

1.1 Privacy Policy

In compliance with the *Privacy Act 1988*, this practice has prepared this privacy policy to describe the way and circumstances under which personal information is collected, stored, used and disclosed and also how complaints are handled by this practice.

The related policy and procedure has been recorded underneath the National Privacy Principle for easy reference. The policy is intended as a guide to staff and patients of this practice and for the advice of the broader community.

For the purposes of this policy, no distinction has been made between the handling of personal information and sensitive information (including health information); therefore all information will be referred to as "personal information" throughout this policy.

1.2 APP 1 – Collection

Collection of personal information must be fair, lawful and not intrusive. A person must be told the organisation's name, the purpose of collection, that the person can get access to their personal information and what happens if the person does not give the information.

Policy

- This practice will only collect personal information necessary to provide our patients with a quality health service.
- Personal information about a patient will only be collected by lawful and fair means and directly from the patient wherever possible.
- If information is collected about a patient from another party, this practice, will whenever possible, advise the patient of this.
- Wherever practical this practice will only collect information directly from the patient. This may not be possible if the patient is unconscious or otherwise incapable of providing that information.
- We will ensure that each patient providing personal information is informed about and understands the purpose of collecting the information. They will also be advised as to whom or under what circumstances their personal information may be disclosed to another party and how they can access the information held about them by this practice. This will be carried out via notices and/or brochures and/or verbally.
- We will ensure that patients who are asked to provide personal information understand the consequences, if any, of providing incomplete or inaccurate information.

1.3 APP 2 – Use and Disclosure

An organisation should only use or disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.

Policy

- This practice will ensure that personal information will only be used for the purpose it was collected, or that would reasonably be expected by the patient providing the information.
- If the identified information is to be used for a secondary or unrelated purpose, such as data analysis or research, we will obtain informed consent from the patient.
 - > Individuals will be given the opportunity to refuse such use or disclosure.
 - > If a patient is physically or legally incapable of providing consent, a responsible person (as described under the Act) may do so.

- We will only disclose personal information without consent where such disclosure is required by law, or for law enforcement, or in the interests of the patient's or the public's health and safety.
 - > We will keep records of any such use and disclosure.
- Information may be disclosed to a responsible person (as described under the Act).

1.3.1 Notifiable Diseases

Policy

Under the *Public Health Act 2005*, medical practitioners are to report infectious diseases as specified. Notifications of cases are made to the Metro South Public Health Unit.

Procedure

It is the responsibility of the treating doctor or nominated person to notify the Metro South Public Health Unit of any communicable diseases.

1.3.2 Medical Students

Policy

Patients may not wish to have their personal health information used for education purposes. This practice respects its patient's right to privacy and where possible will use de-identified data for case studies. We will always inform patients of impending medical students participating in practice activities and ask patients to consent to this.

1.3.3 Research and Quality Program

Policy

Where it is desired to publish material related to clinical work or for practice continuous quality improvement activities, the anonymity of patients is to be preserved. Research requests are to be approved by the practice principal.

The patient must consent to any specific data collection for research purposes. If the data is required by or in accordance with rules established for accreditation by RACGP or other diligent professional health agencies, then data will be de-identified where possible, with related obligations of confidentiality upon health professionals engaging in these activities.

1.3.4 Disease Registers (For Public Health Purposes)

Policy

For cervical screening, CARDIAB, breast screen and other disease specific registers consent is required from the patient to use their personal health information for this purpose. The patient is given the opportunity to decline inclusion in these types of registers.

1.3.5 Subpoena, Court Order, Search Warrant and Coroner

Policy

Information will be released if a subpoena, court order, search warrant or coroner is received. If the doctor is concerned about confidentiality issues, he/she may decide to challenge it in court if sufficient evidence amounts to possible breach in confidentiality.

Procedure

1. Inform the patient's doctor and practice principal.
2. Retrieve the patient's medical record from the filing area.

3. Record the date of court case in the patient's medical record.
4. Make a copy of the record.
5. Retain the copy in file and mark as a duplicate on each page with reason for the copy noted inside.
6. Sometimes a staff member is required to take the medical record to court. Telephone the relevant solicitor or Clerk of courts and try to arrange a confidential courier to transport the record in, as an alternative.
7. Telephone closer to the day requested, if a staff member must take the record physically to court, to ensure the date is correct and the case is still on.
8. Return the record to the practice after the review by the court unless otherwise instructed by the court.

1.3.6 Relatives and Friends

Policy

No information is to be released unless the patient has authorised another person to be given access if they have the legal right and a signed authority.

Separate records are advised for all family members but especially for children whose parents have separated and care must be taken that sensitive demographic information about either partner is not recorded on the demographic component of the record.

1.3.7 Police and Lawyers

Policy

Police and lawyers must obtain a signed patient consent (or subpoena, court order or search warrant) for release of information. The request is directed to the doctor. Where only a signed patient request is obtained the doctor is not legally obliged to release information.

1.3.8 Insurance Company and Social Welfare Agency

Policy

No information to be given without express written consent from the patient. All enquires must be directed to the patient's doctor. Release of information is an issue between the patient and the doctor.

1.3.9 Employers

Policy

If the patient has signed consent to release information for a pre-employment questionnaire or similar report then direct the request to the doctor who will respond with the required information. Otherwise no information is to be released. When in doubt always refer the request to the doctor. Patient may seek access via privacy law.

1.3.10 Emergencies

Policy

Where immediate treatment is necessary to preserve a life or prevent serious injury, all attempts are made to gain the patient's consent. This may not be successful in all cases prior to administering emergency care.

1.3.11 Informed Consent

Policy

Our doctors inform their patients of the purpose, benefit and risks of proposed treatment or investigations. We believe that patients need to receive sufficient information to allow them to make informed decisions about their care.

Information is clear and given in a form that is easy to understand, whether it be verbally, in a diagram with explanation, brochure, other handout/leaflet or poster.

Doctors take into consideration the patient's ethnicity and principal language spoken. Steps are taken to ensure an interpreter is utilised where necessary and at the patient's request. Issues of personality, personal fears and expectations, beliefs and values are also considered.

There is no coercion by our doctors. Our patients can choose to reject their doctor's advice or seek a second opinion. Doctors also inform patients of potential additional costs and out of pocket expenses for treatments and investigations, prior to them being carried out, whether they would be done on site or referred to medical specialists.

Patients are asked to be open and should be able to feel free to discuss all health issues and proposed treatments, without the fear of reprisals.

Patient consent is obtained for the following:

- Minor operative procedures on-site (verbal consent)
- Third party observation or participation in patient consultation (verbal consent)

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 states that consent may be 'express' or 'implied'.

- Express Consent – clear and unmistakably states, obtained in writing, orally or in any clear other form where consent is clearly communicated.
- Implied Consent – e.g. patient presents to doctor, discloses health information and this is written down by the doctor/entered on computer during the consultation; eg. doctor collects specimen and sends it to pathology, reason to consider that the patient is giving implied consent to passing necessary information to the laboratory.

1.4 APP 3 – Data Quality

An organisation must take reasonable steps to make sure that the personal information it collects uses or discloses is accurate, complete and up-to-date.

Policy

This practice will take reasonable steps to ensure that personal information kept, used or disclosed by the practice is accurate, complete, and as up to date as practicable.

Medical records are confidential legal documents. Doctors and staff have a responsibility to maintain the privacy of every medical record, which is each patient's right. As a key component for the continuing management of our patients, accurate and complete records are kept.

Each patient has an individual medical record incorporating a health summary, progress notes, referrals made and responses received including pathology, x-ray; documentation of telephone calls, home visits, after hours communication and all hospital visits made.

Doctors, practice nurses, allied health practitioners and authorised students of this practice are responsible for documenting their own notations for care given to their patients. For each consultation the doctor notes the following details in the medical record:

- Doctor's name

- Date
- Reason for consultation
- Other problems managed
- Management plan
- Planned dates for review
- Medications prescribed with route, frequency, other directions for use and number of repeats
- Preventative care
- Referrals to other health care practitioners
- Consent issues

Appropriately filed pathology, x-ray and related referrals and results are in the medical record.

All entries are dated and initialled or signed. Information in the medical record is not prejudicial, derogatory nor irrelevant and is legible being able to be read by other health care practitioners for the ongoing management of the patient.

Referrals to other health care providers contain sufficient information for continuing health management with signature, designation and date. A copy remains in the medical record.

Patients who attend our practice on a regular basis have a health summary included in their medical record. The record also contains family and social history, past and active problems, allergies and sensitivities, medication, immunisation status and any risk factors present.

A note is recorded in the patient information sheet and a poster is in the waiting room recommending that patient's advise reception if their personal details need to be updated.

1.5 APP 4 – Data Security

Policy

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access modification or disclosure.

- All personal information held by this practice will be:
 - > If in paper form, received and stored in a secure, lockable location;
 - > If in electronic form, protected from theft, loss or corruption;
 - > Accessible by staff only on a "need to know" basis;
 - > Protected from viewing or access by unauthorised persons; and
 - > Not taken from this practice offices unless authorised and for a specified purpose.
- We will destroy or permanently de-identify personal information that is no longer required by this practice.
- We will ensure that all personal information transmitted electronically will be appropriately encrypted before transmission.

Procedure

The following guidelines are followed for maintaining security:

- Practice records are to be maintained, handled and stored in a manner which will prevent:
 - > Loss
 - > Breaches of confidentiality
 - > Unauthorised access
- Maintain Privacy/Confidentiality from others (e.g. patients, public and staff) under all circumstances including patient:

- > Address
- > Telephone number
- > Results
- Written/telephone requests – always follow the correct procedure.
- Ensure appropriate disposal of documents including patient files, accounts and business records.
- This practice maintains an accurate recording system to update and track files, especially changes of name or address. Correct disposal requirements must be observed.

Security is maintained for files at all times. During practice hours the file storage area is unlocked. At the end of the working day the Practice Manager, a doctor or delegated staff member locks the filing area.

1.5.1 Computer

Policy

It is the policy of this practice that data held on the practice's computer system is secured to prevent unauthorised access, exploitation and loss of data.

Staff members, temporary staff and contractors that require access to the practice's systems are required to sign confidentiality agreements before commencing work. Please refer to Section 10 – Confidentiality Agreements template.

Electronically held data will be protected from exploitation by organisations that may sell the data for commercial purposes. Disks, faxes and computer printouts are positioned or stored out of sight when not in use.

Computer equipment is located in physically secure areas within the practice or is secured by anti-theft and data loss protection devices (lockable cables, drive locks).

1.5.2 E-mail

Policy

Patient information is only sent via e-mail if it is securely encrypted according to industry and best practice standards. Refer to Section 5 – Computer Administration for more details.

1.5.3 Facsimile

Policy

The following procedure is to be strictly adhered to, due to the medico-legal nature of our patient information:

- When faxing patient information, the fax number and identification of the recipient must be confirmed before transmitting.
- Record "Confidential" on the fax coversheet.
- Check the number dialled before pressing 'SEND'.
- Keep transmission report produced by the fax as evidence that the fax was sent. Also confirm the correct fax number on the report.

1.6 APP 5 – Openness

An organisation must have a policy document outlining its information handling practices and make this available to anyone who asks.

Policy

- This practice is committed to advising patients about its information handling practices.
- This Privacy Policy will be made available to any person requesting it.
- A Privacy Statement describing our approach to privacy will be on public display.
- Brochures detailing this practice personal information handling practices will be provided to any person requesting access to it.

1.7 APP 6 – Access and Correction

Generally speaking, an organisation must give an individual access to personal information it holds about that individual on request.

Policy

- Under normal circumstances this practice will provide a patient with access to their personal information within 30 days of receiving a request for access.
- All requests are asked to be provided in writing through use of the Patient Request for Access to Personal Information form supplied. Identification is also requested to ensure that a false application is not lodged.
- There will be no fee associated with lodging a request for access, however, an administration fee may be charged as set out in the Request for Access application.
- Patients will be provided with an opportunity to discuss their personal information with an appropriate member of staff when access is sought, however a fee for the doctor's time may be charged.
- Provision of access to a patient's personal information will be undertaken in a way that is appropriate to the person's particular circumstances, e.g. use of interpreters, etc.
- If a patient believes that information held by this practice is inaccurate or incomplete, we will take steps to amend or correct the information.
- This practice may refuse access if it reasonably believes that:
 - > A person's health, safety or wellbeing may be compromised by releasing the information; or
 - > Providing access would be unlawful or would prejudice a legal investigation.
 - > Providing access would affect the privacy of others.
 - > The request for access is frivolous and/or vexatious.
 - > The information held in the patient's medical record would be used against the doctor in a medico-legal matter.
- Under circumstances other than those described above where information is withheld, this practice will ensure that its practices are consistent with the provisions of APP 6.
- If information is withheld under APP 6.4, this practice will provide an explanation to the patient as to the reasons why this was the case.

Procedure

Please refer to Section 10 – Privacy Request for Access Checklist for a suggested template on handling an information request.

1.7.1 Corrections in Medical Record

Policy

A patient may ask to have their personal health information amended if he/she considers that is not up to date, accurate and complete. Our practice will 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, our practice attaches a statement to the original record outlining the patients' claims.

It is the policy of this practice that identified errors are not permanently removed. It will be noted in the record that the information has been deemed incorrect, incomplete or not up-to-date, add changes to correct the information and initialled and dated by the author with an explanatory note beside or below the original item. Thus the reason for the incorrect entry is clearly documented with the new entry underneath or in the next available position. The new entry is signed or initialled and dated.

Procedure

If an error occurs in writing, within the medical record:

1. The error is to be crossed through the course of entry in a single line, initialled and dated, by the author.
2. Provide an explanatory note beside or below the original item.
3. New information is recorded, signed or initialled and dated.

1.8 APP 7 – Identifiers

Generally speaking an organisation must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government 'agency'.

Except where circumstances allow (APP 7.2), this practice will not use Medicare or Veterans Affairs numbers or other identifiers assigned by a Commonwealth or State/Territory agency to identify personal information.

1.9 APP 8 – Anonymity

Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do so.

Policy

Where it is lawful and practicable to do so, this practice will allow patients to provide information anonymously.

- A patient who chooses to access the services of this practice anonymously will be advised of any potential consequences resulting from their decision. For example where the lack of a contact name or address may jeopardise care in an emergency situation.
- We will not automatically preclude a patient from participating in the activities of this practice because they request anonymity.

1.10 APP 9 – Trans border Data Flows

An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.

Policy

This practice will only transfer personal information about a patient to someone who is in a foreign country if:

- The patient consents to the transfer; or
- The recipient is bound by legislation that is substantially similar to the APPs; or
- This practice is reasonably sure that the information will not be held, used or disclosed inconsistently with the APPs.

1.11 APP 10 – Sensitive Information

An organisation must not collect sensitive information unless the individual has consented, it is required by law – or in other special specified circumstances, for example, relating to health services provision and individual or public health or safety.

Policy

This practice will only collect sensitive information other than health information about a patient if:

- the patient consents; or
- the collection is required by law; or
- such collection is consistent with the provisions of APP 10.