1.0 Policy Statement

Northern Australia Primary Health Limited (NAPHL) is committed to ensuring the privacy and confidentiality of personal/private information. This policy outlines how Northern Australia Primary Health Limited (NAPHL) collects and manages personal and sensitive information in accordance with the Australian Privacy Principles (APP).

2.0 Purpose and Background

NAPHL is required to adhere to the *Privacy Act 1988, National Disability Insurance Scheme Act 2013, other relevant legislation* and the APP.
There are 13 APPs to which NAPHL must adhere. The APPs regulate how NAPHL may collect, use, disclose and store personal/privacy information and how individuals may access personnel.
These are:

1. An open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

A privacy policy is required to ensure that NAPHL's collection and handling of private and sensitive information is consistent, and adheres to the APPs at all stages of the information lifecycle. (collection, use, disclosure, storage, destruction and de-identification).

3.0 Scope of Policy

This policy applies to all employees, contractors, volunteers and students.

4.0 Policy Detail

NAPHL collects and uses private and sensitive information necessary to undertake its functions to improve health outcomes.

All business units of NAPHL are required to ensure that their processes for the collection, storage, use, disclosure and disposal of personal or sensitive information adheres to this policy.

Collection of information

In the course of providing services, NAPHL collects personal and sensitive information as required by law, or for NAPHL to conduct its functions and activities. Collection purposes include:

- Providing and facilitating healthcare
- Providing information and networking services to members
- Conducting research
- Human Resources management.

Personal information collected by NAPHL may include:

- Contact details
- Complaint details
- Information regarding language preference and proficiency

- Employment status
- Current and prior education details.

NAPHL will obtain written consent from consumers prior to collection of sensitive information, unless a permitted general situation exists as per the APP. NAPHL will provide notification at the point of collection of both sensitive information and personal information, as to the purpose for collection, and what the information will be used for.

NAPHL only collects personal and sensitive information by lawful and fair means, and only collects personal or sensitive information about a consumer directly from that consumer unless it is unreasonable or impractical to do so.

All information collected by NAPHL will be used for the primary purpose for which it was collected. NAPHL may use or disclose the information for a secondary purpose if subclause 6.2 of the APPs applies:
"6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:
    (i) if the information is sensitive information — directly related to the primary purpose; or
    (ii) if the information is not sensitive information — related to the primary purpose; or
(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or
(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or
(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body."

Collection of information at NAPHL allows for the use of anonymity or pseudonymity where possible. Consumers should note that certain business activities and functions of NAPHL will not allow for anonymity or pseudonymity when information is collected, as this may be unsafe or impractical.

Collection of information from consumers under the age of 18
NAPHL collects information from consumers that are under the age of 18 (referred to as a minor from hereon). Consent to collect sensitive information will be obtained from the minor, or the minor's parents or guardian, depending on the results of a case by case basis review by the collecting officer of whether the consumer is capable of making their own decisions. If the minor is considered to be capable of making their own decisions, the private information of the minor will be treated as that of an adult, and will not be disclosed to third parties (including parents or guardians) unless the minor has consented to this disclosure.

Security and disclosure of information
NAPHL will take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. NAPHL use appropriate technologies and processes such as access control procedures, network firewalls, encryption and physical security to protect privacy.

Personal and sensitive information collected by NAPHL will be held in an appropriately secure manner, depending on the information and method of collection, including:

- Online and offline databases
- Online file servers
- Locked drawers or filing cabinets

Personal and sensitive information is only able to be accessed and used by consumers that require the information to undertake NAPHL activities for which the information was collected. Access to personal and sensitive information is granted to employee on a 'needs to know' basis. Attempts to access personal or sensitive information by an unauthorised employee, or use by an employee of personal or sensitive information for any other purpose than that which it was collected (except in permitted general situations) is forbidden, and may result in disciplinary action.

Cross-border disclosure of personal information
Occasionally NAPHL may hold personal information offshore in order to utilise a service that is required to perform the primary purpose for which the information was collected. NAPHL takes reasonable steps to ensure the security and handling of the information adheres to the APPs, and that the recipient of the information is subject to a similar law or binding scheme to the *Privacy Act 1988* and the APPs.

Access to, and correction of, personal information
Consumers have a right to access their personal information. In order to access personal information, a consumer should contact their NAPHL service provider in the first instance. The service provider is required to verify the identity of the consumer, and to provide the consumer with access to the requested personal information within 30 days, unless an exception applies under the APP.

If a consumer notifies the service provider that personal information held by NAPHL is inaccurate or incorrect, the service provider is to review the personal information, and correct the information within 30 days, unless the service provider is satisfied that the information held by NAPHL is correct.

Consumers have a right to ensure that health information is confidential. Provided a consumer is competent to request access to information, no other person is entitled to access information without the patient's authority. This includes partners/spouses/relatives and parents (where the minor is considered capable of making their own decisions).

Online Security Breach
Online security breach can be split into two categories:

- Online Security Breach (cyber breach): includes physical breach e.g. someone steals a laptop or the loss of a USB stick with sensitive information stored on it.
- Data Breach: especially in a medical setting where you have multiple identifiers, private and confidential information.

Disposal of information
NAPHL will destroy or permanently de-identify any personal information which is in its possession or control and which is no longer needed for the purpose for which it was collected provided NAPHL is not required under an Australian law or court/tribunal or otherwise to retain the information.
If information is no longer required for the primary purpose for which it was collected, is must be disposed of in accordance with the NAPHL Retention and Disposal Schedule.

Media consent
NAPHL considers on a case by case basis whether media consent is required from consumers that may be exposed to the media. Generally this is required from employees or consumers that will directly interact with the media, or feature in NAPHL developed marketing or communication outputs.

CCTV Cameras
NAPHL does use camera surveillance systems (commonly referred to as CCTV), at its Townsville Mental Health facility (Riverway) for the purpose of maintaining the safety and security of its employees, consumers, visitors and other attendees to the facility. The format of this monitoring and recording system is a 24 hour motion detected visual surveillance (not including sound) and is considered "overt surveillance" i.e. clearly visible cameras and signage that will notify persons that the area they are in is under surveillance and the purpose for the surveillance.

NAPHL will comply with the Information Privacy Act 2009, the Right to Information Act 2009, APPs and this Privacy Policy in respect of any information collected via its CCTV systems.