# [insert organisation name/logo]

# Personal Records Policy

**Document Status:** **Draft or Final**

**Date Issued:** **[date]**

**Lead Author:** **[name and position]**

**Approved by:** **[insert organisation name] Board of Directors on [date]**

**Scheduled Review Date:** **[date]**

## Record of Policy Review

| Review Date | Person Initiating/Leading Review | Other People Consulted |
|---|---|---|
| | | |

Triggers for Policy Review (tick all that apply)

- ☐ Standard review is timetabled.
- ☐ A gap has been identified
- ☐ Additional knowledge or information has become available to supplement the policy.
- ☐ External factors
  - ☐ Policy is no longer relevant/current due to changes in external operating environment.
  - ☐ There are changes to laws, regulations, terminology and/or government policy.
  - ☐ Changes to funding environment, including requirements of funding bod(y)ies
- ☐ Other (please specify).
- ☐ Internal / organisational factors
  - ☐ A stakeholder has identified a need, eg by email, telephone etc
  - ☐ A serious or critical incident has occurred, requiring an urgent review.
  - ☐ Need for consistency in service delivery across programs and organisations.
  - ☐ Separate, stand-alone policy is now warranted
  - ☐ A near miss has occurred, requiring a review to prevent a serious/critical incident in the future

Additional Comments

[*for example, policy now covers details related to new legislation*].

# Personal Records Policy

## 1. Purpose and Scope

***[if no personal records are kept]*** This policy seeks to ensure that any personal information kept by **[insert organisation name]** is relevant, and is managed in a way that protects individual privacy and confidentiality.

The **[insert organisation name]**'s personal records management system exists to ensure that an information file is created for each individual, that a record of support **[and treatment]** is maintained effectively, and personal privacy and confidentiality are protected.

The policy applies to all staff, volunteers and students involved in the management of personal information.

This policy does not provide detailed information on privacy and confidentiality – refer to the Privacy and Confidentiality Policy.

***[Please see where your CMO sits on the personal records continuum (separate attachment) to assist with identifying underpinning principles for your policy]***

## 2. Definitions

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

Reasonable physical safeguards include:

- Locking filing cabinets and unattended storage areas
- Physically securing the areas in which the health and other personal information is stored
- Not storing health and other personal information in public areas
- Positioning computer terminals and fax machines, or using screen guards, so that they cannot be seen or accessed by unauthorised people or members of the public.

Reasonable technical safeguards include:

- Using passwords to restrict computer access, and requiring regular changes to passwords
- Establishing different access levels so that not all staff can view all information

- Ensuring information is transferred securely (for example, not transmitting health information via non-secure email)
- Using electronic audit trails
- Installing virus protections and firewalls.

Reasonable administrative safeguards include not only the existence of policies and procedures for guidance but also training to ensure staff, Board members, students and volunteers are competent in this area.

An electronic audit trail records details of attempts to create, access, print, copy, alter and/or delete electronic documents

Recovery coordination is the process for facilitating, coordinating and seeking supports from a range of people / organisations, in order to progress towards individual recovery goals. The recovery coordinator drives recovery coordination; it is assumed that the individual receiving support has the capacity to (now, or in the future) be the recovery coordinator for their own journey.

## 3. Principles

Personal files are an important source of information about individuals, their values, aspirations, health, social needs, recovery and support. Information in personal files will be complete, accurate and relevant.

Personal files enhance safety and continuity of care by the accurate recording of personal details and history.

The protection of personal privacy and confidentiality is a guiding principle in the collection, use and storage of personal information.

Effective management of personal files enables **[insert organisation name]** to demonstrate the flow of individual support and make effective use of staff time.

## 4. Outcomes

The personal records management system is systematic, compliant with legislation and quality standards, informative and protects the interests of the individual and **[name of organisation].**

Personal files are effectively established, reviewed, maintained and retained.

Personal information is secure, accessible, relevant and used primarily for the benefit of the individual.

## 5. Functions and Delegations

| Position | Delegation/Task |
|---|---|
| Board of Directors | Endorse Personal Records Policy. |
| Management | Comply with Personal Records Policy and associated procedures.<br><br>Be familiar with legislative requirements and ethical standards regarding the collection, storage, use and security of personal information.<br><br>Monitor systems that are in place to adequately collect, store, use and secure personal information.<br><br>[insert position]<br>Review personal files on a regular basis. |
| Staff | Comply with Personal Records Policy and associated procedures in the collection, storage and use of personal information.<br><br>Be familiar with legislative requirements and ethical standards regarding the collection, storage, use and security of personal information. |

## 6. Risk Management

Systems are in place to ensure personal privacy and confidentiality. All personal documentation is stored securely in a manner so that unauthorised access is prevented.

Staff are provided with ongoing support and information to assist them to effectively manage personal files.

Personal files are reviewed **[insert frequency]** to monitor compliance with the Personal Records Policy.

## 7. Policy Implementation

This policy is developed in consultation with all staff and approved by the Board of Directors.

This policy is to be part of all staff orientation processes and all employees are responsible for understanding and adhering to this policy.

This policy should be referenced in relevant policies, procedures and other supporting documents to ensure that it is familiar to all staff and actively used.

This policy will be reviewed in line with the quality improvement program and/or relevant legislative changes.

## 8. Policy Detail

***[if no personal files are kept]*** **[insert organisation name]** does not keep personal files, but keeps some personal information about individuals. This information includes:

- **[eg name]**
- **[eg attendance]**
- **[eg payment]**

Personal information is kept secure by …..

All information related to an individual is placed in the personal file.

**[insert organisation name]** ensures staff effectively establish, develop, maintain, review, retain, secure and dispose of personal files.

### 8.1 Establishment of Personal Files

Confidential files are held for all individuals accepted into the service/program.

A personal file is established following completion of service entry processes and acceptance into the **[insert organisation name]** program. In establishing a personal file, the allocated staff member is to clearly explain to the individual:

- Information which will be held by **[insert organisation name]**
- How information will be kept secure
- Under what circumstances information may be disclosed to others
- The process for making a complaint in relation to suspected misuse of personal information.
- How to request access to personal information held by the organisation, see Access to File Procedure.

For more information, see Rights and Responsibilities and How to Make a Complaint.

### 8.2 Personal File Structure

**[Personal files will vary across organisations depending on the "personal file continuum"; from no personal file to a highly structured file required by the organisation]**

**[The following applies to a highly structured file required by the organisation]**

Personal files will be clearly identified with a name and/or individual code and will include the following information **[insert information required by the organisation]**:

***[eg Service Entry information***
***Carer, Guardian, Advocate information***
***Assessment – identifying values and strengths***
***Rights, responsibilities and legal information including consent forms***
***Medical information (including medication list and allergies)***
***Recovery plan***
***Interdisciplinary contacts***
***Recovery coordination and contact notes***
***Recovery coordination meeting minutes and notes***
***Correspondence and copies of personal documents / cards***
***Individual feedback***
***Service exit information].***

### 8.3 Development and Maintenance of Personal files

The individual's recovery coach ensures that all sections of the personal file are complete and up-to-date.

All pages of the recovery plan and progress notes contain:

- The individual's name or individual code
- Date of entry
- Page number.

Entries in personal files are:

- Brief, timely, accurate and complete
- Factual, objective and sequential
- Do not contain value judgements or abbreviations
- Legible and signed, dated, with name of author printed
- Written in black or dark blue ink
- To have any mistakes crossed out and initialled, with no liquid paper/white out used.

Progress Notes will be written according to the Progress Notes Guidelines

### 8.4 Review of Personal files

The **[insert relevant position/s]** will review at least **[insert the number of files]** files **[insert frequency]** to ensure all sections of the file are complete and current, and that entries in files are appropriate. The file review will be based on a random

selection of current files and will be completed using the Personal File Review Tool. Results of the review will be analysed and used to raise issues of concern and to improve record keeping quality.

Refer to the Personal File Review Procedure for more details.

### 8.5 Retention of Personal files

Personal files are retained at **[insert organisation name]** due to the possibility that:

- The individual may return to the service
- Litigation or other legal proceedings
- There will be a need for **[insert organisation name]** to provide evidence that it fulfilled its duty of care obligations (for example, if a person became a danger to themselves or others).

Personal files will be securely stored for a period of 7 years after the person has ceased receiving services from **[insert organisation name]**.

### 8.6 Disposal of Personal files

As indicated in the Handbook to Health Privacy (2007), health information files will be destroyed 7 years after the person ceases to receive **[insert organisation name]** services.

Personal files will be disposed in a manner which ensures that they cannot be retrieved and protects the privacy of individuals and others.

### 8.7 Personal Access to Files

Individuals have the right to access their own information on request except under specific circumstances provided for in the Health Records and Information Privacy Act 2002 (NSW). The individual, or their authorised representative, can make a request to access their **[insert organisation name]** personal file in writing or by discussing and documenting (documentation is to be completed by the allocated **[insert organisation name]** staff member).

For more information, refer to the Privacy and Confidentiality Policy and Personal File Access Procedure.

### 8.8 Amendment to Personal files

individuals, or their authorised representatives, will make a request to amend their **[insert organisation name]** personal file in writing or discussed and documented

(documentation is to be completed by the allocated **[insert organisation name]** staff member).

If an individual, or their authorised representative, requests an amendment to the information held in their personal file, you may amend (by way of corrections, deletions or additions) the information to ensure:

- the information is accurate
- the information is relevant, up to date, complete and not misleading, taking into account the purpose for which the information is collected and used.

If a **[insert organisation name]** staff member is unsure whether to grant a request to amend information in a personal file (e.g. if the individual is questioning medical records or a diagnosis), the request should be forwarded to the CEO/Manager. **[Insert organisation name]** may refuse a request to amend information contained in a personal file if it is satisfied that the purpose of the amendment does not meet the criteria specified above. If **[insert organisation name]** decides to refuse to amend the personal file, a written reason for the refusal (with the reason relating to the exemptions above) must be given.

If the requested amendments are refused, the individual may make a statement about the requested changes which is to be attached this to the personal file.

**[Insert organisation name]** is required to respond to a request to amend information in writing within 45 days of receiving the request.

### 8.9 Security of Personal files

All personal documentation is to be kept securely with consideration given to physical, technical and administrative security safeguards. For more information, refer to the Privacy and Confidentiality Policy.

### 8.10 Disclosing Information from Personal files

Personal information should only be disclosed outside of an organisation for the primary purpose for which the information was collected. Information may be disclosed for secondary purposes if:

- **[Insert organisation name]** has the individual's consent
- 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)
- Information is provided to another person or organisation involved in the ongoing care of the patient, or the ongoing service to the individual

- Investigating and managing adverse incidents or complaints about care or patient safety
- Using information for quality improvement activities such as personal file reviews
- Managing a legal claim made by the individual

If a request is made for **[insert organisation name]** to disclose personal 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. Any requests to disclose information to an external organisation should be directed to the CEO/Manager.

## 9. References + Resources

*This policy is adapted from the NADA Client File Management Policy.*
http://www.nada.org.au/index.php?option=com_content&task=view&id=236&Itemid=44

### 9.1 Internal

Personal Records Continuum
Privacy and Confidentiality Policy
Feedback and Complaints Policy
Individual Supports Policy
Service Entry Policy
Service Exit & Re-Entry Policy
Personal File Access Procedure
Personal File Review Procedure
Personal File Review Tool
Rights and Responsibilities
How to Make a Complaint

### 9.2 External

Privacy Act 1988 (Commonwealth)
Health Records and Information Privacy Act 2002 (NSW)
Handbook to Health Privacy (2007)
Public Health Act 1991 (NSW)

### 9.3 Quality and Accreditation Standards

**EQuIP4**

Provided by the Australian Council on Healthcare Standards (ACHS)

Standard 1.1: Consumers/patients are provided with high quality care throughout the care delivery process.

Criterion 1.1.3: Consumers/patients are informed of the consent process, understand and provide consent for their health care.

Criterion 1.1.8: The health record ensures comprehensive and accurate information is recorded and used in care delivery.

Standard 2.3: Information management systems enable the organisation's goals to be met.

Criterion 2.3.1: Records management systems support the collection of information and meet the organisation's needs.

Criterion 2.3.3: Data and information are used effectively to support and improve care and services.

**EQuIP5**

Provided by the Australian Council on Healthcare Standards (ACHS)

Standard 1.1: Consumers/patients are provided with high quality care throughout the care delivery process.

Criterion 1.1.3: Consumers/patients are informed of the consent process, and they understand and provide consent for their health care.

Criterion 1.1.8: The health record ensures comprehensive and accurate information is collaboratively gathered, recorded and used in care delivery.

Standard 2.3: Information management systems enable the organisation's goals to be met.

Criterion 2.3.1: Health records management systems support the collection of information and meet the consumer / patient and organisation's needs.

Criterion 2.3.3: Data and information are collected, stored and used for strategic, operational and service improvement purposes.

**Health and Community Service Standards (6th edition)**

Provided by the Quality Improvement Council (QIC)

Standard 1.6: Knowledge (including research and the collection, storage and sharing of information) is managed in a systematic, ethical and secure way, and the organisation uses it to inform service review and development.

Evidence Question: What is the evidence that:

c) information is stored in an organised way that is easily accessible to approved staff and consumers and, when necessary, is secure and legally compliant?

d) protocols on the sharing of information about consumers exist and are used?

g) the organisation maintains a comprehensive, confidential, secure and accurate record system for each consumer?

Standard 1.8: The organisation ensures compliance with all relevant laws and regulations.

Evidence Questions: What is the evidence that the organisation:

a) is aware of the legislative framework that applies to its operations?

b) maintains internal processes to monitor compliance regularly?

c) has and uses protocols to remedy the situation whenever non-compliance occurs?

Standard 2.1: Assessment and planning are undertaken at individual and community levels to ensure services and programs are responsive to identified needs.

Evidence Questions: What is the evidence that:

e) assessments and plans are documented?

### 9.4 National Mental Health Standards

Criterion 1.13: The organisation upholds the right of consumers to have access to their own health records in accordance with relevant Commonwealth, state / territory legislation.

Criterion 6.14: The right of consumers to have access to their own health records is recognised in accordance with relevant Commonwealth and state / territory legislation / guidelines.

Criterion 6.15: Information about consumers can be accessed by authorised persons only.

Criterion 7.1: The organisation has clear policies and service delivery protocols to enable staff to effectively identify carers as soon as possible in all episodes of care, and this is recorded and prominently displayed within the consumer's health record.

Criterion 7.8: The organisation ensures information regarding identified carers is accurately recorded in the consumer's health record and reviewed on a regular basis.

Criterion 7.10: The organisation actively seeks information from carers in relation to the consumer's condition during assessment, treatment and ongoing care and records that information in the consumer's health record.

### 9.5 Recovery Oriented Service Self-Assessment Tool (ROSSAT)

Evidence items are:

Item 1.2: Policy and procedures are in place and provide understanding and responses to diversity, privacy, confidentiality and information/record sharing, professional boundaries and expectations, identify and address non-recovery oriented attitudes or behaviours, that safeguard all people against abuse and discrimination, and outline processes for reporting abuse of workers and/or consumers and are accessible and applied in practice.

Item 1.10: The organisation maintains an information system that facilitates the appropriate collection, use, storage, transmission and analysis of data to enable review of services and outcomes at an individual and service level. This is done in accordance with information management and related Commonwealth, State / Territory legislation and Acts.

Item 4.2a: Policies and procedures are in place that relate to privacy and confidentiality, the obtaining of consumer consent to share their information and communication techniques available.

### 9.6 NSW Disability Services Standards (DSS)

2.3: The service provider, in consultation with each service user, identifies and documents the individual, ongoing and changing needs of the person with a disability and the approaches for meeting those needs.

4.9: Each service user has the right to see any information the service provider keeps in respect of him/her.