

6.1 Privacy and Security of Personal Health Information

Policy

This practice is bound by the Commonwealth Privacy Act 1998 and Privacy Amendment (Private Sector) Act 2000 and also complies with relevant Western Australian laws. These include include:

- [Freedom of Information Act 1992](#)
- [Health Services \(Conciliation and Review\) Act 1995](#)
- [State Records Act 2000](#)

‘Personal health information’ means health information which either specifically identifies the individual or from which their identity can reasonably be ascertained.

The maintenance of privacy requires that any information regarding individual patients, including staff members who may be patients, may not be disclosed either verbally, in writing, in electronic form, by copying either at the FGPN office, on the FSD van or outside it, during or outside work hours, except for strictly authorised use within the patient care context or as legally directed.

All patient information must be considered private and confidential, even that which is seen or heard and therefore is not to be disclosed to family, friends, staff or others without the patient’s approval. Any information given to unauthorised personnel will result in disciplinary action and possible dismissal.

Each staff member is bound by his/her privacy clause contained within the employment agreement which is signed upon commencement of employment at FGPN. (Refer Section 2).

Security policies and procedures for patient information are documented.

All information received in the course of a consultation between a doctor and the patient is considered personal health information. This information includes medical details, family information, address, employment and other demographic data obtained via the New Patient Form. Medical information can include past medical and social history, current health issues and future medical care. It includes the formal medical record whether written or electronic and information held or recorded on any other medium e.g. letter, fax, or electronically.

Doctors, allied health practitioners and all other staff and contractors associated with FGPN have a responsibility to maintain the privacy of personal health information and related financial information. The privacy of this information is every patient’s right.

The physical medical records (electronic) and related information created and maintained for the continuing management of each patient are the property of this organisation. The organisation ensures the protection of all information contained therein. This information is deemed a personal health record and while the patient does not have ownership of the record he/she has the right to access under the provisions of the Commonwealth Privacy Act. Requests for access to the medical record will be acted upon only if received in written format.

RACGP 3rd Edition Std 4.2.1

Procedure

Personal health information should be kept where staff supervision is easily provided and kept out of view and access by the public e.g. not left exposed on the desk, in waiting area or other public areas.

Care should be taken that the general public cannot see or access computer screens that display information about other individuals. To minimise this risk screen filters are used.

Doctor, nurse and other staff should be aware that conversations in the main van area can often be overheard outside and as such staff should take care discussing confidential and sensitive patient information. Whenever sensitive documentation is discarded the organisation uses an appropriate method of destruction.

Correspondence

Electronic information is transmitted over the public network in an encrypted format using secure messaging software. Where medical information is sent by post the use of secure postage or a courier service is determined on a case by case basis.

Incoming patient correspondence and diagnostic results are opened by a designated staff member. (Coordinator or delegate)

Items for collection or postage are left in a secure area not in view of the public.

Facsimile

Facsimile, printers and other electronic communication devices in the practice are located in areas that are only accessible to the general practitioners and other authorised staff. Faxing is point to point and will therefore usually only be transmitted to one location.

All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver.

- Write, "Confidential" on the fax coversheet.
- Check the number dialled before pressing 'SEND'

- Keep the transmission report produced by the fax as evidence that the fax was sent.
- Also confirm the correct fax number on the report.

Faxes received are managed according to incoming correspondence protocols (Refer Section 6).

The organisation uses a fax disclaimer notice on outgoing faxes.

Fremantle GP Network Ltd

*10 Silas Street, East Fremantle WA 6158 | PO Box 4186, Myaree Business Centre, WA, 6960
Ph: (08) 9319 0555 | Fax: (08) 9339 8355 | Email: reception@fremantlegpnetwork.com.au*

NOTICE - This fax and any files transmitted with it are confidential and are only for the use of the person to whom they are addressed. If you are not the intended recipient you have received this fax in error. Any use, dissemination, forwarding, printing, copying or dealing in any way whatsoever with this fax is strictly prohibited. If you have received this fax in error, please inform us, then destroy any printed copy. This document is UNCONTROLLED when printed

RACGP 3rd Edition Std 4.2.1&4.2.2& 4.2.

Emails

Patient information may only be sent via email if it is securely encrypted according to industry and best practice standards.

PROCEDURE FOR SENDING SECURE EMAIL

FGPN Staff can send secure email to anyone with an email address

Sender Step 1 (recommended)

Send a standard e-mail advising recipient that you will be sending a secure message and that they should follow the instructions contained in this e-mail

Sender Step 2

Send a secure e-mail by adding the keyword '**Encrypt**' to the subject line. Eg. **Encrypt**message from Alison

Recipient Step 1

Encrypted email is received in a sealed envelope

Recipient Step 2

Recipient follows email instructions to register their identity (first time only)

Recipient Step 3

Recipient uses previously created login details to authenticate to view and reply to secure message via their web browser

11/17/2008

Paper Based documents/correspondence

Paper based documents and correspondence are scanned on the patient computerised medical record. Paper based documents are kept for 3 months in a locked cabinet. These documents are only retrieved by authorised staff. All paper based documents are securely destroyed after 3 months.

Documents are not left in public or unauthorised areas of the FSD van or office.

RACGP 3rd Edition Std 4.2.1& 4.2.2

Computerised Records

The organisation has systems in place to protect the privacy, security, quality and integrity of the personal health information held electronically. Appropriate staff are trained in computer security policies and procedures.

There is a staff member designated with the responsibility for overseeing the maintenance of the FGPN computer security and adheres to protocols as outlined in the IT Policy and Procedure Guidelines.

Refer to Section 5 Practice Administration

6.2 3rd Party Requests for Access to Medical Records/Health Information

Policy

Requests for 3rd Party access to a medical record should be initiated by either receipt of correspondence from a solicitor or government agency or by the patient completing a Patient Request for Personal Health Information Form. Where a Patient Request Form and signed authorisation is not obtained, the organisation is not legally obliged to release information.

Where requests for access are refused, the patient may seek access under relevant privacy laws.

An organisation 'holds' health information if it is in their possession or control. If the organisation has received reports or other health information from another organisation such as a medical specialist, it is required to provide access in the same manner as for the records it creates. If the specialist has written 'not to be disclosed to a third party' or 'confidential' on their report, this has no legal affect in relation to requests for access. The organisation is also required to provide access to records which have been transferred from another health service provider.

Requests for access to the medical record may be received from various 3rd Parties including:

1. Subpoena/court order/coroner/search warrant
2. Relatives/Friends
3. External doctors & Health Care Institutions

4. Police /Solicitors
5. Health Insurance companies/Workers Compensation/Social Welfare agencies
6. Employers
7. Government Agencies
8. Accounts/Debt Collection
9. Students (Medical& Nursing)
10. Research /Quality Assurance Programs
11. Media
12. International
13. Disease registers
14. Telephone Calls

Requests from patients under the Privacy Legislation is discussed in 6.3

Procedure

As a rule, no patient information is to be released to a 3rd Party unless the request is made in writing and provides evidence of a signed authority to release the requested information, to either the patient directly or a third party.

Written requests should be noted in the patient's medical record. Requests should be forwarded to the designated person within the organisation for follow-up.

Requested records are to be reviewed by the treating medical practitioner or principal doctor prior to their release to a third party.

The organisation retains a record of all requests for access to medical information including transfers to other medical practitioners.

Where hard copy medical records are sent to patients or 3rd Parties copies are forwarded not original documentation wherever possible. If originals are required copies are made in case of loss.

Security of any health information requested is maintained when transferring requested records.

6.2.1 Subpoena, Court Order, Coroner Search Warrant

Note the date of court case and date request received in the medical record. Whether a physical or electronic copy of the record is required,

follow the procedure outlined above. Refer also to section 8.1.5 “Management of Potential Medical Defence Claims”.

On occasions, a member of staff is required to accompany the medical record to court or alternatively a secure courier service may be adequate. If the original is to be transported, ensure a copy is made in case of loss of the original during transport. Ensure that the record is returned after review by the court.

RACGP 3rd Edition Std 4.2.1

6.2.2 Relatives/Friends

A patient may authorise another person to be given access if they have signed authorisation from the patient. See 6.3 Patient Requests for Personal Health Information. See also NPP2 Use & Disclosure.

Individual records are advised for all family members, but especially for children whose parents have separated, and care must be taken that sensitive demographic information relating to either partner is not recorded anywhere other than in the patient record in Medical Director. Significant court orders relating to custody and guardianship should be recorded as an alert on the children’s records.

RACGP 3rd Edition Std 4.2.1

6.2.3 External Doctors & Health Care Institutions

Direct query to patient’s doctor and or the practice coordinator.

RACGP 3rd Edition Std 4.2.1

6.2.4 Police/ Solicitors

Police and solicitors must obtain a case specific signed patient consent (or subpoena, court order or search warrant) for release of information. The request is directed to the doctor.

RACGP 3rd Edition Std 4.2.1

6.2.5 Health Insurance Companies /Workers Compensation/ Social Welfare Agencies

Release of information and completion of related treating doctor's reports is an issue between the patient and the doctor.

RACGP 3rd Edition Std 4.2.1

6.2.6 Employers

If the patient has signed consent to release information for a pre-employment questionnaire or similar report then direct the request to the treating doctor.

RACGP 3rd Edition Std 4.2.1

6.2.7 Government Agencies

Medicare Australia/Department of Veterans Affairs

Depending on the specific circumstances information may be need to be provided. It is recommended that doctors discuss such issues with the relevant medical defence organisation.

State Registrar of Births, Deaths & Marriages

Death certificates are usually issued by the treating doctor.

Centrelink

There are a large number of Centrelink forms (treating doctor's reports) which are usually completed in conjunction with the patient consultation.

RACGP 3rd Edition Std 4.2.1

6.2.8 Accounts/ Debt Collection

The Freo StreetDoctor does not charge any patients.

RACGP 3rd Edition Std 4.2.1

6.2.9 Students (Medical & Nursing)

The organisation does participate in medical/nursing student education. The organisation acknowledges that some patients may not wish to have their personal health information accessed for educational purposes. Patients are always advised of any impending student involvement in the organisation's activities and seeks to obtain patient consent accordingly. The organisation respects the patient's right to privacy.

RACGP 3rd Edition Std 4.2.1

6.2.10 Researchers/Quality Assurance Programs

Where the organisation seeks to participate in human research activities and/or continuous quality improvement (CQI) activities, patient anonymity will be protected. The organisation will also seek and retain a copy of patient consent to any specific data collection for research purposes.

Research requests are to be approved by the CEO and must have approval from a Human Research Ethics Committee (HREC) constituted under the NH&MRC guidelines. A copy of this approval will be retained by the organisation.

Accreditation is a recognised peer review process and the reviewing of medical records for accreditation purposes has been deemed as a "secondary purpose" by the Office of the Federal Privacy Commissioner. As a consequence, patients are not required to provide consent.

RACGP 3rd Edition Std 4.2.1& 4.2.3

6.2.11 Media

All enquiries should be directed to the CEO. Staff must not release any information unless it has been authorised by the CEO and patient consent has been obtained.

RACGP 3rd Edition Std 4.2.1& 4.2.3

6.2.12 International

Where patient consent is provided then information may be sent overseas however the practice is under no obligation to supply any patient information upon receipt of an international subpoena.

RACGP 3rd Edition Std 4.2.1& 4.2.3
NPP9 Transborder Data Flows

6.2.13 Disease Registers

This practice submits patient data to various disease specific registers (cervical, breast, bowel screening etc) to assist with preventative health management.

Consent is required from the patient on an opt in or opt out basis and patients are advised of this in the FSD information leaflet.

RACGP 3rd Edition Std 1.3.1, 4.2.1 & 4.2.3

6.2.14 Telephone Calls

Requests for patient information are to be treated with care and no information is to be given out without adherence to the following procedure:

Note the telephone number, name (and address) of the caller and forward this onto the treating doctor/principal or Coordinator where appropriate.

RACGP 3rd Edition Std 4.2.1

6.3 Patient's Request for Access to Personal Health Information Under the Privacy Legislation

Policy

Patients of the organisation have the right to access their personal health information (medical record) under legislation. The Commonwealth Privacy Act 1998, Private Act Amendment 2000 and Health Privacy Principle 6 (HPP 6). This principle obliges health service providers and other organisations who hold health information about a person, to give them access to their health information on request, subject to certain exceptions and the payment of fees (if any).

Public sector organisations continue to be subject to the *Freedom of Information Act 1982*.

The organisation complies with both laws and the National and Health Privacy Principles (*NPPs & HPPs*) adopted therein. See summary headings of Principles in this section. Both Acts give individuals the right to know what information a private sector organisation holds about them, the right to access this information and to also make corrections if they consider data is incorrect..

NATIONAL PRIVACY PRINCIPLES:



- NPP 1: *Collection of personal information by an organisation.*
- NPP 2: *How an organisation may use and disclose personal information in its possession.*
- NPP 3: *Relates to the quality of the data held by an organisation.*
- NPP 4: *Organisation must take reasonable steps to make sure the personal information it holds is secure*
- NPP 5: *Requires an organisation to be open about what personal information it holds and its policy on the management of personal information.*
- NPP 6: *Relates to access and correction of personal information held by an organisation about an individual, by that individual.*
- NPP 7: *The use of identifiers assigned by a Commonwealth Agency*
- NPP 8: *Individuals have the option of not identifying themselves when entering transactions with organisations*
- NPP 9: *Regulates the transfer of personal information held by an organisation in Australia*
- NPP10: *Limits on when an organisation is permitted to collect sensitive information*

As adopted within Commonwealth Privacy Amendment (Private Sector) Act 2000

We have a privacy policy in place that sets out how to manage health information and the steps an individual must take to obtain access to their health information. This includes the different forms of access and the applicable time frames and fees.

Reports by Specialists

This information forms part of the patient's medical record, hence access is permitted under privacy law.

Diagnostic Results

This information forms part of the patient's medical record, hence access is permitted under privacy law.

Note: Amendments to the Privacy Act apply to information collected after 21st December 2001, however they also apply to data collected prior to this date provided it is still in use and readily accessible.

We respect an individual's privacy and allow access to information via personal viewing in a secure private area. The patient may take notes of the content of their record or may be given a photocopy of the requested information. A GP may explain the contents of the record to the patient if required. An administrative charge may be applied, at the GPs discretion and in consultation with the Privacy Officer, e.g. for photocopying the record, X-rays and for staff time involved in processing request.

Procedure

A notice is displayed in our waiting room and on our web site advising patients and others of their rights of access and of our commitment to



privacy legislation compliance. An information brochure is also available that provides further details if required.

Release of information is an issue between the patient and the doctor. Information will only be released according to privacy laws and at doctor's discretion. Requested records are reviewed by the medical practitioner prior to their release and written authorisation is obtained.

Request Received

When patients request access to their medical record and related personal information held at the organisation, each request is documented and the organisation endeavours to assist patients in granting access where possible and according to the privacy legislation. Exemptions to access will be noted and each patient or legally nominated representative will have their identification checked prior to access being granted.

A patient may make a request verbally at FSD, via telephone or in writing e.g. fax, email or letter. No reason is required to be given. The request is referred to the patient's doctor or delegated Privacy Officer.

A Request for Personal Health Information form is completed to ensure correct processing.

Once completed, the form is scanned into the patient record.

Request by another (not patient)

An individual may authorise another person to be given access, if they have the right e.g. legal guardian, and if they have a signed authority. Under NPP 2 Use and Disclosure, a 'person responsible' for the patient (including a partner, family member, care, guardian or close friend), if the patient is incapable of giving or communicating consent, may apply for and be given access for appropriate care and treatment or for compassionate reasons. Identity validation applies.

The Privacy Act defines a 'person responsible' as a parent of the individual, a child or sibling of the individual, who is at least 18 years old, a spouse or de facto spouse, a relative (at least 18 years old) and a member of the household, a guardian or a person exercising an enduring power of attorney granted by the individual that can be exercised for that person's health, a person who has an intimate relationship with the individual or a person nominated by the individual in case of emergency.

Children

Where a young person is capable of making their own decisions regarding their privacy, they should be allowed to do so according to Federal Privacy Commissioner's Privacy Guidelines. The doctor could discuss the child's record with their parent. Each case is dealt with subject to the individual's

circumstances. A parent will not necessarily have the right to their child's information.

Deceased Persons

No mention is made of deceased patient's access in Commonwealth Privacy Legislation.

More current fact sheets can also be downloaded from <http://www.privacy.gov.au/publications/index.html#>

Contact the Office of The Information Commissioner of Western Australia info@foi.wa.gov.au

Collate & Assess Information

Arrange for the treating doctor or coordinator to access the computer record. Refer to the patient request form to help identify what information is to be given to the patient.

Data may be withheld under Privacy Legislation NPP6 Access & Correction for the following reasons.

- Where access would pose a serious threat to the life or health of any individual
- Where the privacy of others may be affected
- If a request is frivolous or vexatious
- If information relates to existing or anticipated legal proceedings
- If access would prejudice negotiations with the individual
- If access would be unlawful
- Where denying access is required or authorised by law

See National Privacy Principles in full for comprehensive list of exclusions <http://www.privacy.gov.au/>.

Access Denied

Reasons for denied access must be given to the patient in writing. Note these on request form. In some cases refusal of access may be in part or full.

Use of Intermediary When Access Denied

If a request for access is denied an intermediary may operate as facilitator to provide sufficient access to meet the needs of both the patient and the doctor.

Provide Access



Personal health information may be accessed in the following ways:

- View and inspect information
- View, inspect and talk through contents with the doctor
- Take notes
- Obtain a copy (can be photocopy or electronic printout from computer)
- Listen to audio tape or view video
- Information may be faxed to patient

Check Identity of Patient

- Ensure a visible form of ID is presented by the person seeking access. E.g. driver's licence, passport, other photo identification. Note details on request form.
- Does the person have the authority to gain access? Check age, legal guardian documents; is person authorised representative?

If the patient is viewing the data, supervise each viewing so that patient is not disturbed and no data goes missing.

If a copy is to be given to the patient ensure all pages are checked and this is noted in the request form.

If the doctor is to explain the contents to a patient then ensure an appointment time is made.

Requests to Correct Information

A patient may ask to have their personal health information amended if he/she considers that is not up to date, accurate and complete. (NPP 6.5 and 6.6)

The organisation must try to correct this information. Corrections are attached to the original health record.

Where there is a disagreement about whether the information is indeed correct, the organisation attaches a statement to the original record outlining the patients' claims.

Time Frames

Acknowledge request - within 14 days. Complete the request - within 30 days

RACGP 3rd Edition Std 4.2.1

6.3.1 Privacy Officer

Policy

The Coordinator the FSD Privacy Officer who implements and monitors adherence to all Privacy Legislation in relation to FSD business.

The FSD Coordinator acts, on behalf of FGPN, as the FSD liaison for all privacy issues and patient requests for access to their personal health information.

If staff have any queries concerning privacy law i.e. Commonwealth Privacy Act 1998 and Privacy Amendment (Private Sector) Act 2000 then refer to the FGPN Quality Officer.

RACGP 3rd Edition Std 4.2.1

6.3.2 Privacy Audit

Policy

From time to time or in the event of any issues or complaints relating to privacy matters, the organisation conducts a review of privacy policies and procedures.

Procedure

The Quality Officer reviews the following items:

- What is the primary purpose of the organisation?
- What data do we collect and document? NPP1
- How do we store this information? NPP5
- What data do we disclose and to whom? NPP2
- When and how do we obtain patient's consent? NPP2

Information is collected from hard copy and electronic storage devices and issues discussed with GPs and staff to gain the most current information.

National and State privacy laws are referenced with any updates being noted and acted upon.

6.4 Medical Records Administration Systems



The organisation uses Medical Director and Pracsoft for the storage and management of patient health information.

6.4.1 Creating a New Medical Record

Once patient name, address, date of birth and related demographic details are received, the nurse enters this information into the patient record.

RACGP 3rd Edition Std 4.2.1& 4.2.2

6.4.2 Retrieving a Medical Record for a Current Patient

Computerised patient records are only accessed by authorised doctors and staff via secure login/password.

RACGP 3rd Edition Std 4.2.1

6.4.3 Filing Reports (Pathology, X-Ray, Consultant's etc)

Paper based diagnostic test results and other incoming patient correspondence must be dated and passed on to the patient's treating doctor. If the report has not been ALSO delivered electronically, the paper copy should be given to the Duty Doctor for his/her attention, before filing it into the treating doctors file.

Once the treating doctor has seen/actioned the report, it should be initialled and dated then left to be scanned into the client record.

The organisation scans all patient paper based correspondence with copies of this data securely stored for 3 months following scanning.

Original copies are shredded after 3 months.

If results are received electronically, they are to be checked by the duty doctor daily, and the appropriate action box marked. The ordering doctor will review the result at the next opportunity, review any recommendations and modify such as appropriate.

RACGP 3rd Edition Std 4.2.1

6.4.4 Errors in Medical Record



Corrections in the electronic record should be recorded by referring to the date of the original entry and the associated amendment.

Refer to NPP6/HPP6 Access & Correction, which refers to the patients right's to have their personal health information amended if he/she can establish that it is not accurate, complete, misleading or up to date.

RACGP 3rd Edition Std 4.2.1& 4.2.2

6.4.5 Allergies and Alerts

Alert notification may be required for allergic responses, drug reactions, previous aggressive behaviour or guardianship/custody arrangements.

It is organisational policy to ensure that all patients have their allergic status recorded.

Alert notifications are documented in the electronic medical record.

Patients with no known allergies have an alternative to the default message inserted.

RACGP 3rd Edition Std 4.2.1

6.4.6 Back Up of electronic medical records

In order to avoid lengthy down time, disruption, and medico-legal issues frequent backups are essential and form a critical component of the practice disaster recovery plan.

Refer the organisation's IT policy and procedure guidelines and the computer security procedure in Section 5. Backups are performed routinely as part of the normal operation of the clinic with the Coordinator responsible for checking and maintaining the backup procedures. Backups are stored off site.

FGPN has an Information Disaster Recovery Plan in case of emergencies such as power failures and natural disasters which will protect and save the information on computers.

RACGP 3rd Edition Std 4.2.2

6.4.7 Retention of Records and Archiving

Patient Health Records must be kept until the patient is 25 years of age, if a child, or a minimum of 7 years following the last year of the patients attendance, whichever is greater.

This organisation retains electronic records indefinitely.

Records of deceased patients are kept indefinitely.

RACGP 3rd Edition Std 4.2.4

6.4.8 Transfer of Medical Records

Transfer of medical records from the organisation can occur in the following instances:

- For medico-legal reasons e.g. record is subpoenaed to court.
- When a patient asks for their medical record to be transferred to another practice, due to moving residence or for other reasons.
- Where an individual medical record report is requested from another source.

Procedure

Receiving a request

In accordance with state and federal privacy regulations, it is the policy of this organisation not to transfer medical records unless a signed request form is received from the patient requesting the transfer. The request form should contain the name of the receiving practitioner or practice, and clearly identify by name, address and date of birth the patient whose record is required.

When fulfilling a request, the normal response of the organisation is to prepare a summary letter (manually or via clinical software) and include copies of relevant correspondence and results pertinent to the ongoing management of the patient. It should be noted in the history who the summary has been sent to, who authorised the transfer and when. The original records should always be retained for medico-legal purposes.

Note: There are a number of ways the information can be transferred, depending on the request from the patient and clinic: via secure post; encrypted email (if computerised records), or, if the organisation is releasing copies of the entire record and the patient requests access, the Coordinator or doctor may wish to make an appointment time with the patient to offer an appropriate explanation.

Making a request



When requesting records from another clinic, the patient should be identified by name, address (both current and former if applicable) and date of birth with the request being from a named doctor of the practice and confirmed by the patient's signature.

Make a copy of the medical record and the patients' signed request letter/form and dispatch the copy to the new practice, retaining the original on site for a minimum of 7 years. Note on the first page of the medical record that the patient has transferred. Include the name and address of the new practice and the dispatch details (eg via priority mail or confidential courier or in an electronic form).

RACGP 3rd Edition Std 4.2.1& 4.2.3