Document No: 2025/016

PRIVACY AND CONFIDENTIALITY POLICY

Contents

REVISION HISTORY

Latest update 2025 approved by Board 25/02/2025

POLICY STATEMENT

Family Planning Australia collects and stores the personal information of:

- Clinical clients
- Research participants
- Education course participants
- Shop customers
- Project partners and other external stakeholders
- Staff
- Prospective staff
- Website visitors
- Student / Work placement participants
- Volunteers
- Donors

Family Planning Australia is committed to the open and transparent management of personal information and to compliance with the Australian Privacy Principles and other legislation.

In order to meet this commitment, Family Planning Australia:

- educates staff about information privacy
- informs stakeholders of Family Planning Australia privacy policy and procedures for managing personal information
- handles complaints received in an efficient and appropriate manner
- monitors privacy compliance.

PURPOSE

In relation to personal information collected by non-government health care organisations in NSW, there are three main laws that protect the privacy of Family Planning Australia clients and participants:

These are:

- Privacy Act 1988 (Cth), the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Australian Privacy Principles
  - 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
- the Privacy and Personal Information Protection Act 1998 (NSW) [PPIP]
  - applies to NSW state and local government agencies
  - sets privacy standards for dealing with personal information
  - is administered by Privacy NSW
- the Health Records and Information Privacy Act 2002 (NSW) [HRIPA]
  - applies to NSW state and local government agencies
  - sets privacy standards for dealing with personal health information

- applies to private sector persons and organisations in NSW
- is administered by Privacy NSW.

In addition, NSW Health has developed the Privacy Manual for Health Information 2015 as a guide to the obligations imposed by the HRIPA.

While, the privacy principles are generally consistent across the three Acts, Family Planning Australia must take care to ensure that specific obligations are met where necessary. Where conflict arises between HRIPA (NSW) and the Privacy Act (Clth), the Privacy Act will apply. *(Source: Privacy NSW Privacy Essentials - No 2 2004)*

Advice received from Legal Branch NSW Health, Privacy NSW and the Office of the Privacy Commissioner is that if any areas of concern arise, the specific legislation should be closely reviewed and if necessary, legal advice sought to clarify responsibilities. *(Source: correspondence from Privacy NSW and Office of the Privacy Commissioner March 2008, verbal communication from staff of Legal Branch, NSW Health March 2008)*

The aim of this policy statement is to summarise Family Planning Australia's privacy obligations and to document procedures in place to meet these obligations. Staff are advised of their privacy obligations at staff induction, and reminded at staff meetings, staff newsletters and alerts in electronic systems etc. Each year, staff are asked to sign a Commitment to Confidentiality as a reminder of their privacy obligations.

SCOPE

All Family Planning Australia staff and Directors of the Board.

DEFINITIONS

Term	Meaning
Confidentiality and privacy	*"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.
Personal information	The PPIP Act and HRIPP Act define 'personal information' as 'any information or opinion about an identifiable person'. This could include: • written records about a person

Term	Meaning
	• a photograph, image of a person or a recording of a person's attendance at training • 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.
Personal health information	"Health information' is defined to mean: • information or an opinion, that is also personal information, about: • the health or a disability (at any time) of an individual, or • an individual's expressed wishes about the future provision of health services to him or her, or • a health service provided, or to be provided, to an individual, or • other personal information collected to provide, or in providing, a health service, or • other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances, or • genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual. (Other types of genetic information that are not health information fall within the definition of 'sensitive information" (Extracted from the Office of the Australian Information Commissioner) The HRIP defines 'personal health information' as information collected in connection with providing health services, including information or opinion about: • a person's physical or mental health or disability • a person's express wishes about the future provision of health services for themselves • a health service provided or about to be provided to a person. (Privacy Manual for Health Information 2015 pg. 5)
Sensitive information	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*

Term	Meaning
	(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	Privacy principles do not apply to personal information which is stored in such a way that individuals cannot be identified. (Reference Office of the Australian Information Commissioner) NSW privacy law extends for 30 years after death. Commonwealth privacy law does not create privacy obligations for deceased individuals.

POLICY DETAILS

Family Planning Australia complies with the Australian Privacy Principles as follows:

Australian Privacy Principle 1 (APP1): Commitment to open and transparent management of personal information

Family Planning Australia procedures for the collection and disclosure of personal information are outlined in detail below and in summary athttps://www.fpnsw.org.au/about-us/policies/privacy-policy. Individuals seeking further information about our privacy policy are invited to complete the request form on the website.

Australian Privacy Principle 2 (APP2): Anonymity and pseudonymity

As far as possible, Family Planning Australia enables clients and participants to receive services anonymously or via a pseudonym, or by providing only limited personal information.

Family Planning Australia requires 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, the collection of course participant details for compliance and reporting requirements 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 and for specific purposes.

Sensitive information will be collected only when and as reasonably necessary for, or directly related to, Family Planning Australia activities and with the consent of the individual.

Family Planning Australia 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". (section 7.2 Privacy Manual for Health Information 2015).

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 providers as part of a referral. (section 10.0 Privacy Manual for Health Information 2015).

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 Family Planning Australia collects will be provided to clients and participants in brochures, registration forms, posters and on the website.

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; (section 11.2 Privacy Manual for Health Information 2015)
- with the express consent of the individual (section 11.2.2 Privacy Manual for Health Information 2015)
- authorised by or under law

All FPA clinical services, education and activities are confidential. No information about a person or the fact they attended a FPA service or education is to be divulged or discussed with any person, including the person's family members or friends, unless specifically authorised by the person. In the case of clinical services before the release of any information contained within that client's file, Clinical staff are required to confirm the client's identity, asking the client to provide three of the four approved identifiers (see Confirming Identity of Clients policy):

- Name
- Address
- Date of birth
- FPA file number

Requests from a client for information from their health care record, other than test results, should be made in writing (see Provision of Health Care Summaries policy). It is the responsibility of the Medical Coordinator, or delegate, to check the identifying information provided by the client against FPA records and then to confirm the identity of the person requesting the information. Depending on whether the client is present, this may be done by:

- checking the signature on the written request against the signature on the client's license / passport/ forms signed previously
- contacting the client to confirm the request and verifying the client's name, date of birth, address and other information.

If the Medical Coordinator has any concerns, the client should be asked to attend the clinic in person so that their identity can be verified.

> *Patients should be given as much prospective information as possible concerning the types of people to whom their health information may subsequently be disclosed. This advice will reduce the number of situations in which implicit consent for routine information transfers is relied upon. If a patient has not been advised that his or her information will be disclosed, clinicians need to satisfy themselves that they are acting in the individual patient's best interests and that broader social benefits outweigh the social cost of compromising confidentiality.*
>
> ***Sharing patient information between professionals: confidentiality and ethics***
>
> *Annette J Braunack-Mayer and Ea C Mulligan*

Information may be sent to the client's GP only with the client's express permission. Please refer to Provision of Health Care Summaries.

For education purposes where a participant's attendance is subsidised by an employer Family Planning Australia may provide, on written request from the employer, general information about the participant's attendance and ongoing progress.

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 FPA clinical records consult the Director Integrated Health Service or Medical Director.

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 FPA and on any other occasions when a breach of confidentiality may be necessary, including;

- 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 16 years of age) or young person (a young person is 16 or 17 years of age) is at serious risk of harm (see the FPA Child Protection Policy). Further information on obligations for mandatory reporters in these and similar circumstances follows below.

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.

For education, disclosure of personal information may be required for the purposes of compliance with regulatory authorities and contracts, such as reporting to funding bodies. Wherever possible, de-identified data will be used for such purposes.

Mandatory reporting obligations

Reference is made to sections 23 and 24 of the Children and Young Persons (Care and Protection) Act 1998 (NSW). These sections of the Act outline specific examples of circumstances that can be defined as placing a young person "at risk of significant harm" and empower mandatory reports in reporting these circumstances to the authorities.

Individuals are also bound by responsibilities as outlined in the NSW Mandatory Reporter Guide. This guide provides mandatory reporters with an on-line decision making support tool to assist in decisions around these processes.

HIV confidentiality

Amendments to the Public Health Act 2010 which commenced in September 2017, allow HIV information to be accessed by clinical staff treating a client with HIV. Previously, HIV information has only been available to staff directly involved in care and treatment of the client's HIV infection and HIV-related counselling. NSW Health Guide to Managing HIV Information

Medicare

Medicare captures the personal health information of FPA clients, in the form of demographic and service delivery data, through the bulk billing process. It is important that FPA 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:**

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 Australia, the contractor must be asked to sign a FPA 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

Family Planning Australia 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. Family Planning Australia 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, Family Planning Australia will respond appropriately in a timely way.

As a health promotion charity, FPA is not subject to the Spam ACT.

Australian Privacy Principle 8 (APP8): Cross-border disclosures

Family Planning Australia 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

Family Planning Australia 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

Family Planning Australia 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

Family Planning Australia 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 Family Planning Australia 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.

See Data Security and Handling Standards and IT and Cloud Systems Usage Policy

Family Planning Australia 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. HPIPA Sect 25(2).

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 Family Planning Australia is a training organisation and a second doctor or nurse may be present during the consultation HPIPA Sect 10(e)
- clients are consulted before a third party attends the consultation Refer to Family Planning Australia Third party present in consultations
- 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, Family Planning Australia staff engaged in quality management and data audit will access client records for the purposes of ensuring data integrity, accuracy and completeness. Family Planning Australia 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 Family Planning Australia IT and Cloud System Usage Policy and Procedure.
- 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 (*section 11.2* Privacy Manual for Health Information 2015*).*

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 Management of Health Records policy

e. during the management of results

- results are managed in accordance with Management of requests, results, reminders, referrals & correspondence Policy

f. scanning

- At Family Planning Australia the scanning process often requires the scanned image to be saved on a public folder on the F:drive prior to be being redirected to relevant client file. The scanned images must be deleted from Family Planning Australia 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. Please refer to Private Sector Information Sheet 20- Scanning Proof of Identity documents Office of Privacy Commissioner.

Security for course participants

The personal information of participants who attend courses is protected in the following ways:

a. during the course

- only staff directly involved in the administration of a course have access to a participant's file
- information about course attendance, progression and completion is only accessed by those staff who are responsible for the overall coordination of each course

b. through quality assurance measures

- In line with established audit protocols, Family Planning Australia staff engaged in quality management may access participant records for the purposes of ensuring data integrity, accuracy and completeness. Family Planning Australia recognises that information integrity is critical for quality evaluation of education, planning and reporting to funders
- Staff will access electronic participant records through their individual user names and passwords. Access to records follows the Family Planning Australia IT and Cloud System Usage Policy and Procedure
- Participant information may be disclosed to an external auditor or quality assessor for the purposes of monitoring, evaluating or auditing the provision of a particular course.

c. during file storage and retrieval

- access to files is restricted in the student management system
- any paper files are stored securely during the day and locked at night
- files are disposed of as prescribed in the Document management policy

d. scanning

- At Family Planning Australia the scanning process often requires the scanned image to be saved on a public folder on the F:drive prior to be being redirected to relevant participant file. The scanned images must be deleted from Family Planning Australia 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. Please refer to Private Sector Information Sheet 20- Scanning Proof of Identity documents Office of Privacy Commissioner.

Australian Privacy Principle 12 (APP12): Access to personal information

Family Planning Australia will consider all requests for access to the personal information held, subject to considerations of risk and harm to others and commercial sensitivity.

Clients and course participants are welcome to contact a member of staff, who will refer the request to the relevant manager. When information is not made available, Family Planning Australia will provide an explanation to the applicant.

Australian Privacy Principle 13 (APP13): Correction of personal information

When requested, Family Planning Australia will endeavor 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, Family Planning Australia will provide an explanation and advice will be provided about lodging a complaint. In place of amending the information, the individual and Family Planning Australia may agree to incorporate a statement about the accuracy of the information in the record.

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

Family Planning Australia 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

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

RELATED DOCUMENTS

Office of the Australian Information Commissioner

NSW Health - Privacy Manual for Health Information

COMPLIANCE STRATEGY

Item	Audit frequency /evidence	Person responsible
Signed Commitment to Confidentiality	Annual	Executive