

CONFIDENTIALITY & PRIVACY

Activ8 are committed to protecting the confidentiality and privacy of participant's personal information which the organisation collects and administers. Persons dealing with us understand our practices in relation to the management of personal information.

Definition

Personal information (as defined by the Privacy Act 1988)

Is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

Sensitive information (As defined by the Privacy Act 1988)

Is information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, or health, genetic or biometric templates, that is also personal information.

Confidentiality

Implies the relationship of confidence between the organisation and individuals.

Purpose

All systems (operational and service delivery) are developed with the principle of privacy and confidentiality as an integral component. This ensures that legislation, service level agreements and best practice is adopted throughout

Scope

Applies to all staff and contractors engaged in service provision or admin support for NDIS participants

Policy

All new and current records will be administered in accordance with the Australian Privacy Principles and Activ8's record keeping policy.

Staff members have access to this policy document and receive training in privacy principles.

Staff members and contractors sign a privacy and confidentiality agreement form upon commencement with the organisation.

Policies & Procedures are reviewed annually.

In order to meet best practice service provision and associated internal reporting requirements, Activ8 collect personal and health information of participants initially and throughout servicing including:

- Contact details (name, address, email, etc.)
 - Personal details (date of birth, gender, income, emergency contacts, etc.)
 - Information on personal issues and experiences, areas of interest and relationships
 - Family background or supports that participant may have in the community
 - Health information and/or medical history
 - Important cultural information and practices
 - Criminal history
 - Credit card or bank account details, donation history
 - Australian Business Number (ABN)
 - Support plan goals and funding and progress made towards goals
 - Service agreements

The information is collected via a variety of methods including face to face or telephone interview, Artificial intelligence assistance, review of reports and supporting information and information forms and questionnaires.

Subject to consent we may reveal and/or discuss relevant information with other service providers where needed. A copy of the signed consent form is kept accessible on the participant's internal client file and can be provided in response to external requests as needed and in a timely fashion so as not to delay communications.

Information is directly transferred or entered into an electronic case file specific to the participant, including hard copy notes. Activ8 uphold paperless records management, however, should there be a paper-based record, this will be destroyed via shredding/confidential waste bin removal following the information being recorded on the electronic case file.

Participant information is only accessible to appointed key workers/ practitioners, management, and administration staff, thereby reducing the visibility of information to the necessary few. Access to the database is password protected.

Any students on placement at Activ8 may only access files with the consent of the participant or their guardian. All records are backed up to a cloud-based server (hosted in Australia) daily. Testing of the backed-up data occurs monthly and periodically.

The majority of personal, background health and other demographic information is entered at commencement of services, so as to reduce the likelihood of error, new client files may only be created by the administration team or management

Staff who work in our organisation are required to ensure the privacy and confidentiality of the organisation's information and the privacy and confidentiality of the participant's information. Staff must not access inappropriate information or share any information related to their work through social media sites. Any reference to a participant such as a "success story" or publishing participant feedback is actioned only where consent has been granted

Dignity and privacy are further extended to participants, their guardians, and other key stakeholders via the provision of secure and confidential meeting rooms, whereby confidential discussions may take place.

Requests to Access information follow Activ8's policy: Access to Information.

Artificial Intelligence

Activ8 Mind utilise AI technology which has been embedded within our dedicated customer relationships management database (SPLOSE). The technology has been established and tested specifically in relation to the provision of health and allied health information. These AI tools comply with the Australian Privacy Principles. Transcription tools and AI note summaries which are client related remain stored with the SPLOSE CRM which is hosted in Australia.

Activ8 Mind consent forms explicitly reference and seek specific consent for the use of AI technology.

Further information regarding our use of AI is noted in the policy doc
ORG POL Artificial Intelligence

Exemptions for disclosure

A legal requirement to disclose personal information may override the APPs; this is known as a 'duty of care'.

Situations where this may occur include the following:

- Where there is serious risk of abuse or physical harm to the individual or other person, including our participants, the general public and own employees
- Where the disclosure is required under a law
- Where the individual would reasonably expect us to use or give that information, e.g., referral processes
- When the disclosure is necessary by or for a law enforcement agency (e.g., prevention, investigation, prosecution of punishment of criminal offences, protection of public revenue, preparation or implementation of a court or tribunal order.)

In the event that a legal need for disclosure arises, the employee will inform their supervisor or manager prior to making the decision to breach confidentiality and privacy. This decision will also be communicated to the individual, unless such advice to the individual is not allowed by legislation

Associated Documents

Code of Conduct
Consent Form

Consent Form – young person