

Confidentiality and Information Sharing Policy

1. Policy

Participants have both an ethical and legal right to privacy and confidentiality. Staff will recognise and respect each Participant's right to privacy and confidentiality in all aspects of their life.

Privacy is the state of being free from unsanctioned intrusion. This means the right to keep information and activities secret and of being kept out of the presence or view of others.

Confidentiality is respecting the confidence of another or discretion in keeping secret information.

All Participants' information kept by RenaissCare is recorded, maintained, stored and made available in ways that respect Participants' rights to privacy and confidentiality. Except in cases of emergency, the Participant's consent is obtained before information is sought or released.

Information regarding Participants is not passed on to their families without the Participant's or their legal guardian's permission. Information is only disclosed against the wishes of the Participant or legal guardians in certain circumstances. Such circumstances include any situation that poses a serious threat to the life, safety or health of any individual or other legal or legislative requirements.

RenaissCare will in all aspects of its operation comply with the *Privacy Act 1988 and The Privacy Amendment (enhancing privacy protection) Act 2012*. This legislation gives people who engage with private organisations the right to know what information an organisation holds about them and the right to correct/amend inaccurate or out of date information. All organisations are required to comply with the principles contained within the legislation. The intent of the act is to protect personal privacy by establishing rules for collecting, using, storing, securing and disclosing personal information.

Requirements under the Act

Under the Act RenaissCare must take reasonable steps to ensure that Participants/families/staff/government bodies and non-government service providers are aware:

- That RenaissCare may collect personal information from them
- Of the purpose for which this information is being collected
- To whom RenaissCare may pass that information onto

The legislation requires that all information RenaissCare obtains from individuals is to be:

- Collected by fair and honest means without intimidation/deception.
- To be stored in a safe and secured manner when not in use. Storage of all personal documents should be held in a locked area.
- Management are responsible for the secure disposal of confidential information.
- Accurate and up to date.
- Able to be corrected if it is not accurate.
- Only used for the primary purpose for which it was collected (unless consent is provided from the individual/family member/carer/guardian to collect information for a secondary purpose).
- Able to be accessed upon request unless special exemptions apply (see procedure).

The Legislation does not try to stop organisations collecting information. The Legislation encourages organisations to be more transparent about why they are collecting information and what they are doing with the information.

RenaissCare must at all times, ensure all Participants' records are kept confidential and used in accordance with what they are intended to be used and not disclose the information in accordance with *Disability Services Act 2006* Division 7 s198 (3), Section 9 of the *Disability Services Regulation 2017* and Chapter 4, Part 2 of the *National Disability Insurance Scheme Act 2013*.

2. Purpose

To provide guidance to RenaissCare employees on the expected standards of confidentiality, professional integrity and judgement expected when disclosing or sharing information about a person with a disability.

3. Scope

All staff of RenaissCare.

4. Procedure

Data and Document Security

Staff are to share the responsibility to protect the security of personal information. All staff are responsible to protect personal information from misuse, loss, unauthorised access or inappropriate disclosure. Personal information will be protected through the following ways:

- All files will be stored in a locked room
- Information will only be available to staff who need access to information
- No unattended files in work areas
- All staff will destroy personal information if the information is no longer needed for the purposes it was collected, taking into consideration any legislative requirements. Appropriate methods of destruction include: Shredding paper records or using an authorised company for secure disposal (e.g. document destruction bins)
- Each Participant has the right to see any information that RenaissCare keep about them
- All information captured is stored electronically and backed-up on password protected back-up servers, so that we may resume Participant service delivery and key communications within 1 – 2 hours of any disaster impacting our primary facilities and systems.

Collection

Staff will only collect relevant personal information to:

- Provide quality services
- Carry out the functions, supports and activities on behalf of the organisation
- Identify emerging or future demand for service
- Meet our statutory, licencing, regulatory or legal requirements

Obtaining Consent

Consent to collect personal information will be sought from Participants at the outset of service engagement, via the terms outlined in the *Service Agreement*, and an *Information Consent Form – Support Coordination*, or *Persons Information Consent Form* is to be completed (whichever applies).

Generally, consent is provided in writing, but if verbal, this is recorded in the Participant file.

Consent to take or use photographs must be obtained for each occurrence.

Use & Disclosure

Staff will maintain confidentiality of personal information.

- Staff shall not disclose or use personal information without the consent of the individual and/or appointed guardian/administrator without the specific written consent of the Participant/guardian. However, relevant information may be used or disclosed on a 'need to know' basis in order to provide a quality service and carry out functions and activities.
- When responding to phone queries, support workers must verify who they are speaking to. If there is any doubt, refer to the matter to their Manager.
- Support workers must not discuss details about a Participant without their permission, or within the hearing range of another person. Conversations on the phone or in the home must always be discreet and not in the public domain. Support workers must always be mindful that the sound of voices can carry within a home.

RenaissCare may disclose or use personal information under the following circumstances:

- If the information is health information and the use or disclosure is necessary for research and compiling statistics relevant to public health and safety;
- If there is a serious and imminent threat to a person's health or safety;
- If there is a reason to suspect that unlawful activity has been engaged in and the use of/or disclosure is required or authorised by government, statutory bodies and/or the law;
- There is a clear possibility of harm;
- There is an agreement of information sharing across departments;
- There is an ethical reason such as the need to protect the person with a disability.

Data Quality (accuracy of information)

Staff will take reasonable steps to ensure that information collected is accurate.

- When collecting, using or disclosing personal information, staff will ensure that the information is accurate and correct and verified by the individual concerned and/or their nominated family member/ carer/ guardian/ administrator/ external service provider.
- This requirement also extends to information collected from statutory bodies (e.g. Office of Public Guardian, Public Trust), State/Federal Government or law enforcement bodies.
- Checking telephone numbers and addresses before sending personal information.

Each document created by RenaissCare, will include the Version number and date of creation.

Openness, Access, and Correction

- Staff will inform individuals about what personal information is held about them, provide access to that information (except where exemptions apply or doing so would be unlawful) and provide the opportunity to correct inaccurate or out of date information.
- Upon request by a Participant, staff will inform the Participant of what personal information RenaissCare holds about them. Individuals do not have to give a reason when asking for access to their own personal information. As part of the request for information, staff may require and ask that the individual provide suitable verification of their identity.
- Where information is provided to an individual, staff will offer:
 - A private environment for the individual to view their personal information
 - A suitably qualified staff member of the Participant's choice to remain with the Participant to view the content and explain the content and information being viewed and the opportunity to correct or amend any incorrect or out- of – date information
- Under the legislation, the following specific situations exempt access to personal information. Exemptions include when:
 - Providing access would pose a serious and imminent threat to the life or health of any individual
 - Providing access would have an unreasonable impact upon the privacy of other individuals
 - The information relates to existing or anticipated legal proceedings between RenaissCare and the individual
 - Providing access to the information may prejudice RenaissCare' negotiations with the individual
 - Providing access would be unlawful
 - Denying access is required or authorised by law and
 - Providing access would prejudice an investigation of possible or alleged unlawful activity

However, if access is denied, staff must provide clear reasons as to why access has been denied and/or give the individual access to those parts of the records/file which are not exempt.

Identifiers

The government assigns identifiers to individuals.

- A government identifier is a unique combination of letters and the numbers (e.g. Medicare number). An identifier assigned by the Commonwealth Government agency must not be adopted, used or disclosed by organisations.
- RenaissCare' position is that when an individual contacts us for general information, we respect their right to exercise anonymity by not providing us with their personal details. However, once an individual accepts a service or support, staff will commence collecting information in accordance with RenaissCare' policy statement regarding the collection of personal information.

Sensitive Information

Under the Legislation, RenaissCare can collect, use, store and disclose sensitive personal and health information provided staff undertake these tasks in a manner that complies with the ten National Privacy Principles (NPPs).

Breach of confidentiality may result in disciplinary action being taken and will be viewed as gross misconduct.

Privacy – Photography Policy

For safety reasons, Participants must not be identified in photographs. At all times the following must apply:

- The Participant must give permission to have their photo taken and if applicable have their decision maker/guardian approval.
- Written consent must be obtained for each individual photo.
- Photos must not contain an identifiable background or signage (for example, company car logos, government logos, etc).
- Participants should not be excluded from beneficial social experiences associated with photographs, videos recording and other published medial such as school photographs and sports club articles, but permission must always be sought from the Participant and/or their decision maker/guardian.
- Consideration should be given to what is in the Participant’s best interests, and to any adverse consequences that may result through the publication of a photograph (for example, safety concerns for the Participant should their whereabouts become known). Consultation should occur with the Participant, RenaissCare’ Management and key stakeholders before publication is allowed.
- If a Support Worker becomes aware of any published information that identifies a Participant, inadvertently or otherwise, they must report this their Manager immediately.

Privacy – Technology and Social Media Policy

Social networking websites and mobile phones have become popular tools for people with a disability, children and young persons to socialise with and share information. Our Participants may be vulnerable to having their personal information used for the purpose of bullying, stalking, their location being identified or exploitation and therefore their personal information should be safeguarded by staff.