1.0 Revision History

Revision Date	Revision No.	Change	Responsible Person
29 Oct 2019	1.4	Policy and procedure consolidated	Quality Manager
19 Nov 2020	1.5	Policy reviewed (NDIS standards)	Quality Manager
20 Oct 2023	1.6	Policy reviewed	Quality Manager

2.0 Persons Affected

All employees and contractors engaged by of North and West Remote Health.

3.0 Policy

NWRH is committed to protecting the privacy and confidentiality of clients, staff and stakeholders in the way health information is collected, stored and shared.

NWRH holds two types of information that are covered by this policy: personal information and organisational information.

NWRH recognises the need to be consistent, cautious and thorough in the way that information about clients, staff and stakeholders is collected, stored and shared.

All individuals 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 or legal framework, or both.

All staff are to have an appropriate level of understanding about how to meet the organisation's legal and ethical obligations to ensure privacy and confidentiality.

NWRH is committed to ensuring that information is used in an ethical and responsible manner.

4.0 Definitions

Privacy provisions of the *Privacy Act 1988* govern the collection, storage and sharing of personal information provided to NWRH by clients, staff, and stakeholders.

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

Consent means 'expressed consent or implied consent'. The four key elements of consent are:

- The client is adequately informed before giving their consent;
- The client gives consent voluntarily;
- The consent is current and specific; and
- The client has the capacity to understand and communicate their consent

Expressed Consent is given explicitly, either orally or in writing

Implied Consent refers to a person indicating their agreement through their actions or by cooperating with the health professional's instructions. Implied consent is adequate for minor or routine procedures and is not required to be documented in the clients record.

Health Information is all identifying "personal information collected to provide a health service. In the Australian Privacy Principles (APP's) 'Health information' comes under the definition of 'sensitive information.

Individual means any person such as a client, staff member, stakeholder or a member of the public.

Organisational information includes publicly available, and some confidential, information about organisations. Organisational information is not covered in the *Privacy Act1988,* 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 an individual (Office of the Federal Privacy Commissioner, 2001). It may include information such as names, addresses, bank account details and health conditions and interventions. The use of personal information is guided by the *Federal Privacy Act 1988.*

The **public domain** in relation to confidentiality is "common knowledge"; that is, information that can be accessed by the general public.

Solicited and Unsolicited Personal Information is all personal information received by an APP entity is either solicited or unsolicited personal information. Section 6(1) defines 'solicit' but does not define *'unsolicited'*. Therefore, personal information reviewed by an entity that does not fall within the definition of *'solicited'* is *'unsolicited'* personal information.

5.0 Procedures

All staff and Board Directors are made aware of this policy during orientation and acknowledge this policy by signing form 3004A.

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

The privacy of personal information is defined by legislation (*Privacy Act 1988*). NWRH acts in accordance with these legal requirements at all times as underpinned by the policy outlined below.

NWRH also strives to respect the confidentiality of other sensitive information. However, in the spirit of partnership, we share information with clients and other involved individuals and organisations (subject to consent), where it would be in the best interest of the client, or other individual, to do so.

5.1 Collection of information

Personal information collected by NWRH is only used for purposes that are directly related to the functions or activities of the organisation. These purposes include:

- Enquiry about programs.
- Referral to programs.
- My Health Record system.
- Contractual and Reporting purposes.
- Providing treatment and support to clients.
- For the purpose of actioning a referral including sharing personal information with NWRH and other healthcare providers.
- Administrative activities, including human resources management.

- Sector development activities including external data collection portals e.g. My Aged Care, RHealth etc.
- Community development activities including case study presentations.
- Compliment, Complaint and Feedback handling.
- Quality Improvement and Clinical Governance requirements.

When collecting health and personal information, NWRH provides information to clients regarding:

- The purpose for collecting information.
- How information will be used.
- Assess if an interpreter is required, if so arrange for this service before proceeding to collect information and consent.
- Assess if an interpreter or family member is required for cultural reasons before proceeding to collect information from Aboriginal and Torres Strait Islander clients.
- To whom (if anyone) information may be transferred and under what circumstances information will be transferred.
- Limits to privacy of personal information.
- How a client can access or amend their health information.
- How a client can make a complaint about the use of their personal information.
- Assess if a client requires a carer/support person or other authorised representative be present during the collection of health and personal information.

5.2 Use and disclosure

NWRH only uses personal information for the purposes for which permission was given, or for purposes that are directly related to one of the functions or activities of the organisation. Personal information may be provided to government agencies, other organisations or individuals if:

- The client has consented. This consent may be evidenced by a signature or obtained verbally and documented.

(For example a General Practitioner may in the process of providing a referral for a client to receive services tick a box to indicate that the client understands or confirm with an family member directly related for cultural reasons that the client consents to the referral being sent.)

- It is required or authorised by law
- It will prevent or lessen a serious and imminent threat to somebody's life or health

All clients/and or carers must understand the organisation's purpose of use and disclosure of personal information and must acknowledge their understanding through reading and signing, or verbally approving, Form 4023A Client Consent form. This must be uploaded and documented on the client's file.

Further information regarding the use and disclosure of client information can be found in the “Request for Release of Client Information Policy and Procedure”.

5.3 My Health Records System

The ‘My Health Record System’ is reflected in NWRH’s Consent form. Under the ‘My Health Record System’, clients:

- have the ability to set a number of privacy controls on their digital health record;

- can set a code that restricts access to providers for certain documents contained within their record, they can also set a different code that restricts access to providers to their entire record; and
- can ask to remove or amend a clinical document, and if the medical practitioner agrees, the [Insert Name of Organisation] shall take steps to amend or remove the document as soon as possible.

5.4 Data quality

NWRH takes steps to ensure that the personal information it collects is accurate, up-to-date and complete. These steps include maintaining and updating personal information when we are advised by individuals that their information has changed (and at other times as necessary), and checking that information provided about an individual by another person is correct.

5.5 Data security

NWRH takes steps to protect the personal information it holds 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 or 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 so that they cannot be seen or accessed by unauthorised people or members of the public

Reasonable **technical** safeguards include:

- Two step Authentication process and additional passwords to access NWRH electronic medical records.
- Establishing different access levels so that not all staff can view all information
- Ensuring information is transferred securely where possible or where not possible ensuring that appropriate safeguard measures have been taken
- 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 are competent in this area.

5.6 Access and correction

Individuals may request access to their own personal information. Access will be provided unless there is a sound reason under the *Privacy Act1988* or other relevant law to withhold access. Other situations in which access to information may be withheld include:

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

NWRH 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, NWRH may refuse the request.

If the requested changes to personal information are not made, the individual may make a statement about the requested changes and the statement will be attached to the record.

NWRH is responsible for responding to queries and requests for access and amendment to personal information. NWRH requires payment of fees for access to client information. Request's will be notified of the fees for accessing medical records by invoice when requests are processed. Refer to Request for Release of Client Information Policy and Procedure (4021) for further information.

5.7 Anonymity and identifiers

Wherever it is lawful and practicable, individuals will have the option of not identifying themselves or requesting that NWRH does not store any of their personal information. Where delivery of health services by NWRH or its subcontractors is required then it would not be practicable to provide anonymity. As required by the *Privacy Act 1988*, NWRH will not adopt a government-assigned individual identifier number, such as a Medicare number, as if it were its own identifier or client code.

5.8 Collection use and disclosure of confidential information

Other information held by NWRH may be regarded as confidential, pertaining either to an individual 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.

If they are unsure whether information is sensitive or confidential to NWRH or its clients, staff and stakeholders, staff members are to refer to the CEO and/or relevant Executive Manager before transferring or providing information to an external source.

Organisational information

All staff agree to adhere to the NWRH*'s* Code of Conduct when commencing employment. The Code of Conduct outlines the responsibilities to the organisation related to the use of information obtained through their employment.

Staff information

The Employee 'Personnel File Storage Policy (3047)' 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

NWRH 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 NWRH 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.

Detailed information regarding the collection, storage and sharing of client information can be found in 4024 Clinical Records Management Policy and Procedure.

5.9 When Information can be Disclosed Without your Consent

We will only disclose your health information to a third party with your consent, unless:

- The disclosure is directly related to the primary purpose for collection;
- In an emergency situation, where release of information is necessary to aid medical treatment; or
- We are required by law to disclose the information (e.g. reporting of communicable diseases, suspected child abuse and/or neglect – refer 2008 Incident Reporting).

5.10 Breach of privacy or confidentiality

If staff are dissatisfied with the conduct of a colleague regarding privacy and confidentiality of information, the matter should be raised with the staff member's direct Line Manger. If this is not possible or appropriate, follow the delegations indicated in the 'Grievance Policy (3022)'. Staff members who are deemed to have breached privacy and confidentiality standards set out in this policy may be subject to disciplinary action.

If a client or stakeholder is dissatisfied with the conduct of a NWRH staff or Board Director, a complaint should be raised in accordance with the 'Compliments, Complaints and Feedback Policy and Procedure (4011)'. Information about making a complaint will be made available to clients, stakeholders and can be found on the NWRH Website. Additionally, a complaint can be taken over the phone or in person by any staff member.

5.11 Notifiable Data Breaches

A Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

Examples of a data breach include when:

- A device containing customers' personal information is lost or stolen
- A database containing personal information is hacked
- Personal information is mistakenly provided to the wrong person.

All suspected and/or confirmed Data Breaches are required to be reported to the ICT Team immediately. The ICT Manager, in consultation with the Senior Executive, who will report the Breach to The Australian Information Commissioner (Commissioner). By responding quickly, we can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

Refer to 1055 Notifiable Bata Breach Action and Response Plan for further information.

6.0 Expected outcomes

NWRH provides quality services in which information is collected, stored and shared in an appropriate manner that complies with both legislative requirements and ethical obligations.

All staff understand their privacy and confidentiality responsibilities in relation to personal information and organisational information about NWRH, its clients, staff and stakeholders. This understanding is demonstrated in all work practices; refer to Form 3004A Confidentiality Statement.

All clients understand how their personal information is collected, used and disclosed prior to commencing services with NWRH; refer to Form 4023A Client Consent Form.

7.0 References

NWRH Policy, Procedure, Forms

- Procedure 3004 Privacy and Confidentiality Procedure
- Policy 1030 Password and Network Security
- Policty 2008 Incident Reporting
- Policy 3022 Grievance
- Policy 3047 Employee Personnel File Storage
- Policy 4021 Request for Release of Client Information
- Form 4023A Client Consent Form
- Form 4023B Authority to Release Confidential Information
- Policy 4024 Client Records Management
- Form 4011B Client Feedback Form (Pictorial)
- Form 3004A Confidentiality Statement

Relevant Legislation and Guidelines

- *Privacy Act 1988*
- *Aged Care Act 1997*
- *Domestic and Family Protection Act 2012*
- *Family Responsibilities Commission Act 2008*
- *Mental Health Act 2016*
- 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
- AS/NZS ISO 9001:2015 Quality management systems – Requirements; 7.5.4 Customer Property
- AS/NZS ISO 9001:2015 Quality management systems – Requirements; 7.5.3 Control of Documented information
- Domestic and Family Violence Information Sharing Guidelines (May 2017)