PRIVACY POLICY AND PROCEDURE

1. Purpose

This *Privacy Policy and Procedure* ensures that consent is obtained to collect, use and share a client's personal information as is a client's legal right and the legal responsibility of EPIS.

2. Who this policy and procedure applies to

This policy and procedure applies to any EPIS worker, that is, an employee, volunteer or student on placement who is required to obtain consent from a client to collect, use and share their personal information.

3. What this policy and procedure covers

This policy and procedure covers the collection, use and sharing of client's personal information and is compliant with the *Privacy Act 1988*, *NDIS Act 2*013 and *Aged Care Act 1997*.

4. Principles

The following principles apply in implementing this policy and procedure and align with those of the *Office of the Australian Information Commissioner, Australian Government*[1].

Principle	Description
Legal	EPIS will ensure the collection, use and sharing of personal information is legal, fair and non-intrusive.
Consent and cultural security	EPIS will only collect, use or share personal information if the individual has consented. Clients will be advised about the collection, use and sharing of personal information in a culturally secure manner to ensure consent is actually obtained.
Use and sharing	EPIS will only use or share personal information for the purpose for which it was collected unless the individual has consented.
Information quality	EPIS will take reasonable steps to make sure that the personal information it collects, uses or shares is accurate, complete and up-to-date.
Security	EPIS will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
Openness	EPIS will make this policy and procedure available to anyone who requests it and make it available on the EPIS website.
Access and correction	EPIS will provide clients access to their personal information on request in a supportive manner in accordance with the *Client Record Management Policy and Procedure.*

5. Policy and Procedure

The following covers EPIS policy and procedural requirements on privacy. The *Collecting and Sharing of Personal Information Consent Form* must be used to discuss and obtain consent with all clients.

EPIS policy statements on privacy are in Appendix A.

[1] Australian Government, Office of the Australian Information Commissioner, July 2019, *Australian Privacy Principles Guidelines, Privacy Act 1988*

5.1 Consent

5.1.1 Personal and sensitive information

Consent must be obtained from clients to collect sensitive information and, where possible, to collect all personal information.

Consent must be obtained to share personal information.

See Section 5.2 and Section 7 for definitions of personal information and sensitive information.

5.1.2 Expressed or implied consent

Expressed consent is given openly and obviously, either verbally or in writing. Expressed consent must be obtained to collect sensitive information and share personal information.

Implied consent is when there is a reasonable belief that a client has given consent and must only be used in extenuating circumstances and be approved by a Support Coordinator.

5.1.3 Requirements for obtaining consent

EPIS workers must consider the following when discussing and obtaining consent using the *Collecting and Sharing of Personal Information Consent Form*.

Consent must be informed

The consequences of giving or not giving consent must be explained to the client clearly, simply, without jargon and in the client's language, should this be required, otherwise it is not valid.

Consent must be voluntary

Clients must not be forced or pressured to give consent and the following must be discussed:

- Options available to them if they choose not to consent.
- Consequences to them if they do not consent.

Consent must be current and specific

Consent is given at a particular time and for specific circumstances and it must not be assumed that it continues indefinitely. When asking for consent:

- There must be an explanation as to the reason for the request.
- The request must be as specific as possible rather than broad, vague or for an undefined future.

Capacity to give consent

Clients must have the capacity to give consent. This means they must be able to:

- Understand what they are being asked to decide to give or not give consent to.
- Understand the consequences of giving or not giving their consent.
- Base their decision on reason.
- Communicate their decision.

Common situations to be alert for when a client may not be able to consent include:

- Children and young people under 18 years of age.
- Clients with a physical, intellectual, cognitive or psychosocial disability, or dementia.
- Clients who are temporarily incapacitated, for example, a temporary psychiatric illness, severe trauma or distress.
- Clients for whom English is not their first language.

In these situations, the Support Coordinator must consider:

- The information being provided in the client's language, preferably using a qualified interpreter.
- A guardian or person with enduring power of attorney providing consent.

As far as practical, the client who lacks capacity is to be involved in the consent decision.

5.2 Type of information collected

The personal information EPIS collects must only be what is reasonably necessary to provide safe, quality services to a client.

EPIS workers may collect the following personal information:

- Name, signature, address, phone number or date of birth of the client.
- Name and contact numbers of relevant family members or carers.
- Name and contact number of the client's medical practitioner and other relevant health care providers.
- Sensitive information.

The type of sensitive information EPIS workers may collect is:

- Health and medication history.
- Social information related to housing, employment and income.
- Cultural background.
- Religious beliefs and practices.

To keep this information current, EPIS workers must review a client's personal information annually.

5.3 Storage of personal information

All personal information must be stored in accordance with the *Client Records Management Policy and Procedure* to ensure security:

- Client paper files must be stored securely in the assigned filing cabinet. Access to these files must be limited to EPIS employees, an auditor or health professionals from another organisation delivering services in an EPIS facility.
- Client electronic files are stored on *Best Practice* with access limited to EPIS employees, an auditor or health professional from another organisation delivering services in an EPIS facility.
- Records for Aboriginal and Torres Strait Islander clients must be kept indefinitely, records of children aged under 18 years, must be kept until seven (7) years after they turn 18 years of age, records for all other clients must be kept for seven (7) years after the client ceases receiving services from EPIS.
    - Archiving of paper and electronic files occurs after when a client leaves the service and these files are stored in a secure filing cabinet.
    - Paper and electronic files are destroyed by shredding paper files and permanent deleting of electronic files to ensure security.

5.4 Sharing of personal information

Consent must be obtained from the client prior to sharing any personal information to another person or organisation except when:

- EPIS has a statutory obligation to disclose certain information about a client, for example, subpoenas, warrants, or coronial inquests.
- EPIS considers the client is at risk to themselves.

- EPIS considers the client is a risk to another person(s).
- The health professional is delivering services to the client in an EPIS facility.

5.5 Access to personal information

Clients have a right to access and make changes to their personal information in accordance with the *Client Records Management Policy and Procedure.*

5.6 Change or withdraw consent

Clients can change or withdraw their consent at any time with regard to their personal information. Should a client want to do this a new *Collecting and Sharing of Personal Information Consent Form* must be completed.

5. Use of client's information for EPIS publications

Should EPIS wish use to use a client's personal information, including photos of a client, for any publications, eg; annual report, website, expressed consent must be obtained and documented accordingly and separately to the *Collecting and Sharing of Personal Information Consent Form.*

6. Responsibilities

6.1 All EPIS workers

All EPIS workers must**:**

- Obtain expressed consent to collect sensitive information and share any personal information using the *Collecting and Sharing of Personal Information Consent Form* as per Section 5.

6.2 Support Coordinators

In addition to 6.1, Support Coordinators must:

- Endorse implied consent being obtained as per Section 5.1.2.
- Manage situations when a client does not have the capacity to consent as per Section 5.1.3.

6.3 Executive Team

In addition to 6.1, the Executive Team must:

- Provide for the safe and secure storage of personal information, including archiving.
- Provide for the safe destruction of personal information.

7. Definitions

Personal information: is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Sensitive information: is a subset of personal information and incudes information or opinion about an individual's health, racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record and could be used to discriminate against that person.

8. Appendix 1: Policy statements

9. Related documents

Internal	
EPIS policies and procedures	*Client Records Management Policy and Procedure*
EPIS frameworks	
EPIS tools, checklists, forms	*Collecting and Sharing of Personal Information Consent Form*
External	
Policy	
Legislation	*Aged Care Act 1997* *NDIS Act 2013* *Privacy Act 1988*
Aged Care Standards	***Standard 1 – Consumer dignity and choice (key standard)*** *Standard 8 – Organisational governance*
NDIS Practice Standards	***Core Module 2 – Provider Governance and Operational Management (key module)*** *Core Module 1- Rights and Responsibilities*
Other	*Australian Government, Office of the Australian Information Commissioner, July 2019, Australian Privacy Principles Guidelines, Privacy Act 1988*

Version Control

Policy name	Privacy Policy and Procedure		
Policy endorser	CEO	**Date:**	14/01/2022
Policy owner	Operations Manager	**Version:**	1
Policy review date	14/01/2023		
Electronic file path	Projex – Policies and Procedures		

8: Appendix 1: Policy Statements

Policy Statement 1

Expressed consent must be obtained to collect sensitive information and share personal information except:

- In extenuating circumstances when implied consent can be obtained with a manager's endorsement.
- When the information is required by a statutory authority and is a legal requirement.
- When a client is deemed at risk to themselves.
- When a client is deemed at risk to another person(s).

Policy Statement 2

The obtaining of consent must be informed, voluntary, current and specific and cover the reasons why the collecting or sharing of personal information would be beneficial to a client and the consequences of not doing so. The *Collecting and Sharing of Personal Information Consent Form* must be used as the tool to do this.

Policy Statement 3

A client must have the capacity to give consent. When they do not, an alternative arrangement must be made and endorsed by a manager. This includes making alternative arrangements such as an interpreter when English is not a first language, or using a guardian or person with enduring power of attorney.

Policy Statement 4

Clients have the right to access and make changes to their personal information and change or withdraw their consent with regard to their personal information at any time and will be supported to do so.

Policy Statement 5

Personal information must be stored securely including when it is archived and it must be destroyed securely in accordance with the *Client Record Management Policy and Procedure*.

Policy Statement 6

Records for Aboriginal and Torres Strait Islander clients must be kept indefinitely, records of children aged under 18 years, must be kept until seven (7) years after they turn 18 years of age, records for all other clients must be kept for seven (7) years after the client ceases receiving services from EPIS.

Policy Statement 7

Should EPIS wish use to use a client's personal information, including photos of a client, for any publications, eg; annual report, website, expressed consent must be obtained and documented accordingly.