to ensure that necessary outcomes are affected and effective.

5.3 Stage 3. Notify the Office of the Australian Information Commissioner

- Taking into consideration the Response Team's recommendation, the Director will determine whether there are reasonable grounds to suspect that a Notifiable Data Breach has occurred
- If there are reasonable grounds, the Director must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach)

6.0 Relevant documents

- Data Breach Process Report
- Notifiable Data Breach

7.0 References

- NDIS Practice Standards and Quality Indicators 2021
- Privacy Act 1988
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act)