



PRINTED COPIES ARE NOT CONTROLLED

Policy***Confidentiality and privacy of health and other information (C 6.3 A - D)***Accreditation link: [C 6.3 \(A - D\)](#)

All patient health information must be considered private and confidential, and therefore must not be disclosed to family, friends, staff or others without the patient's consent. This information includes medical details, family information, address, employment and other demographic and accounts data obtained via reception.

All practice team members are aware that any information given to unauthorised personnel will result in disciplinary action, possible dismissal and other legal consequences.

Informing patients on managing confidentiality and personal health information (C6.3 A)

Our practice has developed and implemented a privacy policy that details how we manage data, it includes data:

- collection
- use and disclosure
- quality and security
- correction
- access
- complaints
- overseas transfer

Patients, their family and carers can access our privacy policy via our website.

All members of the practice receive training in the significance and obligations of the Privacy Act and the Australian Privacy Principles, the importance of confidentiality and our privacy policy. Training records are stored in PracticeHub. It is the responsibility of the Practice Manager to ensure all training records are completed and current.

At the commencement of their employment/engagement the team member must sign a confidentiality agreement, the completed agreement is stored in their employment file in Practice Hub.

A template for the patient privacy policy can be found here [RACGP Privacy policy template](#)

A copy of our practice's privacy policy is attached to this page.

Informing patients how to access their health information (C6.3 B)

Patients of our practice are informed of their rights to access their personal health information in accordance with the Australian Privacy Principles (APP). This is done via the practice information sheet, notice in the waiting area, the practice website, and via an information brochure.

Prior to a patient signing consent to the release of their health information patients are made aware they can request a full copy of our privacy policy and collection statement.

Patient consent for the transfer of health information to other providers or agencies is obtained on the first visit. A copy of our consent form is attached.

Once signed this form is scanned into the patient's record and its completion noted. Note: Consent for transfer of information differs from procedural consent.

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.

Note: Specialist reports and diagnostic reports form a part of the patient's medical record, hence access is permitted under privacy law.

1. Request received (from a patient)

On request for access to personal health information, our practice documents each request and endeavours to assist patients in gaining access according to the Privacy Act and APP, we:

1. Document the patient's request using the Request for Personal Health Information form and forward a request to the patient's healthcare practitioner or delegated Privacy Officer to check for exemptions
 - A patient may make a request verbally at the practice, via telephone or in writing e.g. fax, email or letter - no reason is required to be given
2. Complete all steps to confirm identification of the patient or legally nominated representative prior to access being granted
3. Provide personal health information within period of time as outlined in the Privacy Act
4. Note any exemptions to access
5. Log a record of the request in the Access Register and file or scan the form into the patient's record.

Refer to **C6.3 A** above for practice member training and training record requirements.

2. Request by another (not a 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 & Disclosure, a 'person responsible' for the patient (including a partner, family member, care, guardian or close friend), if that 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 1998* 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

3. 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.

4. Deceased Persons

A request for access may be allowed for a deceased patient's legal representative if the patient has been deceased for 30 years or less and all other privacy law requirements have been met. Ref: Sec 28

Health Records Act. No mention is made of deceased patient's access in Commonwealth privacy legislation.

Responding to a request - specific steps

When a request is received, we refer to the steps below as a guide:

1. Acknowledge Request

- Each request is acknowledged with a letter sent to the patient, confirming request has been received.
- Send the letter within 14 days or sooner as recommended by the National Privacy Commissioner.
- Acknowledgement will include a statement concerning charges involved in processing the request.

2. Fees Charged

- Discuss with the individual what information they want access to, and the likely fees, before undertaking their request for access.
- The fees which an organisation can charge for providing access must not be excessive and must not apply to the mere lodgement of a request for access.
- National Privacy Principle (NPP) 6.4 aims to prevent organisations from using excessive charges to discourage individuals from making requests for access to their medical records.
- If an organisation incurs substantial costs in meeting a request for access, then the organisation could charge a reasonable fee to meet the administrative costs involved. For example, an organisation could recover some of the costs of photocopying or of the staff time involved.

3. Collate & Assess Information

- Retrieve patient's hardcopy medical record or arrange for the treating doctor or practice principal 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 the National Privacy Principles in full for comprehensive list of exclusions.*

4. 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.

5. Use of Intermediary When Access Denied

- If 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.

6. 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. 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.

7. 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 6.5/6/6)
- Our practice 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, our practice attaches a statement to the original record outlining the patients' claims.

8. Time Frames

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

Transferring patient health information (C6.3 C)

Receiving a request

To ensure timely, authorised, and secure transfer of patient health information we use secure messaging service encryption method. The patient may consent to their information being sent without such protection, this consent must be documented and recorded in the patient's medical record.

Confidential data is not to be sent via email or the internet.

Electronic transfer of a patient's health information cannot proceed unless requested by the patient. The patient's consent is documented in their health record in the form of a completed Request to Transfer Medical Records form.

The request form should contain:

- the name of the receiving practitioner or practice.
- the name, address (both current and former if applicable) and date of birth the patient whose record is required.
- the reason for the request.

When fulfilling a request, this practice may choose to either

- prepare a health summary printout (via clinical software) and include copies of relevant correspondence and results pertinent to the ongoing management of the patient.
- make a copy of the medical record and dispatch the copy to the new Practice, retaining the original on site for a minimum of 7 years.

The requesting clinic is advised if we propose to transfer a summary or a copy of the full medical record. If they have a preference the format can be negotiated or they can choose not to proceed with the transfer and seek a copy through a separate access request.

If there is going to be any expenses related to the transfer the requesting clinic is advised prior to sending the medical records and once the fee has been paid we process the request as soon as possible.

Any charges must not exceed the prescribed maximum fee.

The patients' signed request letter/form and a notation that the patient has transferred is made on the medical record. Include the name and address of the new Practice and the dispatch details (e.g. via priority mail or confidential courier or in an electronic form)/

Refer C6.3 A above, for practice member training and training record requirements.

The IT team is responsible for the maintenance of secure messaging software; troubleshoot and managing issues with the secure messaging software vendor. The Practice Manager is responsible for reviewing this use of secure messaging service, addressing any discrepancies identified, updating procedures as required and providing updates to all practice team members.

Our healthcare professionals send all health information using secure messaging.

Our practice has advised external healthcare professionals/organisations that the practice's method of transferring patient health information is using secure messaging. All secure messaging contact details on the Healthcare Provider Directory and Endpoint Location Service are accurate and up to date.

All reasonable steps are taken to protect the health information from loss and unauthorised disclosure during the transfer.

This practice does not allow individuals to collect the file and take it to their new provider.

Making a request

Access to a new patient's previous record can assist with maintaining the continuity of care of the patient.

When requesting records from another clinic a standard request for transfer of medical records template (see sample below) should be used.

This should contain:

- the patient's details, the patient should be identified by name address (both current and former if applicable) and date of birth.
- the reason for request including the name of the Doctor making the request.
- the request for transfer of patient files should be authorised by the patient.

If the files will be requested electronically, specific details of the format needs to be included such as HTML or XML

If the clinic advises you that the patients are likely incur out of pocket expenses related to transfer please advise the patient prior to accepting the transferred medical records

Authorised access to patient health records, prescription pads, and other official documents (C6.3 D)

Our practice has secure storage *electronic and/or physical* locations for all official documents, including prescription forms, administrative records, templates and letterhead.

Document	Location (<i>insert site information</i>)
official documents	electronic -, shared drive, clinical software, access-controlled area
prescription forms	clinical software, access-controlled area

administrative records	clinical software, access-controlled area
templates	clinical software, access-controlled area
letterhead	clinical software, access-controlled area

Protection against Theft of Information

There are significant risks if providing confidential information by email: only do so via secure internet sites with an https address, when the site displays a security lock in the status bar.

Caution must be exercised when entering into online purchasing arrangements. Online purchases normally involve the use of credit or charge cards, and all care should be exercised when using this method of payment over the Internet. It is imperative that only secure pages (i.e. https:) have sensitive data entered onto them.

Only staff who have been issued with a My GP Hub Corporate Credit Card for the purpose of purchasing of goods and/or services on-line are permitted to use said card.

Useful information:

[Australian Privacy Principles](#)

[Privacy basics and data breaches](#) (Avant Learning Centre)

[Providing medical records to a third party](#) (Avant Learning Centre)