PRIVACY POLICY

1. Background

Family Planning Queensland is strongly committed to protecting the privacy of all individuals with whom it interacts or through who use its products and/or services.

Family Planning Queensland collects personal information in order to conduct its business and to meet its legislative obligations. Organisationally it is bound by legislation in the management of matters relating to the privacy of personal information.

Family Planning Queensland is committed to treating the personal information we collect in accordance with the Australian Privacy Principles (APP) in the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (Reform Act).

The APP provide a privacy protection framework that supports the rights and obligations of collecting, holding, using, accessing and correcting personal information. The APP consists of 13 principle-based laws which apply equally to paper-based and digital environments. The APP complements the long-standing FPQ organisational obligation to manage personal information in a regulated, open and transparent manner.

This policy does not apply to personal information collected by Family Planning Queensland that is exempted under the Privacy Act.

2. Purpose

To enable transparency of Family Planning Queensland’s operations according to the Australian Privacy Principles.

To communicate Family Planning Queensland's collection, use and management of personal information (including health information).

To communicate the circumstances under which FPQ would be required to disclose personal information to third parties.

To ensure clients and staff of Family Planning Queensland (FPQ) are comfortable with entrusting their personal information to the organisation.

To provide guidance for staff in compliance with the legislative requirements related to personal information collection, use, security and disclosure.

To provide public access to FPQ privacy policy.

3. Scope

All FPQ Staff, visitors, contractors, members, clients / beneficiaries, donors, online users.

4. Abbreviations and Definitions

Australian Privacy Principles (APP’s):

The Australian Privacy Principles as per Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (Reform Act) as from March 12th 2014.
Cookies:
A "cookie" is a packet of information stored on your computer that allows the FPQ server to identify and interact more effectively with your computer.

Health information:
Information or an opinion about:
- The health or a disability of an individual
- An individual’s expressed wishes about the future provision of health service to him or her
- A health service provided
- Other personal information collected to provide, or in providing a health services
- Other personal information about an individual collected in connection with the donation.

Misuse:
Information held is used for a purpose other than a permitted purpose.

Personal information:
Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in material form or not, for example:
- A person’s name and address
- Medical records
- Bank account details
- Photographs of an individual
- Videos including CCTV footage
- Information about likes and dislikes
- Place of employment.

Reasonable steps:
Determination of what are considered ‘reasonable steps’ to ensure information security will depend on the circumstances, including the following:
- The nature of the entity holding the personal information i.e. size and business model
- The nature and quantity of personal information held i.e. sensitive information
- The risk to the individuals concerned if the personal information is not secured
- The data handling practices of the entity holding the information
- The ease with which a security measure can be implemented.

Sensitive information:
As defined in Section 6 of the Privacy Act means:
(a) Personal Information or an opinion about an individual's:
- Racial or ethnic origin
- Political opinions
- Membership of political associations
- Religious beliefs or affiliations
- Philosophical beliefs
- Memberships of professional / trade associations
- Sexual preferences or practices
- Criminal record;
- Health information about an individual; or
- Genetic information about an individual that is not otherwise health information.
5. Policy Statement

5.1. Open and transparent management of personal information
FPQ, by way of this policy confirm open and transparent management of personal information in accordance with the Australian Privacy Principles.

FPQ will provide employees with training to enable them to understand the importance of good information handling and security practices including their responsibilities with respect to the protection of personal information.

5.2. Anonymity
FPQ will, where lawful and practicable, give individuals the option of not identifying themselves when dealing with FPQ.

5.3. Collection of Personal Information and notification of the collection
FPQ will collect and use personal information (including health information and sensitive information) that is directly related to the functions or activities of the organisation (clinical, education and training settings) or activities carried out in support of its corporate functions such as human resources, business administration, property management and public relations activities.

FPQ will only collect personal information from the individual where there is a legitimate reason to do so. FPQ will collect personal information from another individual when the person has delegated another individual to provide the information on their behalf e.g. Next of kin.

FPQ staff will take reasonable steps to ensure patients understand:
- what information has been and is being collected
- why the information is being collected, and whether this is due to a legal requirement
- how the information will be used or disclosed
- why and when their consent is necessary
- the procedures for access and correction of information, and responding to complaints of information breaches, including by providing this policy.

Personal information includes “sensitive information”. FPQ will only collect sensitive information that is required for the primary purpose of client care. If sensitive information is required for secondary or unrelated purposes such as data analysis or research, FPQ will always obtain the informed consent of the client.

FPQ may store the personal information we collect from you in various forms, including through an electronic medical record system, in which the data is stored in a secure external environment. FPQ will comply with the APPs, and this Privacy Policy, in respect of your personal information in whatever form that information is stored by us.

Personal information may also be collected when an individual:
- completes a course registration form
- seeks support or advice via the telephone or via email or request FPQ contact
- purchases a product
- makes and/or attends a clinical appointment.

5.3.1 Personal health information
FPQ needs information about a client’s past and current health to provide high quality care.

This information is called “personal health information”.

The clinic staff will need to collect personal information as a provision of clinical services to a client at the practice. Collected personal information will include:
- client name, address and contact details
- Medicare number (where available - for identification and claiming purposes)
- healthcare identifiers
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors.

FPQ will only collect information that is relevant to a client’s care. Clients are encouraged to ask the doctor, nurse or educator if they are uncertain about why the information is being collected.

5.3.2 Dealing with Unsolicited Personal Information

FPQ evaluates all unsolicited information it receives to decide if it should be kept, acted on or destroyed.

5.4 Use or disclosure of Personal Information

FPQ will use and disclose information only for the purpose it is given to us, or for purposes related to one of its activities in clinics and education or training settings.

FPQ will not disclose an individual’s personal information to a third party unless the person has consented to this release. FPQ will take all reasonable steps to maintain the privacy of all information except as is otherwise required by law. If the data is to be used for secondary or unrelated purposes such as data analysis or research, FPQ will obtain the informed consent of the person.

5.4.1 Use or disclosure of Personal Health Information

Clinical Services will not disclose personal information to any third party other than in the course of providing medical services, without full disclosure to the client or the recipient, the reason for the information transfer and full consent from the client.

Exceptions to disclose without patient consent are where the information is:

- required by law
- necessary to lessen or prevent a serious threat to a patient’s life, health or safety or public health or safety, or it is impractical to obtain the patient’s consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of a confidential dispute resolution process.

Personal information will only be used for the purpose of providing medical services and for claims and payments, unless otherwise consented to. Some disclosure may occur to third parties engaged by or for the clinic for business purposes, such as accreditation or for the provision of information technology. These third parties are required to comply with this policy. FPQ clinicians will inform the patient where there is a statutory requirement to disclose certain personal information (for example, some medical conditions require mandatory notification).

5.5 Direct Marketing

FPQ will not use any personal information in relation to direct marketing to a client without that clients expressed consent.

Patients and clients may opt-out of direct marketing at any time by notifying FPQ through a letter or an email.

5.6 Quality of Personal Information

FPQ will take all reasonable steps to make sure that information we collect or disclose is accurate, complete and up to date.
5.7 Security of Personal Information

The personal information FPQ holds is stored in a secure manner. FPQ and our contracted partner(s) will protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure. We use technologies and processes such as access control and network firewalls to protect your privacy. When information is no longer needed it will be destroyed (unless it is required under law to retain the record).

Personal information held by FPQ will be:

- received and stored in a secure location
- accessible by staff on a need to know basis only
- protected from viewing by unauthorised persons
- not taken from FPQ premises unless authorised and for a specific purpose.

5.8 FPQ website and IT system security and privacy

Use of the FPQ website, will not enable personal identification of an individual user and FPQ will not collect personal information unless specifically provided to FPQ through an online transaction. All of this information is used by FPQ for aggregated statistical analyses or systems administration purposes only. No attempt will be made to identify users or their browsing activities, except where required by law.

FPQ use cookies (see definitions) and other internet technologies to manage its website and online products and services. FPQ may collect non-personal information from an individual browser through its server to aid website management including:

- the type of browser and operating system used to access
- the Internet Service Provider and top level domain name
- the address of any referring web site
- the accessing of a computer's Internet Protocol (IP) address.

5.8.1 Links to other sites

FPQ may create links to third party websites. FPQ are not responsible for the content or privacy practices employed by websites that are linked from our website.

5.8.2 Emails

FPQ’s internet service provider or information technology staff may monitor email traffic for system trouble shooting and maintenance purposes only.

5.9 Access and correction of Personal Information

Information will be made available to an individual who requests their personal information including their medical records. Clients are encouraged to make this request in writing, and FPQ will respond within a reasonable time.

We may refuse access if we reasonably believe that:

- the request does not relate to the personal information of the person making the request
- a person’s health, safety and wellbeing may be compromised by releasing the information
- providing access would be unlawful or would prejudice a legal investigation
- the request is frivolous and/or vexatious
- the information relates to an existing or anticipated legal claim between FPQ and the client, and the information would not be accessible through the legal discovery process.

FPQ will take reasonable steps to correct personal information where it is clear that the records are not accurate or up to date. If you believe that information held by FPQ is incorrect or inaccurate, we will take all reasonable steps to amend or correct the information.
From time to time, the clinicians will ask clients to verify the personal information held by the service is correct and up to date.

Clients may also make a written request for the staff to correct or update their information.

FPQ will respond in writing to an individual where a request to access their personal information or to grant access in the manner requested by the individual OR a request for correction to personal information is refused, and state the reasons for refusal and the mechanism to complain about the refusal.

5.10 Identifiers

FPQ will adopt its own identifier system in respect of individuals. FPQ will not use or disclose the identifier unless necessary for client care.

5.11 Cross-border disclosure of Personal Information

The Commonwealth Privacy Act limits the flow of information outside Australia.

FPQ will not disclose personal information to anyone outside Australia without need and without client consent.

5.12 Breach of personal information

FPQ will respond to a suspected or known breach of personal information including informing an individual(s) of a breach, investigating breaches, identifying causes and correcting deficits and where required notifying other parties.

5.13 Enquires or complaints

Enquiries or complaints regarding this policy or the handling of personal information should be directed to:

Chief Executive Officer
Family Planning Queensland
Postal address: PO Box 215, Fortitude Valley<Qld 4006
Street address: 100 Alfred street, Fortitude Valley, Qld, 4006
Email: ceo@fpq.com.au
Tel: 07 3250 0240

6. Supporting Documents

Privacy Procedure – Clinics
Privacy Procedure – Education and Administration

7. References

Australian Privacy Principles (APP) guidelines (Privacy Act 1988).
Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cwlth)
APP fact sheets

7.1 Further information on privacy

You can obtain further general information about your privacy rights and privacy law from the Office of the Australian Information Commissioner by:

- calling their Privacy Hotline on 1300 363 992
- visiting their web site at http://www.oaic.gov.au/ (External link)
- writing to:

  The Australian Information Commissioner
8. **Accountability and Responsibility**

Chief Executive Officer

- **Policy Owner:** Accountable for implementation, compliance with and maintaining the level of performance of this policy.

Executive Support Coordinator

- **Policy Custodian:** Overarching responsibility for the policy ensuring it is implemented, monitored, reported against and reviewed.

FPQ Managers and Employees

- **Policy Implementation:** Adopt, action and comply with Policy

9. **Policy Review**

This policy will be reviewed regularly following organisational or legislative changes or, as a minimum, every (3) years.

10. **Authorisation**

   **Name:** Alice Evans

   **Role:** CEO

   **Date:** 18th June 2014

11. **History of this Policy**

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Approval Date:</th>
<th>Authorised By:</th>
<th>Sections Modified and Summary of Changes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>Release</td>
</tr>
<tr>
<td>2</td>
<td>18/9/2011</td>
<td>CEO</td>
<td>Review</td>
</tr>
<tr>
<td>3</td>
<td>18/9/2013</td>
<td>CEO</td>
<td>Review</td>
</tr>
<tr>
<td>4</td>
<td>18/6/2014</td>
<td>CEO</td>
<td>Major review in accordance with amendment to Privacy Act. Policy updated.</td>
</tr>
</tbody>
</table>

| 5           |                |                |                                          |