

# CS3.5 Participant Record Management

## Purpose

1. To provide guidance to all SAVVY employees on effective participant management.

## Alignment with Practice Standards

1. Module 1: Rights and Responsibilities
2. Module 2: Provider Governance and Operational Management

## Legislative Alignment

1. Privacy Act 1988 (Cth)
2. Privacy Amendment (Private Sector) Act 2000
3. Privacy Amendment (Enhancing Privacy Protection) 2012
4. Australian Human Rights Commission Act 1986 (Cth)

## Key Responsible Executive

Chief Executive Officer

## For More Support

Your People Manager

## Policy Statement

1. SAVVY is committed to the collection and storage of appropriate information, which demonstrates compliance with legislative requirements, relevant standards, best practices and expectations of the community it serves.
2. SAVVY will ensure that records are maintained in such a way that they are legible, traceable and accessible. Records will be retained and registered detailing where they are stored or disposed of, as well as who is responsible for the management of this process.

## Definitions

1. Record – information of any kind and in any form that was created, received and maintained as evidence of business or service delivery activities and transactions performed by the organisation.

- Secure – refers to reasonable physical, technical and administrative mechanisms in place to prevent privacy and confidentiality breaches.

## Delegations

Roles	Responsibilities
Board of Directors	<ul style="list-style-type: none"> <li>Endorse and ensure compliance with the Service User Records Policy and Procedure</li> <li>Be familiar with the organisation's legislative requirements regarding privacy and the collection, storage and use of personal information</li> </ul>
CEO	<ul style="list-style-type: none"> <li>Manage and monitor compliance with this policy</li> <li>Support staff competence and compliance with this policy and procedure</li> <li>Develop, disseminate and maintain program and service materials, including service user communication and recording tools</li> </ul>
Management	<ul style="list-style-type: none"> <li>Manage and monitor compliance with this policy</li> <li>Support staff competence and compliance with this policy and procedure</li> <li>Develop, disseminate and maintain program and service materials, including service user communication and recording tools</li> <li>Ensure all staff are equipped to handle complaints in a professional manner and adhere to the complaint management process</li> </ul>
Staff, volunteers, contractors and students	<ul style="list-style-type: none"> <li>Comply with the Service User Record Policy and Procedure</li> <li>Act in accordance with legislation and organisation's systems in place to record and protect privacy and personal information</li> </ul>

## Procedures

- Service user records are an important source of information about themselves, their health and social needs and their treatment. Information in service user files will be complete, accurate and relevant.

2. Establishment of service user files
  - a. Confidential records are held for all service users accepted into SAVVY.
    - i. A service user record is established following completion of intake processes and acceptance into the SAVVY program. In establishing a service user record, the allocated staff member is to clearly explain to the service user:
    - ii. The nature of any personal information to be held by SAVVY
    - iii. How information will be kept secure
    - iv. Under what circumstances information may be disclosed to others
    - v. The process of making a complaint in relation to suspected misuse of personal information
    - vi. How to request access to his/her service record
  - b. Refer to Service User Rights Charter and Feedback Brochure.
3. Service user records structure
  - a. Service User records will be clearly identified with a name and include the following:
    - i. Intake
    - ii. Assessment
    - iii. Rights, responsibilities and legal information
    - iv. Medical information (if relevant)
    - v. Support agreements
    - vi. Consent forms
    - vii. Referrals out
    - viii. Progress notes
    - ix. Case conference minutes and notes
    - x. Correspondence in/out, and
    - xi. Exit information.
4. Development and maintenance of service user records
  - a. The worker will ensure that all sections of the record are complete and up-to-date. Progress notes contain:
    - i. The service user's name
    - ii. Date of entry
    - iii. Page number
    - iv. Entries in service user records are:
      - v. Brief, timely, accurate and complete
      - vi. Factual, objective and sequential
      - vii. Do not contain value judgments or abbreviations
      - viii. Legible, signed, dated and with name of author printed, and
      - ix. Any mistakes are crossed out and initialled, with no liquid paper/white out used.
5. Review of service user files
  - a. The Service Manager will review at least the square root of total service user population plus one file annually to ensure all sections of the file are complete and current and that entries in files are appropriate. The record audit will be based on a random selection of current files and will be completed using the Service User Record Audit Tool.
  - b. Results from the audit will be analysed and used to raise issues of concern and to improve record keeping quality.
6. Retention of service user files
  - a. Service user files are retained at SAVVY due to the possibility that:
    - i. The service user may return to the service
    - ii. Litigation or other legal proceedings, and
    - iii. There will be a need for SAVVY to provide evidence that it fulfilled its duty of care obligations (for example, if a service user became a danger to themselves or others).
  - b. Records of service users who have left the service will be archived after a period of 24 months from the date of the service user's last contact.

- c. Archiving procedures must be adhered to ensuring retrieval of closed records when a service user returns and/or for service user access if and when requested.
7. Disposal of service user records
- a. Records will be destroyed 7 years after the service user ceases to receive SAVVY services.
  - b. Records will be disposed of in a manner which ensures that they cannot be retrieved and protects the privacy of the service user and others.
8. Service user access to files
- a. Service users have the right to access their own information on request. The service user (or their authorised representative) can make a request to access their SAVVY record in writing or by making a verbal request to his/her worker. The staff member will document the request in the record.
  - b. The request is passed to the CEO to assess the request and make arrangements for the service user to view their file:
    - i. File access will be arranged at SAVVY's premises under the supervision of a staff member, at a time which mutually suits the service user , their support person (if applicable) and the staff member
    - ii. The staff member will show the service user the relevant file information, ensuring that the material is returned to the file after it has been viewed or read out (if applicable)
    - iii. The staff member ensures the file is complete, checks that the service user is satisfied with the process, places the access request documentation into the service user file and records a file note indicating the date and time that the service user file was accessed.
  - c. Access will be refused where:
    - i. Providing access would pose a serious threat to the life or health of any person
    - ii. Providing access to the section requested would have an unreasonable impact on the privacy of other people
    - iii. The information relates to legal proceedings between SAVVY and the service user
    - iv. Providing access would be unlawful
    - v. Denying access is required or authorised under another law or has been requested by a law enforcement agency, and
    - vi. Providing access would be likely to prejudice an investigation of possible unlawful activity.
  - d. Where the worker is unsure whether to grant a request to access information in a service user record, the request should be forwarded to the CEO.
  - e. Where SAVVY decides to refuse access, a written reason for the refusal (with the reason relating to the exemptions above) will be provided to the service user. SAVVY is required to respond to a request for access to information in writing within 30 days of receiving the request.
9. Amendment to service user records
- a. The service user (or their authorised representative) can make a request to amend their service user record in writing or by making a verbal request to his/her worker. The staff member will document the request in the record.
  - b. If a service user (or their authorised representative) requests an amendment to the information held in their service user record, you may amend (by way of corrections, deletions or additions) the information to ensure:
    - i. The information is accurate, and
    - ii. The information is relevant, up to date, complete and not misleading, taking into account the purpose for which the information is collected and used.
  - c. If a staff member is unsure whether to grant a request to amend information in a record, the request should be forwarded to the Service Manager.
  - d. SAVVY may refuse a request to amend information contained in a service user record if it is satisfied that the purpose of the amendment does not meet the criteria specified above.

- e. If the Service Manager decides to refuse to amend the service user's record, a written reason for refusal (with the reason relating to the exemptions above) must be given. If the requested amendments are refused, the service user may make a statement about the requested changes, which is to be attached to the record.
  - f. SAVVY is required to respond to a request to amend information in writing within 30 days of receiving the request.
10. Security of service user records
- a. All service user documentation is to be kept securely with consideration given to physical, technical and administrative security safeguards. Refer to the Privacy and Confidentiality Policy.
11. Disclosing information from service user records
- a. Service user information should only be disclosed outside of SAVVY for the primary purpose for which the information was collected. Information may be disclosed for secondary purposes if:
    - i. SAVVY has service user consent
    - ii. There is a serious threat to the health or welfare of any person (including child protection concerns and any notifiable condition under the Public Health Act 1991)
    - iii. Managing a legal claim made by the service user, and
    - iv. Authorised by law e.g. Subpoena or Summons.
  - b. If a request is made for SAVVY to disclose service user information to an external organisation, the request is to be made in writing, identify the person and organisation requesting the information and indicate the reason why the information is being sought.
  - c. Any requests to disclose information to an external organisation should be directed to the CEO.

## References to other SAVVY policies and external sources

- 1. CS1.4 Privacy and Confidentiality

## Summary of attachments

- 1. Nil

## Version Control

- 1. 1 April 2023 - New Policy Creation