3.4 PRIVACY AND CONFIDENTIALITY POLICY

Policy Statement:

FPWNT collects and stores the personal information of: our clinical clients, individuals participating in education training courses, project partners and other external stakeholders, our staff, work placement participants, volunteers and website visitors.

FPWNT is committed to open and transparent management of personal information and to compliance with the Australian Privacy Principles and other legislation. In order to meet this commitment, FPWNT will:

- educate staff and volunteers about information privacy
- inform stakeholders of FPWNT privacy policy and procedures for managing personal information
- handle complaints received in an efficient and appropriate manner
- monitor privacy compliance

Background:

In relation to personal information collected by non-government health organisation in the NT main laws that protect the privacy of FPWNT client are the Privacy Act 1988 (CTH), the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Australian Privacy Principles.

http://www.oaic.gov.au/news-and-events/news/privacy-news/oaic-releases-app-guidelines

- applies to both the Australian Government (Commonwealth) and private sector organisations across Australia
- establishes the Australian Privacy Principles
- is administered by the Office of the Australian Information Commissioner http://www.oaic.gov.au

The aim of this policy statement is to summarise FPWNT's privacy obligations and to document procedures in place to meet these obligation. Staff will be advised of their privacy obligations at staff induction and reminded at staff meetings, staff newsletters and alerts in electronic systems. Staff must sign a Confidentiality Agreement form as a reminder of their privacy obligations.

Definitions and Abbreviations:

Confidentiality and privacy
The concepts of 'privacy' and 'confidentiality' may seem the same, but the terms are not synonymous.
"The common law governing breach of confidence addresses trade secrets and other information which has been conveyed in confidence and which is not readily available to the public. Legislation governing "privacy" addresses the use of personal information about individuals, whether or not that information is publicly available. Confidentiality arises from the "duty of confidence' which is protected both by common law and legislation."

Australia's New Privacy Laws - What Lawyers Need to Know about Their Own Practices
Law Council of Australia October 2001

De-identified information
De-identification of personal information can enable information to be shared or published without jeopardising personal privacy. More information about de-identification is available from the Office of the Australian Information Commissioner. http://www.oaic.gov.au

Confidentiality is important for several reasons:

- It benefits clients by providing a secure environment in which they are most likely to seek medical care and to give a full and frank account of their illness when they do;
- It supports public confidence and trust in healthcare services more generally;
- It expresses respect for clients' autonomy: people have a right to choose who will have access to information about them, and a rule of confidentiality for medical practitioners reassures patients that they can determine who will be privy to their secrets.

These are three robust arguments for maintaining confidentiality, but there are some circumstances in which breaches of confidentiality are permissible, and sometimes even necessary.
Sharing patient information between professionals: confidentiality and ethics
Annette J Braunack-Mayer and Ea C Mulligan
MJA 2003 178 (6): 277-279
Retrieved from http://www.mja.com.au/public/issues/178_06_170303/bra10520_fm.htm l 16 July 2009

Personal information

The PPIP Act defines 'personal information' as 'any information or opinion about an identifiable person'. This could include:

- written records about a person
- a photograph or image of a person
- DNA samples that identify a person
- Information about a person that is not written down, but which is in the possession or control of the agency.

Sensitive information (as defined in S6 Privacy Act 1988):
(a) information or an opinion about an individual's:
(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual preferences or practices; or
(ix) criminal record;
that is also personal information; or
(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information.

Exclusions
Commonwealth privacy law does not create privacy obligations for deceased individuals.

SCOPE:

All FPWNT staff and volunteers.

POLICY DETAILS:

FPWNT complies with the Australian Privacy Principles as follows:

- *Australian Privacy Principle 1 (APP1)*
  - commitment to open and transparent management of personal information

FPWNT procedures for the collection and disclosure of personal information are outlined in detail below. Individuals seeking further information about our privacy policy are invited to complete a request form.

- *Australian Privacy Principle 2 (APP2)*
  - anonymity and pseudonymity.

As far as possible, FPWNT enables clients to receive services anonymously or via a pseudonym, or by providing only limited personal information.

FPWNT may require full client names and current contact details in some circumstances including the provision of ongoing clinical care when the client needs to be advised of test results etc. In general, the decision regarding degree of personal information required will be made by the staff member providing the service e.g. clinician, researcher or educator who will explain the consequences of not providing the information requested.

- *Australian Privacy Principle 3 (APP3)*
  - collection of solicited personal information

Where possible, information will be collected directly from the individual. Information will not be collected 'just in case' it is needed.
Sensitive information will be collected only when and as reasonably necessary for or directly related to Family Planning NT activities and with the consent of the individual.
FPWNT will ensure that collection of personal information is not unreasonably intrusive.
Information should be collected in an environment where the potential for other people to overhear is minimised. Where it is not possible to collect information directly from the client, the information supplied will be checked for accuracy. This includes information collected from other health provider as part of a referral.

- *Australian Privacy Principle 4 (APP4)*
  - dealing with unsolicited information

Sometimes information is received that was not sought, an example may be information about a client's criminal behaviour that is irrelevant to their clinical care. Information received is this way will be deidentified or destroyed.

- *Australian Privacy Principle 5 (APP5)*
  - notification of the collection of personal information

Reasonable steps will be taken at or before the time of collection to ensure that the individual is aware of:

- the purposes for which the information is being collected and how the information is likely to be used
- the organisations (or types of organisations) to which the information would be disclosed, if any
- details about the individual's right to access the information, to seek correction or make a complaint

Details about the information FPWNT collects will be provided to clients.

- *Australian Privacy Principle 6 (APP6)*
  - use and disclosure of personal information

Information collected will only be used or disclosed for the primary purpose for which it was originally collected, unless it is disclosed for one of the following reasons:

- for a secondary purpose which is related to the primary purpose and which may be reasonably expected by an individual
- with the express consent of the individual
- authorised by or under law

All FPWNT clinical services and activities are confidential. No information about a client or the fact they attended a FPWNT service, is to be divulged or discussed with any person including the client's family members or friends unless specifically authorised by the client. Clinical staff are required to verify the client's consent.

Information may be sent to the client's GP only with the client's express permission. Please refer to FPWNTP Client Request for File Information.

Exemptions to the right to confidentiality

Exemptions to confidentiality occur where the release of such information is required in the interests of patient care or where disclosure is required by law or for medical insurance purposes.

For further information on the release of clinical information contained within FPWNT clinical records consult the Clinic Coordinator/ Medical Director/CEO.

Legal exceptions to the client's rights to confidentiality exist, and these are to be made clear to the client at their first visit to FPWNT and on any other occasions when a breach of confidentiality may be necessary;

- Sharing information/consulting with other health professionals to facilitate the best care and treatment for the client.
- Subpoena of documents.
- Public interest; for example:
  - Staff member has knowledge that the client could harm himself/herself or someone else
  - The client has been reported as a missing person
  - The staff member has knowledge that the client has been involved in a serious crime
  - The staff member has knowledge that a child (a child is a person under 16years of age) or young person (a young person is 16 or 17 years of age) is at serious risk of harm.

Disclosure can occur to a 'person responsible' for an individual if that individual is incapable of giving or communicating consent. In the case of a child or young person, the practitioner needs to make a judgement about that individual's competence. If judged competent, the child or young person can refuse permission for disclosure.

HIV confidentiality

FPWNT staff should be aware of the special provisions that relate to disclosing information about an individual's HIV status. Guidance is provided through a number of health policies including HIV Confidentially. http://www.afao.org.au/about-hiv/hiv-and-the-law/criminalisation

Medicare

Medicare captures the personal health information of FPWNT clients, in the form of demographic and service delivery data, through the bulk billing process. It is important that FPWNT staff understand how Medicare manages personal health information.

The following information has been provided by the Privacy and FOI Branch, Department of Human Services – Centrelink on 2 May 2012 to FPNSW:

Medicare Australia has a policy to protect the personal and sensitive information of children 14 years of age or older. This is known as the Parental Access Policy (the Policy). The Policy aims to balance the need to protect the privacy of an individual's health information with the need for parents and legal guardians to access information about children for whom they are responsible.

A parent cannot obtain detailed claim information about a child on their Medicare Card where that child is 14 years of age or older. A child 14 years of age or older can provide consent for the parent to obtain the information if they choose. A parent can request a Medicare Statement of Benefits for a child that is under the age of 18 years who is on the same Medicare Card as the requesting parent, without the consent of that person. However, the statement only sets out the total cost of Medicare benefits paid for services received by a person on that Medicare Card for the financial year, and does not specify the services received.

The only information that can be requested from Medicare, or viewed online, in relation to children 14 years of age or older, is information relating to the total costs of claims requested, the subsequent benefits paid and the out of pocket expenses. As mentioned, a parent can request further information relating to consultation types if they have the consent of the child, or other legal authorisation such as a Power of Attorney. Where a person aged 14 years of age or older has not provided their consent for disclosure, Medicare will, if asked, forward the request to the individuals most recent or most frequently consulted treating practitioner. The practitioner may provide information to the requesting parent if, in the view of the practitioner, it is ethical and appropriate to do so.

With regard to children aged under 14 years of age, specific claims information can generally be requested from Medicare and can also be viewed in Medicare's online systems provided there is no identified risk of harm to that child associated with the disclosure. Where the child is on the same Medicare Card as the requesting parent, and only appears on that Medicare Card, and the requesting parent knows the child's current address, Medicare will usually release claims information to the requestor.

In cases where the requesting parent and the child are not on the same Medicare Card, or the child's name appears on more than one Medicare Card, or the requestor does not know the child's address as recorded on Medicare's database, there may be a risk associated with the disclosure of the child's information. In these instances those requests will be forwarded to the Privacy and Information Release Section within Medicare for assessment.

Spousal information is not provided to other individuals listed on the Medicare Card. Only the total of benefits paid for taxation purposes is provided in relation to all individuals listed on the card. No

specific claims information for other persons listed on the card can be requested or viewed by spouses unless there is specific authorisation, such as a Power of Attorney.

Disclosure of personal information to contractors

Where it is likely that contractors will have access to personal information held by Family Planning NT, the contractor must be asked to sign a FPWNT Contract for Services or a Confidentiality Agreement. As necessary, specific information handling procedures should be specified and incorporated into the agreement, to ensure that the contractor is aware of the level of sensitivity of the information and the standard of protection required by the organisation.

- *Australian Privacy Principle 7 (APP7)*
  - direct marketing

FPWNT may send direct marketing material to our clients, customers and participants using the contact details they have supplied providing we enable them easily to opt off the mailing list. At the time of collecting personal information, clients should be advised how the information will be used in the future and given the opportunity to opt out.

Sensitive information will only be used for direct marketing purposes where the individual has consented for the information to be used in that way i.e. FPWNT cannot canvass members of a particular racial group without their consent to be contacted in that way.

Where an individual questions the source of the personal information held about them, FPWNT will respond appropriately in a timely way.

- *Australian Privacy Principle 8 (APP8)*
  - cross-border disclosures

FPWNT will not transfer personal information to an overseas recipient without the consent of the individual.

- *Australian Privacy Principle 9 (APP9)*
  - adoption, use or disclosure of government related identifiers

FPWNT will not adopt a government related identifier of an individual as its own identifier. A Medicare number is not an approved identifier for clinic clients but Individual Healthcare Identifier (IHI) can be used to identify clients.

- *Australian Privacy Principle 10 (APP10)*
  - quality of personal information

FPWNT is committed to ensure that personal and health information is accurate and complete.

 personal information is protected from misuse, loss, unauthorised access, modification or disclosure:

 personal information is destroyed or permanently de-identified when it is no longer required

- *Australian Privacy Principle 11 (APP11)*
  - security of personal information,

FPWNT is committed to ensure that personal information is held securely and maintained appropriately. Information may be stored in hard copy documents, or as electronic data. Strategies to protect the information include:

- signed undertakings by staff to abide by confidentiality requirements. This also includes all observers (for example, work placement participants) and FPWNT course participants who take any part in clinical consultations.

- policies on document storage and security
- security measures for access to computer systems
- web site protection measures.

FPWNT will ensure that when personal information is destroyed, a record is kept of the name of the individual to whom the health information related, the period it covered and the date it was disposed of.

Security for clinic clients

The personal health information of clients is protected in the following ways:

a. at reception

- receptionists act to maintain the client's confidentiality by asking for personal information in a way which enables the client to answer discreetly.
- client files are not left unattended or in open view
- strategies such as screen savers, password protected timeout and selecting the angle of computer screens are used to ensure that screens displaying personal health information cannot be easily seen and read by the general public
- receptionists ringing clients confirm that they are speaking to the client before saying where they are ringing from or revealing anything about the appointment
- staff do not discuss clients where they can be overheard by members of the public

b. during consultation

- post graduate doctors or nurses participating in or observing the consultation sign an undertaking to abide by confidentiality requirements
- clients are advised that FPWNT is a training organisation and a second doctor or nurse may be present during the consultation
- clients are consulted before a third party attends the consultation
- the consultation is conducted in a manner which protects the privacy and confidentiality of the client

c. through quality assurance measures

- In line with established audit protocols, FPWNT staff engaged in quality management and data audit will access client records for the purposes of ensuring data integrity, accuracy and completeness. FPWNT recognises that information integrity is critical for quality client care; evaluation of services, service planning and reporting to funders.
- Staff will access electronic client records through their individual user names and passwords Access to records will be audited on an ongoing basis and any breaches in protocol will be addressed in line with the FPWNT Internet, Email and Computer use Policy 3.12
- Client information may be disclosed to an external auditor or quality assessor for the purposes of monitoring, evaluating or auditing the provision of a particular service, as long as the individual reviewing the records is bound by privacy legislation or a professional code of ethics.

d. during file storage and retrieval

- access to files is restricted
- files are stored securely during the day and locked in the compactus/filing cabinet at night
- files are disposed of as prescribed in the Destruction of records policy 3.7

e. during the management of results

- results are managed in accordance with clinical protocols and legislative requirements.

f. scanning

- At FPWNT the scanning process often requires the scanned image to be saved on a public folder prior to be being redirected to relevant client file. The scanned images must be deleted from FPWNT public folders as soon as possible after scanning. The original documents from which the image has been copied must be handled appropriately, stored securely and held for only as long as is necessary, which may include time to complete quality assurance checks.

- *Australian Privacy Principle 12 (APP12)*
  - access to personal information

FPWNT will consider all requests for access to the personal information held, subject to considerations of risk and harm to others and commercial sensitivity. Clinical clients may access their clinical data in accordance with FPWNT Client and Personnel files and Information Access policy 3.5.

Clients are welcome to contact a member of staff, who will refer the request to the relevant manager, or to complete the necessary form. When information is not made available, FPWNT will provide an explanation to the applicant.

- *Australian Privacy Principle 13 (APP13)*
  - correction of personal information.

When requested, FPWNT will endeavour to correct personal information to ensure that it is accurate, up to date, complete and not misleading. This response will be provided within 30 days of receiving the request. If correction is refused, FPWNT will provide an explanation and advice will be provided about lodging a complaint. In place of amending the information, the individual and FPWNT may agree to incorporate a statement about the accuracy of the information in the record. For clinical clients, refer to Policy 3.5.

Managing Proof of Identity Documents to verifying claims made by prospective staff or students

FPWNT is obliged to only collect personal information which is required for a specific purpose. Individuals should be told why the information is required and how it will be handled.

Managing credit card details

FPWNT is committed to protecting the credit card information of clients from loss, misuse and unauthorised disclosure. Please refer to FPWNT Petty Cash Management, Cash Handling & Receipting procedure 5.1

Ratified by Board of Management September 2010
Updated June 2011
Endorsed by the BOM September 2011
Updated August 2013
Reviewed August 2014 and Ratified by Board of Management August 2014