[insert organisation name/logo]

Privacy and Confidentiality 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*].

Privacy and Confidentiality Policy

1. Purpose and Scope

[insert organisation name] is committed to protecting people's privacy and confidentiality in the way information is collected, stored and used.

This policy provides guidance on **[insert organisation name]**'s legal obligations and ethical expectations in relation to privacy and confidentiality.

[Insert organisation name] holds two types of information which are covered by this policy, personal and organisational information.

2. Definitions

Privacy provisions of the Privacy Act 1988 govern the collection, protection and disclosure of personal information provided to **[insert organisation name]**.

Confidentiality applies to the relationship of confidence. Confidentiality ensures that information is accessible only to those legally entitled to have access, and is protected throughout its lifecycle. Confidential information may be marked as such or deemed confidential by its nature, e.g. it is information that is not available in the public domain.

Consent means voluntary agreement to some act, practice or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement.

Individual refers to the person receiving services from **[insert organisation name].**

Person means any person

Organisational information includes publicly available, and some confidential, information about organisations. Organisational information is not covered in the Privacy Act (1988) but some organisational information may be deemed confidential.

Personal information means information or an opinion (including information or an opinion forming part of a database) about a person (Office of the Federal Privacy Commissioner, 2001). It may include information such as names, addresses, bank account details and health information. The use of personal information is guided by the Privacy Act 1988 (Cth); this Act includes Information Privacy Principles that apply to the Federal Government and National Privacy Principles that apply to the private sector.

Health information, which includes medical and hospital records, is considered 'sensitive information' and requires extra protection under privacy law. The Health Records and Information Privacy Act 2002 (NSW) applies to health information in both the private and public health care sector in NSW; legal obligations from this Act are contained in the NSW Health Privacy Principles, which describe what organisations must do when they collect, hold, use, and disclose health information.

The public domain in relation to confidentiality is “common knowledge,” i.e. information that can be accessed by the general public.

3. Principles

[Insert organisation name] is committed to ensuring that information is used in an ethical and responsible manner.

[insert organisation name] recognises the need to be consistent, cautious and thorough in the way that information about people is recorded, stored and managed.

All people have legislated rights to privacy of personal information. In circumstances where the right to privacy may be overridden by other considerations (for example, child protection concerns), staff act in accordance with the relevant policy and/or legal framework.

There have always been exceptions to this principle, in particular when a party to a legal case in court asks through the court process ('issues a subpoena') for medical records that are relevant to the court case.

A failure to keep health records confidential may be a breach of confidentiality. It may also be a breach of specific privacy laws.

All staff, Board members, students and volunteers are to have an appropriate level of understanding about how to meet the organisation’s legal and ethical obligations to ensure privacy and confidentiality.

4. Outcomes

[insert organisation name] provides quality services in which information is collected, stored, used and disclosed in an appropriate manner complying with both legislative requirements and ethical obligations.

All staff and Board Directors understand their privacy and confidentiality responsibilities in relation to personal information and organisational information

about **[insert organisation name]**. This understanding is demonstrated in all work practices.

5. Functions and Delegations

Position	Delegation/Task
Board of Directors	Endorse Privacy and Confidentiality Policy. Be familiar with the organisation's legislative requirements regarding privacy and the collection, storage and use of personal information. Understand the organisation's ethical standards with regards to the treatment of other confidential information relating to **[insert organisation name],** individuals, staff and stakeholders. Comply with Privacy and Confidentiality Policy and associated procedures.
Management	Be familiar with the legislative requirements regarding privacy and the collection, storage and use of personal information. Understand the organisation's ethical standards with regards to the treatment of other confidential information relating to **[insert organisation name],** individuals, staff and stakeholders. Ensure systems are in place across the organisation to adequately protect the privacy of personal information and confidentiality of other sensitive information. Act in accordance with organisational systems in place to protect privacy and confidentiality. Comply with Privacy and Confidentiality Policy and associated procedures.
Staff	Be familiar with the legislative requirements regarding privacy and the collection, storage and use of personal information Understand the organisation's ethical standards with regards to the treatment of other confidential information relating to **[insert organisation name],** individuals, staff and stakeholders. Act in accordance with organisational systems in place to protect privacy and confidentiality. Comply with Privacy and Confidentiality Policy and associated procedures.

6. Risk Management

[insert organisation name] ensures mechanisms are in place to demonstrate that decisions and actions relating to privacy and confidentiality comply with federal and state laws.

All staff, volunteers, students and Board members are made aware of this policy during orientation.

All staff are provided with ongoing support and information to assist them to establish and maintain privacy and confidentiality.

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 **[insert organisation name]**'s quality improvement program and/or relevant legislative changes.

8. Policy Detail

The privacy of personal information is defined by legislation (Privacy Act 1988). At all times, **[insert organisation name]** acts in accordance with these legal requirements which are underpinned by the policy statements 8.1- 8.6 outlined below**. [Insert organisation name]** also strives to respect the confidentiality of other sensitive information. However, in the spirit of partnership, we share information with people and organisations (subject to informed consent), where it would be in the best interest of the individual to do so.

[insert organisation name] upholds the right of individuals and carers to have their privacy and confidentiality recognised and maintained to the extent that it does not impose serious risks to the individual, carer or others.

8.1 Collection of Information

Personal information collected by **[insert organisation name]** is only for purposes which are directly related to the functions or activities of the organisation. These purposes include:

- Enquiry about programs

- Referral to programs
- Providing treatment, care and support to consumers
- Administrative activities, including human resources management
- Sector development activities
- Community development activities
- Fundraising
- Complaints handling.

For more detailed information about these purposes and the information handling practices that apply to them, refer to the Personal Records Policy, Human Resources Policy, Feedback and Complaints Policy and Information Management Policy.

[Insert organisation name] provides information to consumers on collecting health and personal information including:

- Purpose of collecting information
- How information will be used
- Who (if anyone) information may be transferred to and under what circumstances information will be transferred. For example, risk assessment information may be disclosed to another organisation when a consumer transitions from one service to another, or disclosed to a carer when a consumer exits from a CMO to a more independent home-based environment.
- Limits to privacy of personal information
- How a consumer can access or amend their health information
- How a consumer can make a complaint about the use of their personal information.

See also Rights and Responsibilities and How to Make a Complaint.

8.2 Use and Disclosure

[Insert organisation name] provides carers with information about the consumer's recovery journey.

[Insert organisation name] only uses personal information for the purposes for which it was given, or for purposes which are directly related to one of the functions or activities of the organisation. It may be provided to government agencies, other organisations or consumers if:

- informed consent has been provided by the consumer or substitute decision maker
- It is required or authorised by law
- It will prevent or lessen a serious and imminent threat to somebody's life or health

[For CMOs which provide clinical services:** **[Insert organisation name]'s clinical guidelines and practice are in accordance with Commonwealth, state / territory privacy legislation and current guidelines that address the issue of sharing confidential information with carers].

Further information regarding the use and disclosure of personal information can be found in the Personal Records Policy.

8.3 Carers

Carers and especially primary carers nominated under the Mental Health Act have the right to be advised of sufficient information about the person's support needs to allow them to carry out their caring and/or support role.

If the consumer does not consent to information being disclosed to a carer who is normally and appropriately involved in the consumer's support the organisation will consider:

- the consumer's capacity to grant or withhold consent (especially if subject to involuntary treatment);
- the importance of the carer's role in supporting the consumer's care and treatment;
- whether failure to disclose information will expose the consumer or others to serious risks; and,
- the minimum information which may need to be disclosed to the carer(s) to support the consumer's recovery journey, if the carer is to continue to play a significant role in their support.

Any such disclosures will themselves be made in with the stipulation that confidentiality will be respected by those to whom the information is divulged.

8.4 Data Quality

[Insert organisation name] takes steps to ensure that the personal information collected is accurate, up-to-date and complete. These steps include maintaining and updating personal information when we are advised by consumers that it has changed (and at other times as necessary), and checking that information provided about a consumer by another person is correct.

8.5 Data Security

[Insert organisation name] takes steps to protect the personal information held against loss, unauthorised access, use, modification or disclosure and against other misuse. These steps include reasonable physical, technical and administrative security safeguards for electronic and hard copy of paper records as identified below.

Reasonable physical safeguards include:

- Locking filing cabinets and unattended storage areas
- Physically securing the areas in which the personal information is stored
- Not storing 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)
- Establishing, using and regularly monitoring an electronic audit trail, which records details of attempts to create, access, print, copy, alter and/or delete electronic documents.
- 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.

8.6 Access and Correction

Information about consumers can be accessed by authorised persons only.

[Insert organisation name] upholds the right of carers to access information about the person being supported with that consumer's informed consent or otherwise in accordance with principles relating to capacity and consent and the Mental Health Act 2007.

Consumers may request access to personal information held about them. Access will be provided unless there is a sound reason under the Privacy Act or other relevant law. Other situations in which access to information may be withheld include:

- There is a threat to the life or health of a consumer
- Access to information creates and unreasonable impact on the privacy of others
- The request is clearly frivolous or vexatious There are existing or anticipated legal dispute resolution proceedings
- Denial of access is required by legislation or law enforcement agencies.

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

Amendments may be made to personal information to ensure it is accurate, relevant, up-to-date, complete and not misleading, taking into account the purpose for which the information is collected and used. If the request to amend information does not meet these criteria, **[insert organisation name]** may refuse the request.

If the requested changes to personal information is not made, the consumer may make a statement about the requested changes which will be attached this to the record.

[Insert relevant staff position] is responsible for responding to queries and requests for access/amendment to personal information. See Personal records Policy.

8.7 Anonymity and Identifiers

Wherever it is lawful and practicable, consumers will have the option of not identifying themselves or requesting that **[insert organisation name]** does not store any of their personal information.

As required by the Privacy Act 1988, **[insert organisation name]** will not adopt a government assigned individual identifier number e.g. Medicare number as if it were its own identifier/ code.

8.8 Collection use and disclosure of confidential information

Other information held by **[insert organisation name]** may be regarded as confidential, pertaining either to a consumer or an organisation. The most important factor to consider when determining whether information is confidential is whether the information can be accessed by the general public.

Staff members are to refer to the CEO/Manager before transferring or providing information to an external source if they are unsure if the information is sensitive or confidential to any person.

Organisational Information
All staff, Board members, students and volunteers agree to adhere to the **[insert organisation name]** Code of Conduct when commencing employment, involvement or a placement. The Code of Conduct outlines the responsibilities to the organisation related to the use of information obtained through their employment/ involvement/ placement.

The Code of Conduct states that individuals will:

"Use information obtained through their involvement, employment or placement only for the purposes of carrying out their duties, and not for financial or other benefit, or to take advantage of another person or organisation."

Staff Information
The Human Resources Policy details how the organisation handles staff records to manage privacy and confidentiality responsibilities, including the storage of and access to staff personnel files and the storage of unsuccessful position applicants' information.

Stakeholder Information
[Insert organisation name] works with a variety of stakeholders including private consultants. The organisation may collect confidential or sensitive information about its stakeholders as part of a working relationship. Staff at **[insert organisation name]** will not disclose information about its stakeholders that is not already in the public domain without stakeholder consent.

The manner in which staff members manage stakeholder information will be clearly articulated in any contractual agreements that the organisation enters into with a third party.

Personal information
Detailed information regarding the collection, use and disclosure of personal information can be found in the Personal File Management Policy and associated procedures.

8.9 Breach of Privacy or Confidentiality

If staff are dissatisfied with the conduct of a colleague with regards to privacy and confidentiality of information, the matter should be raised with the staff member's direct supervisor. If this is not possible or appropriate, follow delegations indicated in the Feedback and Complaints Policy. Staff members who are deemed to have breached privacy and confidentiality standards set out in this policy may be subject to disciplinary action.

If any person is dissatisfied with the conduct of a **[insert organisation name]** staff or Board member, a complaint should be raised as per the Feedback and Complaints Policy. Information on making a complaint will be made available to any person associated with **[insert organisation name]** and will be found on the **[insert organisation name]** website. Additionally, a complaint can be taken over the phone by any staff member.

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

9. References

9.1 Internal

Personal Records Policy
Code of Conduct
Information Management Policy
Informed Decision Making Policy
Human Resources Policy
Feedback and Complaints Policy
Rights and Responsibilities
How to Make a Complaint

9.2 External

Legislation[1]

Privacy NSW (2009). Privacy Laws in NSW.
http://www.ipc.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_nswprivacy_laws accessed 31st May, 2011.

Privacy Act 1988 (Cth)

- sets privacy standards for dealing with personal information
- applies to Australian Government (Commonwealth) and ACT government agencies
- applies to private sector organisations across Australia
- is administered by the Office of the Federal Privacy Commissioner

Privacy and Personal Information Protection Act 1998 (NSW)

- sets privacy standards for dealing with personal information
- applies to NSW state and local government agencies
- is administered by Privacy NSW

Health Records and Information Privacy Act 2002 (NSW)

- sets privacy standards for dealing with health information
- applies to NSW state and local government agencies
- applies to private sector persons and organisations in NSW
- is administered by Privacy NSW.

[1] From Privacy NSW (2009)

Mental Health Act (NSW) 2007

- sets out rights of consumer to nominate a primary carer
- sets out right of primary carer to be otherwise nominated if consumer lacks capacity
- sets out rights of carers role to be respected (section 68(j))
- Sets out rights of primary carers to information and consultation in regard to treatment and support and in particular discharge planning (sections 71 to 73 and 75 to 79)

Resources

Office of the Federal Privacy Commissioner (2001). *Guidelines to the National Privacy Principles*. Office of the Federal Privacy Commissioner, Sydney.

Office of the Privacy Commissioner (2006). *Privacy Policy*, Office of the Privacy Commissioner, Sydney.

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.

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

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.

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

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 Questions: What is the evidence that:

b) cooperative work practices exist to share knowledge within the organisation?

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?

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?

9.4 National Mental Health Standards

Criterion 1.8: The organisation upholds the right of the consumer to have their privacy and confidentiality recognised and maintained to the extent that it does not impose serious risk to the consumer or others.

Criterion 1.12: The organisation upholds the right of carers to be involved in the management of the consumer's care with the consumer's informed consent.

Criterion 1.14: The organisation enacts policy and procedures to ensure that personal and health related information is handled in accordance with Commonwealth, state / territory privacy legislation when personal information is communicated to health professionals outside the organisation, carers or other relevant agencies.

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

Criterion 7.7: The organisation has documented policies and procedures for clinical practice in accordance with Commonwealth, state / territory privacy legislation and guidelines that address the issue of sharing confidential information with carers.

Criterion 7.9: The organisation provides carers with non-personal information about the consumer's mental health condition, treatment, ongoing care and if applicable, rehabilitation.

Criterion 10.4.3: The organisation, with the consumer's informed consent includes carers, other service providers and others nominated by the consumer in assessment.

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 1.11: Any research being conducted by the organisation enables consumers to either, design and conduct the research, collaborate as partners and/or be consulted as participants. Ethical issues are considered and addressed and prior to consumers participating in any research, informed consent is obtained.

Item 2.3: Supervision, both formal and informal, is available and used to discuss:

- Relationship development and maintenance
- Respectful recovery oriented practice

- Providing holistic support that is responsive to diversity
- Supporting self-directed care by providing information and choice, fostering engagement and maximising personal responsibility
- Incorporating and maintaining a belief in recovery in service provision
- Obtaining relevant and up to date information, share information in appropriate formats, and educate people on how to access information
- Enhancing a person's participation and social inclusion.

Item 2.5: Leaders advocate, champion and model:

- Human rights informing service delivery
- The consumers' voice as central to care and service provision
- The belief that recovery is possible and probable for every person
- Hopeful and optimistic attitudes in dealing with workers, consumers and carers.

Item 2.6: Management:

- Is aware of Commonwealth and State policy directions around recovery orientation and integrates these into practice
- Identifies information relevant to the organisation to increase the knowledge base on recovery and recovery oriented practice, including information for consumers, carers and their families.

Item 3.3: Relationships are formed:

a. Allowing enough time at the beginning of the relationships to get to know each other and develop trust (rapport)
b. Maintaining privacy, confidentiality and transparency
c. Focusing on a person's strengths rather than deficits
d. Focussing on seeing the person first and their illness second
e. Seeking to find out what each consumer's view is regarding purpose and living a meaningful life
f. By understanding a person's previous experiences (what was and wasn't helpful in past treatment and care) and considering these in current recovery plans.

Item 3.20: Workers seek to exchange information with other organisations and agencies to ensure continuity of care (with consent).

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.

Item 4.3e: The organisation provides the opportunity for ongoing training on the obtaining and sharing of knowledge and information including:

- Protocols relating to privacy and confidentiality
- Relevant legislation changes
- Innovative recovery based practice
- New and existing relevant services
- Sharing accessible information and resources relevant to consumers, their families and carers.

Item 5.3: Consumers are provided with the regular opportunity to evaluate relationships, respectful practice, perceptions of stigma and discrimination experienced from workers within the organisation, the consumer self-directed focus, the belief in consumer's recovery, the obtaining and sharing of knowledge and information, the quality and relevance of information provided and participation and social inclusion.

Item 5.3e: Consumers are provided with the regular opportunity to evaluate the obtaining and sharing of knowledge and information, the quality and relevance of information provided, the appropriateness of the format information is provided in and the ability to understand information that is provided.

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.

4.1a: The service provider has developed written policies and procedures for protecting service user's privacy, dignity and confidentiality.

4.1b: The service provider has developed, in consultation with service users, written policies and procedures for protecting service users' privacy, dignity and confidentiality .

4.3: The service provider only collects service user information that is directly relevant to effective service delivery.

4.4: Each service user is informed of the types of personal information that the service provider holds and the reasons for holding this information.

4.5: Each service user's consent is obtained before any information about him/her is sought or released by the service provider

4.6: Each service user's right to dignity and privacy is recognised, respected and protected in relation to personal activities

7.4: Complaints or disputes are handled in a manner consistent with the service provider's policies on privacy.