Handbook for the management of health information in general practice
2nd edition
Acknowledgements

The Handbook for the management of health information in general practice has been produced by The Royal Australian College of General Practitioners (the RACGP).

This handbook is based on the 1st edition of the Handbook for the management of health information in private medical practice which was developed by the RACGP in conjunction with the Committee of Presidents of Medical Colleges (CPMC) and the General Practice Computing Group (GPCG) published in 2002.

The RACGP gratefully acknowledges the assistance provided by the National Standing Committee – General Practice Advocacy and Support, particularly Dr Genevieve Hopkins, also Dr Trish Williams (PhD) from Edith Cowan University and the Policy and Practice Support Unit of the RACGP, for managing the review process.
## Contents

**Definitions**  
1. *Health information*  
   - 1  
2. *Personal health information*  
   - 1  
3. *Confidentiality*  
   - 1  
4. *Privacy*  
   - 2  
5. *Sensitive information*  
   - 2  
6. *Practice*  
   - 2  
7. *De-identified health information*  
   - 2  

1. **Quality and content of medical records**  
   - 3  
2. **Patient consent**  
   - 4  
3. **Advising patients when collecting personal health information**  
   - 7  
4. **Patient access to medical records**  
   - 9  

- **1. Quality and content of medical records**  
  1.1 *Maintaining medical records*  
     - 3  
  1.2 *Accuracy and completeness of medical records*  
     - 3  

- **2. Patient consent**  
  2.1 *Consent may be implied or expressed*  
     - 4  
  2.2 *Patient can withhold consent*  
     - 4  
  2.3 *Group practices*  
     - 5  
  2.4 *Use of information must be relevant to consent*  
     - 5  
  2.5 *Use for training and education purposes*  
     - 5  
  2.6 *Competence to give consent*  
     - 5  
  2.7 *Assessing maturity to give consent*  
     - 6  
  2.8 *Family medical histories (including genetic information)*  
     - 6  

- **3. Advising patients when collecting personal health information**  
  3.1 *The importance of having a written policy*  
     - 7  
  3.2 *Considerations before sharing health information*  
     - 7  
  3.3 *Health information from third parties*  
     - 8  
  3.4 *Anonymity of patients*  
     - 8  

- **4. Patient access to medical records**  
  4.1 *Explanation of the medical record*  
     - 9  
  4.2 *Fees*  
     - 9  
  4.3 *Access of medical records via a third party*  
     - 10  
  4.4 *Amendments/annotation made to medical records*  
     - 10  
  4.5 *Correction of personal health information*  
     - 10  
  4.6 *Issues in withholding access*  
     - 10  
  4.7 *Forms of access*  
     - 11  
  4.8 *Processing a request*  
     - 11
**Definitions**

**Health information**

‘Health information’ is defined as a specific type of personal information. “This information includes personal information that is information or an opinion about the physical or mental health or a disability of an individual”.1

**Personal health information**

In this handbook, the expression ‘personal health information’ refers to:

- information about a patient or a third party obtained by a healthcare service provider from a patient or a third party in the course of providing a healthcare service, or
- an opinion formed by a healthcare service provider about a patient (whether true or not) which is in a form whereby the identity of the person is apparent, or can reasonably be ascertained.

This may include information about the person’s:

- name, address and contact details
- medical history
- Medicare number
- Individual Healthcare Identifier (IHI)
- social circumstances
- health services requested or provided
- expressed wishes about the future provision of health services
- genetic information in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Health information may be held in any form, including:

- paper
- electronic
- visual, eg. X-rays, CT scans, videos and photos
- audio recording.

**Confidentiality**

The Office of the Privacy Commissioner defines ‘confidentiality’ as ‘the general non-legal principle concerned with the obligation of people not to use private information – whether private because of its content or the context of its communication —for any purpose other than that for which it was given to them’.2

It is common for a patient to disclose information to their medical practitioner with the intention that the information will only be used for a health practitioner/patient relationship.
Privacy

In the context of this publication, the term ‘privacy’ relates to the management and protection of personal health information. The National Privacy Principles (NPPs), extracted from the Privacy Act 1988, provide guidance regarding the management of personal health information in the private sector.

The NPPs include:
1. collection
2. use and disclosure
3. data quality
4. data security
5. openness
6. access and correction
7. identifiers
8. anonymity
9. transborder data flows
10. sensitive information.

Sensitive information

The Privacy Act defines ‘sensitive information’ to mean information or an opinion about an individual’s:
- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual preferences or practices
- criminal record or
- health and genetic information.2

Practice

In this handbook the term ‘practice’ refers only to medical practices that operate as a single functional unit for the purposes of patient care, practice management and accreditation, and not to groupings of individual medical practitioners. The practice may operate under one of a range of different business structures, including a company, unit trust or partnership. The practice must have a single privacy policy, with one person within the practice who is responsible for overseeing the implementation and effective operation of the privacy policy and a single point of contact for privacy concerns.

De-identified health information

If health information is unable to be identified with the particular individual, it is no longer personal health information and the privacy concerns are less acute. It is important to acknowledge, however, that de-identified or not, the information should still have consent to be used for purposes other than for which it was originally collected, as well as being disclosed to third parties. Furthermore, it is still appropriate to inform the patient of the possible uses of the data and ensure that the patient has no objection to this use. This advice may be included in a practice policy manual on personal health information or in a practice information leaflet.
1. **Quality and content of medical records**

1.1 **Maintaining medical records**

Medical practitioners must take reasonable steps to ensure their medical records:

- are accurate, complete, well organised and legible
- are up-to-date, in that they reflect the personal health information most recently obtained about the patient concerned
- would allow another doctor to carry on the management of the patient
- do not contain prejudicial, derogatory or irrelevant statements about the patient
- incorporate health summaries in active patient medical records
- use a recall system, subject to patient consent, to provide systematic preventive care and early case detection using scientifically validated guidelines.

As the primary purpose of keeping medical records is to facilitate effective treatment of the patient, it is important that records be accurate and clear. The Privacy Act also requires medical practitioners to take reasonable steps to ensure that the personal health information they are the custodians of and use is accurate, complete and up-to-date.

1.2 **Accuracy and completeness of medical records**

Although medical practitioners may have differing styles of record keeping and may adopt their own abbreviations, the record should nonetheless be comprehensible to others. The medical record is also a tool to facilitate better patient care through the use of health summaries and a recall system.

Benefits in maintaining quality health information can include its reliability in supporting informed decisions about healthcare and treatment, and its role in facilitating the continuity of care when a new healthcare service provider becomes involved, whether temporarily or permanently. Risks relating to poor data integrity can include the misrepresentation of an individual’s health condition.

The medical practitioner should maintain a full, accurate and up-to-date health summary. Neither the summary nor the broader medical record should contain any derogatory, prejudicial or irrelevant statements about the patient.

Relevant NPPs:

1. Collection – subclause 1.1
3. Data quality
2. Patient consent

The consent of the patient must be provided voluntarily and should be the guiding principle for medical practitioners when obtaining personal health information from their patients, using that information, or disclosing the information to other people. Medical practitioners should respect the right of patients to determine how their personal health information is used or disclosed, and should ensure that patients are provided with sufficient information to enable them to fully exercise this right.

Medical practitioners must always ensure that patients agree to have their personal health information included in the medical record. Subject to certain very limited exceptions (refer to Section 5 – Using and disclosing personal health information), patients must consent to any proposed disclosure to third parties.

The consent of the patient is valid only if he or she understands fully how the information is to be used or disclosed. This section must therefore be read together with Section 3 – Advising patients when collecting personal health information.

2.1 Consent may be implied or expressed

In many medical practice contexts, the consent of patients to the recording or use of their personal health information can be implied from the fact that the patient is clearly aware of what the medical practitioner proposes to do with the information and does not indicate any objection. This could be the case, for example where information is entered into the notes in the presence of the patient and no objection is raised, or where the medical practitioner gives an open referral letter to the patient prior to the patient’s visit to a specialist.

Problems may arise, however, if the patients do not fully appreciate what is to happen with the information. Where patients are referred for a second opinion, for example, they may not realise that a summary of the relevant medical history is likely to be sent to another doctor. Medical practitioners should be careful not to assume implied consent too readily, and if there is any doubt as to whether patients consent to a particular use of their information, this should be clarified with them and expressed consent obtained.

As a general rule, it is likely that the consent requirements will be satisfied as long as the medical practitioner is open with patients about how their personal health information is to be used. It is important to ensure there are shared expectations between the medical practitioner and the patient about how personal health information will be used.

Consent by patients to the collection, use and disclosure of their personal health information can be either verbal or written. There is no legal requirement for consent to be in writing. Where particularly sensitive information is involved, including health information, medical practitioners are recommended to make a notation in the medical record confirming that the patient has consented.

2.2 Patient can withhold consent

Some patients may refuse to provide certain personal health information or may withhold consent for particular uses of that information. Medical practitioners must respect their right to do so. Where there is a concern that the patient may suffer detriment if certain information is not collected or used, this should be explained to the patient.

In situations where patients decide to withhold consent, it is recommended that there is a suitable and computer-actionable field in the patient’s notes to record the patient’s particular decision.
2.3 Group practices

In group practices, there is frequently an assumption that all doctors in the practice have access to the records of all patients. This may not accord with what certain patients understand or wish, and is a matter that may need to be explained to patients to ensure they have no objection.

2.4 Use of information must be relevant to consent

Even where the patient has consented to the disclosure of his or her personal health information for a particular purpose, only information relevant for that purpose should be disclosed. For example, a patient who authorises a medical practitioner to send a referral letter or report to another medical practitioner does not necessarily consent to having the whole medical record made available to that medical practitioner. The disclosure should be limited to the information relevant to the referral.

2.5 Use for training and education purposes

The use of personal health information for teaching purposes raises particular privacy concerns. Patients are often not aware that their health information may also be used to assist in teaching. Wherever possible, personal health information should be de-identified before it is used for teaching purposes. Where this is not possible, the doctor must be certain that the patient understands and agrees to this use.

It is important for healthcare service providers to be able to train in ‘real life’ environments. Training and education, in some cases, may be as effective by using de-identified case studies, or in the case of IT training through using simulated data. If a healthcare service provider uses de-identified information for training, consent is not required.

Where the use of health information is necessary for training purposes, the sensitivity of such information needs recognition as some individuals seeking healthcare may not want their information disclosed any more widely than is necessary to receive care. These individuals may not want their information used for training or education activities. The use of information for training and education will therefore usually require the individual’s consent.

Whether consent is needed may depend on the nature of the training activity and the expectations and wishes of the individuals involved. Intrusive training activities, or those less closely linked with service provision, are more likely to require express consent. For instance, videotaping a family therapy session, when the identities of participants will be revealed, is highly likely to require expressed consent.

Where consent is sought, the individual should have a genuine choice and not be pressured to participate. The individual should be told about the specific nature of the activity and the student group involved.

2.6 Competence to give consent

There are some patients who, because of illness or disability, are not competent to give consent for the collection, use or disclosure of their personal health information. In some states, guardianship legislation lays down special rules for consent on behalf of incompetent patients. In other cases, the medical practitioner should speak to the patient’s relatives or carers to obtain their agreement to the proposed use or disclosure of the personal health information. The patient should be involved in the decision to the greatest extent possible.
2.7 Assessing maturity to give consent

The Privacy Act does not specify at what age a person can give consent for the collection, use or disclosure of personal health information. This means that medical practitioners must assess whether a child or young person has the maturity to understand and make their own decisions about the handling of their personal health information.

If the child or young person is not competent to make these decisions, a parent or guardian must do so on their behalf. Medical practitioners should be aware that while no age of consent is specified under the Privacy Act, there are specific statutory provisions in each state and territory dealing with the age at which a child or young person can give valid consent to medical treatment. For children who are not legally able to consent to medical treatment under the relevant state or territory legislation it may be prudent to obtain the consent of a parent or guardian for the use or disclosure of the child’s personal health information.

2.8 Family medical histories (including genetic information)

Where medical practitioners obtain a family medical history from a patient, it is rarely practicable to obtain the consent of the family members for the collection of their personal health information. To address this issue, the Office of the Australian Information Commissioner issued a Public Interest Determination under the Privacy Act.5

The Public Interest Determination allows the collection of family, social and medical histories. This expires on 10 December 2016 inclusive.

Relevant NPPs:

1. Collection, subclause 1.3 (c) (d)
2. Use and disclosure, subclauses 2.1 (b), 2.4, 2.5, 2.6
10. Sensitive information, subclause 10.2
3. Advising patients when collecting personal health information

At the time of collecting personal health information, medical practitioners must take reasonable steps to ensure that the patient understands:

- what information is being collected
- why the information is being collected
- who within the practice will have access to the information
- how the information will be used including, where applicable, that it may be used for research purposes
- where relevant, the fact that there is a statutory obligation to collect the information (eg. disease notification requirements)
- any proposed disclosure of the information to third parties
- that the patient can have access to the information, once collected
- the consequences of not providing the information
- if relevant, that the information will be computerised
- where the information is being collected by the medical practitioner on behalf of an organisation (eg. a medical practice), the identity of the organisation and how to contact it.

The information must be necessary for the purpose for which it is collected, and must be collected in a way that is lawful, fair and not unreasonably intrusive. Wherever it is reasonable and practicable to do so, personal health information about a patient must be collected directly from the patient rather than from third parties. Similarly, wherever it is lawful and practicable to do so, patients must have the option of not identifying themselves when requesting a health service.

At the time of providing personal health information to a medical practitioner, patients must understand how their information may be used or disclosed, and what rights of access will apply. Only then can they make an informed decision about whether to provide the information. Openness on the part of the doctor about how the information will be used can also assist a better understanding by the patient of his or her medical condition and promote shared expectations and a relationship of trust between doctor and patient.

3.1 The importance of having a written policy

Medical practices must have a written policy for their management of personal health information which is readily available to all patients (refer to Section 8 – Data security and retention). It will assist patients to understand how their personal health information may be used if the key elements of the policy, including the matters listed above, are outlined in a patient information leaflet or newsletter.

3.2 Considerations before sharing health information

Whenever personal health information is to be made available to a person other than the treating medical practitioner, particular care should be taken to ensure that the patient understands that this will occur. Patients should understand that practice staff may have access to their records for billing or other administrative purposes.
3.3 Health information from third parties

Although medical practitioners obtain most personal health information direct from the patient (and must do so wherever practicable), they will also receive some personal health information from third parties, such as other treating health professionals.

In the case of information received from third parties, medical practitioners must take reasonable steps to ensure that the patient is made aware of the matters listed above, except where doing so would pose a serious threat to the life or health of any individual.

3.4 Anonymity of patients

Under the Privacy Act, patients must be permitted to remain anonymous when requesting a health service, as long as it is lawful and practicable for them to do so. An example of where it would be unlawful is where a medical practitioner is required to collect identifying information from the patient in order to satisfy statutory disease notification requirements. If a medical practitioner is concerned that a patient may suffer some detriment by remaining anonymous, for example if records of previous tests or treatment cannot be obtained, this should be explained to the patient.

Relevant NPPs:
1. Collection, subclause 1.3
5. Openness, subclauses 5.1, 5.2
8. Anonymity
4. Patient access to medical records

Patients have a right to access their personal health information. In most cases, patient requests for access to information can be satisfied by way of an accurate and up to date summary containing all relevant material. However, patients must be aware of their right to have access to their full medical record and agree on the form of access.

Where a patient requests access to their personal health information, a medical practitioner must respond to the request within a reasonable period after the request is made, and enable access to the information in the manner requested by the patient if it is reasonable and practical to do so.

‘A useful precaution before processing any request for access is to check the identity of the person making the request, to ensure information is not mistakenly disclosed’. Refer to Section 10 – Government related health identifiers.

Where a patient requests an alteration or correction to their personal health information, medical practitioners should note details of the request on the medical record and indicate whether they agree that the request for alteration or correction is appropriate.

Medical practitioners can refuse patients access to their personal health information only if:
• providing access would pose a serious threat to the life, health, or safety of any individual, or to public health or public safety
• providing access would have an unreasonable impact on the privacy of other individuals
• the request for access is frivolous or vexatious
• denying access is required or authorised by law.

Sharing information is integral to good doctor-patient communication and to high quality care, providing an opportunity for health promotion and for building trust. The Privacy Act gives patients a legal right of access to their personal health information, subject only to certain limited exceptions.

4.1 Explanation of the medical record

Where a patient is provided with access to his or her medical record, it is normally desirable for the medical practitioner to be present to clarify any aspects and to permit any concerns of the patient to be discussed and resolved. In some cases, it may be appropriate to refer the patient back to the original author of the letter or medical report.

4.2 Fees

It is unlawful under the Privacy Act to charge the patient a fee for requesting access to personal health information. A fee may be charged to cover the cost of providing access (eg. for file search, copying or printing records) as long as the fee is not excessive having regard to the expense and inconvenience for the medical practitioner. Medical practitioners should bear in mind individual circumstances and capacity to pay for access when considering what charges may apply.

Medical practitioners should also check with their relevant state or territory commissioner of health information organisation for advice regarding the maximum administrative fees allowable.
4.3 Access of medical records via a third party

Medical practitioners can discharge their duty to provide patient access to personal health information by arranging for the patient to obtain the information from a third party, such as the referring doctor. This might be the preferred option for a pathologist, eg. which has had no direct contact with the patient. In all cases, however, the patient must agree on the form of the access and has the right to insist on direct access if desired.

4.4 Amendments/annotations made to medical records

Medical practitioners should not agree to alter personal health information at the request of a patient unless the request for alteration is straightforward, such as amending an address or telephone number. With most requests for alteration or correction, medical practitioners should annotate the record to indicate the nature of the request and whether or not they agree with it. For legal reasons, it is advisable not to alter or erase the original entries in a medical record, and in some circumstances it may be unlawful to do so.

4.5 Correction of personal health information

If a patient requests a medical practitioner to correct their personal health information, the medical practitioner must take steps that are as reasonable in the circumstances to correct that information to ensure that the information is accurate, up-to-date, complete and relevant within a reasonable period after the request is made.

4.6 Issues in withholding access

Access to personal health information can be withheld where a medical practitioner has reasonable grounds for believing that granting access to the medical record will cause a serious threat to the life or health of an individual including harm to physical or mental health. The threat may be to the patient or another person. The threat must be real, not hypothetical or speculative.

In such cases, medical practitioners should consider whether there are alternative ways of satisfying the patient’s request for information that would not involve the same threat, such as by meeting with the patient to discuss any issues in person or, with the patient’s consent, providing the record to another medical practitioner of the patient’s choice.

‘Where there is a legitimate reason to withhold access, it is important to keep in mind that this may only apply to part of the health information on the record, access will still need to be provided to the rest of the information. For example, removing the other person’s identifying details before releasing the information. If this approach is taken, care is needed to ensure the remaining context does not reveal the identity of that person’.4

Where a request for access is refused, the medical practitioner must explain this to the patient and document the reasons for the refusal. If a patient requests access to their personal health information and the medical practitioner refuses, they must, in writing, give reasons for refusal except to the extent that having regards to the grounds for refusal, would be unreasonable to do so and notify the patient about mechanisms available to complain about the refusal.4

It will be rare that personal health information can be withheld because of an unreasonable impact on the privacy of others. There may, for example, be information provided by another family member on a confidential basis, such that it would not be appropriate for the patient to be told the information or the identity of the person who provided it.

However, the medical practitioner must weigh the privacy interest of the third party in such cases against the clear interest of patients to have access to their own personal health information.
Where legal proceedings have been commenced or are threatened against the medical practitioner, documents or other information generated for the purpose of those proceedings may be subject to a claim for legal privilege and do not have to be produced to the patient. In this example, withholding access to certain personal health information is authorised by law.

4.7 Forms of access

Access may be provided in a number of different ways. For example, an individual may look at the information and talk though the contents with their healthcare service provider. They may obtain a copy of the information (eg. a photocopy in the case of paper records, or a copy of an X-ray), take notes on the content, or listen to or view the contents of an audio or video recording. Or they may obtain a print-out of the information if it is stored electronically, or be given an electronic copy of the information.

4.8 Processing a request

It is not a legal requirement that requests be made in writing, and there are likely to be some situations where a written request is unnecessary. For example, if an individual asks a healthcare service provider for a copy of his/her latest test results during the consultation, this request could be handled by simply providing a copy of the information at the time.

If the request is more complex, eg. because it involves collating information from both paper and electronic sources, it may be preferable to ask for the request in writing. A written request allows for more clarity about the information to which access is sought, and it provides a record of the request on file.

A useful precaution before processing any request for access is to check the identity of the person making the request, to ensure information is not mistakenly disclosed (refer to Section 10 – Government related health identifiers).

Relevant NPPs:
6. Access and correction, subclauses 6.1, 6.4
5. Using and disclosing personal health information

For the purposes of this guideline:

• ‘use’ means the use of personal health information within the practice which collected the information
• ‘disclosure’ means the release of the information to a third party.

Subject to the exceptions listed below, personal health information held by medical practitioners can only be used or disclosed:

• for the purpose for which it was collected, or
• for another directly related purpose that is within the reasonable expectations of the patient.

Personal health information can be used or disclosed to others for some other purpose if:

• the patient concerned has consented to the use or disclosure
• the medical practitioner reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual’s life, health or safety, or a serious threat to public health or public safety
• the use or disclosure is required or authorised by law (eg. statutory duties to notify certain infectious diseases or suspected child abuse, or compliance with a subpoena or court order)
• the medical practitioner has reason to suspect unlawful activities or reasonably believes it is reasonably necessary for certain law enforcement purposes
• the information concerns a patient who is incapable of giving consent, and is disclosed to a person responsible for the patient for compassionate reasons or to enable appropriate care or treatment to be provided to the patient
• the medical practitioner believes the use or disclosure is necessary to assist an entity, body or person to locate a person who has been reported as missing or for diplomatic or consular functions or activities
• the use or disclosure is necessary for research or the compilation of statistics, is approved by a properly constituted Human Research Ethics Committee (HREC), and is conducted in accordance with that committee’s requirements.

Any disclosure should be limited to that which is either authorised or required in order to achieve the desired objective. Medical practitioners must not use or disclose a patient’s Medicare number, IHI or any other identifier assigned by or on behalf of a Commonwealth agency, unless required to do so to fulfil their obligations to the agency, or unless the use or disclosure is to lessen or prevent a serious threat to life, health or safety or public health and safety, where required or authorised by law or for certain law enforcement purposes or investigations of suspected unlawful activities.

5.1 Use of information must be within reasonable expectations

Where the proposed use or disclosure is directly related to the purpose for which the personal health information was collected and would have been within the reasonable expectations of the patient at the time of collection, it is not necessary to seek further consent from the patient. For example, if it is made clear to the patient at the commencement of the doctor-patient relationship, or at the time of each relevant consultation that information obtained may be used within the practice for quality assurance or medical research, this activity is permissible under the Privacy Act.

This emphasises the benefits of having a patient information leaflet or some other system to ensure that the medical practitioner and patient at all times have shared expectations as to how the patient’s personal health information is to be used or disclosed.
5.2 Third party disclosure

Where personal health information is to be disclosed to a third party, the medical practitioner must consider what information is relevant for the proposed purpose, and ensure that no personal health information is disclosed unnecessarily. A medical practitioner may not be justified, in forwarding a copy of a patient’s complete medical record to another medical practitioner where the record contains personal health information that has no bearing upon the condition to which the referral relates, or in producing the entire medical file in answer to a subpoena that requires only the production of certain specified documents.

5.3 Electronic transfer of information

The use of electronic means for transferring personal health information will sometimes make it easier to transfer large quantities of information. However, the principles governing the electronic transfer of information are no different from those governing other means of transferring health information. Secure encryption protocols must be in place and medical practitioners must ensure that these are operating effectively.

The consent of the patient is not required where the use or disclosure of the personal health information is necessary to lessen or prevent a serious and imminent threat to an individual’s life, health or safety, or a serious threat to public health or safety. This exception might apply in the case of mental illness, where the patient is threatening to harm other people, or where a person has an infectious disease that is likely to be transmitted to others. In these cases, medical practitioners must satisfy themselves that the disclosure of the information is the only effective way of averting the risk, and the consent of the patient should still be sought if it is appropriate and feasible to do so.

5.4 Change of doctor in the practice

There may be cases where a medical practice is taken over by a new medical practitioner or where a new medical practitioner joins an existing group practice. In such cases, a question arises as to whether the new medical practitioner can have access to the patient records of the practice. Access is only appropriate where the patient concerned has given consent. Often, consent will be implied from the fact that the patient has sought a consultation with the new medical practitioner.

5.5 Transferring records to another healthcare service provider on request

“If a patient wants to transfer their care to another healthcare service provider, they can authorise the disclosure of health information from the original provider to the new provider. A copy of the patient’s personal health information could then be transferred in this way. However, if the original provider declines to transfer the information, then a patient may request access to the health information and seek a copy”.

5.6 Sale or closure of a practice

In the event of the sale or closure of a practice, the medical practitioner (or executor in the case of the medical practitioner being deceased) should take reasonable steps to notify patients and allow them the opportunity to transfer records to another provider.

The correct process for handling patient health information on the closure of a practice can be accessed from the Office of the Australian Information Commissioner at www.privacy.gov.au.

Relevant NPPs:
2. Use and disclosure, subclause 2.1, 2.4, 2.5, 2.6
10. Sensitive information, subclause 10.2, 10.3, 10.4
6. Medical research

Private medical practice may collect health information about a patient if the collection is necessary for any of the following purposes:

1. research relevant to public health or public safety
2. the compilation or analysis of statistics relevant to public health or public safety
3. the management, funding or monitoring of a health service.

Personal health information can be used within a practice for the purposes of medical research with the expressed consent of the patient, or where the research is directly related to the purpose for which the information was collected from the patient and this use is within the reasonable expectations of the patient.

In all other cases, the research should be approved by an Human Research Ethics Committee (HREC) constituted in accordance with National Health and Medical Research Committee (NHMRC) guidelines, and must comply with the committee’s requirements.

The publication of research findings should never be in a form that allows identification of research participants.

The legal and ethical principles governing medical research using human participants make it clear that the consent of the research participant is of paramount importance. Where there is any doubt as to whether the proposed research in the practice is directly related to the purpose for which the information was collected, or that it would be within the reasonable expectations of the patient, expressed informed consent should be obtained in writing. Patients should understand what the proposed research involves, the ways in which their personal health information will be used, and the risks and benefits of agreeing to participate, and if the research is intended to be published.

6.1 When to obtain HREC approval

The Privacy Act only requires approval to be obtained from an HREC in the case of medical research using personal health information without the consent of the patient. However medical practitioners should also obtain HREC approval for research projects involving the transfer of information outside the practice in order to ensure the integrity and adequacy of the consent process. In any event HREC approval will be necessary when the research involves NHMRC funding or is conducted by an organisation that receives NHMRC funding. If the organisation undertaking the research has obtained HREC approval, then the medical practitioner supplying the information does not require additional approval.

6.2 Considerations when participating in research

It should be noted that even if the research has HREC approval, medical practitioners are not obliged to disclose the information if they consider it would be inappropriate to do so.

Where the records of a particular practice are used for carrying out public health or other medical research using de-identified data, patients of the practice should be made aware of this use of their records. This may be done by way of an information sheet in the waiting room.

In the case of epidemiological research, it will generally not be necessary to keep identifiable data sets after the relevant information has been extracted from the patient records. In any event, all research records should be de-identified at the earliest possible time consistent with the proper conduct of the research.
6.3 Circumstances where consent may be waived

The following is taken from the NHMRC’s National Statement on Ethical Conduct in Human Research.

Only an HREC may grant a waiver of consent for research using personal information in medical research, or personal health information. Other review bodies may grant waiver of consent for other research.

Before deciding to waive the requirement for consent (other than in the case of research aiming to expose illegal activity) an HREC or other review body must be satisfied that:

• involvement in the research carries no more than low risk to participants
• the benefits from the research justify any risks of harm associated with not seeking consent
• it is impracticable to obtain consent (eg. due to the quantity, age or accessibility of records)
• there is no known or likely reason for thinking that participants would not have consented if they had been asked
• there is sufficient protection of their privacy
• there is an adequate plan to protect the confidentiality of data
• in case the results have significance for the participants’ welfare there is, where practicable, a plan for making information arising from the research available to them (eg. via a disease-specific website or regional news media)
• the possibility of commercial exploitation of derivatives of the data or tissue will not deprive the participants of any financial benefits to which they would be entitled
• the waiver is not prohibited by state, federal or international law.

Given the importance of maintaining public confidence in the research process, it is the responsibility of each institution to make publicly accessible (eg. annual reports) summary descriptions of all its research projects for which consent has been waived (as above).

‘Research is an important component of general practice in Australia. Practices are encouraged to participate in research both within their own practice and through reputable external bodies’.

Medical practitioners undertaking medical research should be aware of and comply with general guidelines applicable to medical research in Australia, which include the NHMRC’s National Statement on Ethical Conduct in Human Research available at www.nhmrc.gov.au/_files_nhmrc/file/publications/synopses/e72-jul09.pdf.

The Commonwealth Therapeutic Goods Administration’s Clinical trial handbook also has relevant information which can be accessed at www.tga.gov.au/ct/cthandbook.pdf.

Relevant NPPs:
10. Sensitive information, subclauses 10.3, 10.4
7. **Quality improvement and continuing professional development**

Personal health information can be used for quality improvement and continuing professional development activities within the practice where:

- the activities are directly related to the purpose for which the information was collected and are within the reasonable expectations of the patient
- the patient has given expressed consent for the use of personal health information for these activities
- the personal health information has been de-identified
- the activities involve research or the compilation of statistics, have been approved by a properly constituted HREC, and are conducted in accordance with that committee’s requirements.

These would be considered a directly related secondary purpose for information use or disclosure. Therefore in general, the practice would not need to seek specific consent for this use of patients’ health information.6

Ethics approval is not required for a quality improvement activity undertaken within a general practice where the primary purpose is to monitor, evaluate or improve the quality of healthcare delivered by the practice.6

Despite improvement and continuing professional development activities being essential to promoting and maintaining high quality healthcare. Many patients may not understand what these activities are, nor that they may involve access to personal health information by people other than the treating medical practitioner. It is therefore important for medical practitioners to make their patients aware that these activities are carried out as part of the normal functioning of the practice.

This can be achieved through the distribution of patient information leaflets explaining the quality assurance and continuing professional development activities undertaken by the practice, and through direct discussion with patients, with the aim that patients come to expect such ongoing activities, and appreciate the benefits of improved quality standards.

In addition, practices are encouraged to include information about quality improvement activities and clinical audits in the practice policy manual on managing health information.7 Please refer specifically to Criterion 4.2.1 – Confidentiality and privacy of health information of the RACGP Standards for general practices (4th edition).

Quality improvement and continuing professional development activities involving the transfer of personal health information outside the practice. These activities should also comply with relevant guidelines on quality assurance or continuing professional development issued by an appropriate medical college, and be approved by that college or its agent.

### 7.1 Notifying patients of quality improvement activities

Particular care must be taken with highly sensitive personal health information, where the patient may wish absolute confidentiality to be maintained. For example, a patient recently diagnosed with HIV infection, may have no objection to the medical record in general being used for quality assurance or continuing professional development, but may not want his or her HIV status to be known by anyone except the treating medical practitioner. Medical practitioners should be sensitive to these concerns, and respect the patient’s wishes.

Quality improvement and continuing professional development activities must take reasonable steps to ensure that the personal information the medical practitioner collects, uses or discloses is accurate, up-to-date and complete.

**Relevant NPPs:**

2. Use and disclosure, subclause 2.1
3. Data quality
8. **Data security and retention**

Medical practitioners must take reasonable steps to protect the personal health information they hold from misuse and loss, and from unauthorised access, modification or disclosure. Adopting data security measures is an important way of ensuring that personal health information is used appropriately.7

Personal health information should be retained by medical practitioners for as long as it may still be required for use or disclosure in accordance with Section 5 – *Using and disclosing personal health information* of this handbook (and in any event, for any minimum period prescribed by law).

Physical measures for protecting the security of personal health information may include, but are not limited to, having locked filing cabinets, security alarm systems to detect unauthorised access and ensuring no unauthorised after hours access to the surgery.7

Alternatively, measures for protecting electronic security may include the utilisation of password protection, automatic log offs, log file/electronic audit trails, firewalls, malware and virus protection, checking fax numbers before sending personal information and ensuring the encryption of data for high risk transmissions.8

It is important to recognise that information technology systems have the potential to increase the risk of unauthorised disclosure of personal information. Given this, it is equally important that practices develop and implement appropriate policies and procedures that specify which staff have access to personal health information and under what circumstances.8

In addition, medical practitioners must remain cognisant at all times of the uses for which the personal health information was collected, and ensure they do not go beyond what the patient has consented to or reasonably expects.7

Organisations need to assess their security risks and take appropriate measures to protect the integrity of their information systems and networks. Risk assessments should cover information systems for storing, processing and transmitting information.8

Good practice for computer and information security includes both expert monitoring and systems, such as firewalls, routers, network intrusion detection systems, host intrusion detection systems and appropriate encryption. The protective measures will depend on the circumstances and risks involved.7

The RACGP *Computer and information security standards* (CISS) is a guide to gain an understanding of the requirements for computer and information security implementation in general practice. This resource is available at www.racgp.org.au/ehealth/ciss.

8.1 **Retention of records (timeframes)**

The *Privacy Act* requires personal health information to be destroyed or permanently de-identified once it is no longer needed for any authorised use or disclosure under the legislation. The authorised uses or disclosures are listed in Section 5 – *Using and disclosing personal health information* of this handbook. In the case of personal health information collected for the purpose of providing medical advice or treatment, it may be appropriate to retain this information indefinitely so that it is available, if necessary, to assist with the patient’s future diagnosis and treatment.

The practice must ensure that both active and inactive patient health records are kept and stored securely. An inactive patient health record is generally considered to be the record of a patient who has not attended the practice/service three or more times in the past 2 years. It is recommended that inactive patient health records are retained by the practice indefinitely or as stipulated by the relevant national, state or territory legislation.

At the very least, it is recommended that individual patient medical records be retained for a minimum of seven years from the date of last contact, or until the patient has reached the age of 25, whichever is the longer.6
8.2 Minimum state or territory requirements may apply to record retention

Medical practitioners should also be aware that there may be specific legislation in their state or territory requiring a minimum period of retention of medical records.

8.3 Destruction or permanent de-identification of health information

Health information is highly valuable for many reasons, most importantly for an individual’s ongoing healthcare, but sometimes also for wider public health and safety reasons.4

‘This type of information could include records which are no longer required for treatment and care, or for health service management, monitoring or evaluation’.4

8.4 Destruction of health information

Personal health information that is no longer required must be securely destroyed in order to prevent any unauthorised access.

Securely destroyed does not mean deleted from the database or software system; the latter usually means simply flagging that a patient record has been deleted and at some point in the future when maintenance of the database or system is performed, the record may be removed from the index (not actually from the computer database).

Secure deletion has a different purpose to computer security – it is where the records are no longer accessible through normal or forensic means. Deletion from a database does not erase the record from the database nor does it remove the record from the hard disk or other storage medium; it usually means the indexing accessible path is removed only, thereby making it inaccessible via the software only. Although this is sufficient from the perspective of the normal usage by the user via the medical practice software, it is by no means securely deleted. Unless security is erased and overwritten multiple times, the data will remain on the storage medium and is accessible forensically.

8.5 De-identification of the medical record

Medical practitioners may alternatively choose to permanently de-identify the medical record, as long as care is taken to ensure that there is no reasonable prospect of the patient being identified from the remaining information.

The de-identification of personal health information is more than simply removing the patient’s name. Whenever the information is in the form of individual data sets, there is a risk that the data set could be linked to a particular individual on the basis of details of age, postcode and medical condition. The more information included in the data set, the greater the risk of identification.

Furthermore, even where data is aggregated, care should be taken that the number of people in each ‘cell’ or sub-group is sufficient to ensure that the privacy of the individuals involved is not compromised. NHMRC guidelines specify a minimum of five cases in each cell.3

8.6 The use of healthcare identifiers

The use of patient identification numbers instead of names is sometimes helpful as a means of protecting privacy. However, patient identification numbers must not be derived from the patient’s name, date of birth, address, telephone number, Medicare number, IHI (or any other identifier assigned by a Commonwealth agency) or any other information that could identify the person. The identification number should also not reveal any personal health information about the patient.
8.7 Transfer of information overseas

The issue of transferring personal health information outside Australia is particularly important because many countries have privacy standards or laws that are less stringent than those that apply within Australia. Ideally, expressed patient consent should always be sought before transferring personal health information outside Australia.

Personal health information can be transferred to an individual or organisation outside Australia only if:

- the patient has given expressed consent for the transfer, or
- it is impracticable to obtain patient consent, but the proposed transfer of information is for the benefit of the patient and the patient would be likely to give consent, if asked.

8.8 Security policy

To encourage an organisational culture that respects privacy and confidentiality certain practices are recommended to develop and use a security policy. The implementation of a security policy would assist in ensuring that all organisational systems used for processing and storing or transmitting personal information have actioned appropriately.6

For a security policy to be effective, it is essential that the policy is monitored and reviewed on a regular basis. It is equally important for the relevant staff to be made aware of the practice’s security policies including their implementation and management.7

The RACGP CISS provide comprehensive advice regarding the development of an access/security policy.

Relevant NPPs:

4. Data security, subclauses 4.1, 4.2
9. Transborder data flows, subclauses (b), (e)
9. Healthcare provider identified health information

Patient de-identified health information that can be identified with a particular health provider should not be disclosed to third parties without the consent of the healthcare provider concerned, unless there are overriding legal or public interest considerations.

There may be health information that is de-identified so far as the patient is concerned but which still permits the health provider to be identified. An example of such information would be records of drugs prescribed by a particular medical practitioner or details of hospitalisations requested by a particular practice. This information retains some sensitivity from the point of view of the health provider and should be protected against inappropriate disclosure.

9.1 Patient consent required where patient is identified

Where the health information enables the patient and the health provider to be identified, the patient retains the right to control the flow of that information. However, where only the healthcare provider can be identified, the consent of the health provider should be obtained before any disclosure of the information is made.

This protects the privacy interests of the healthcare provider and enables the health provider to ensure that even where patient health information is de-identified it is not used in inappropriate or unauthorised ways.

Relevant NPPs:
2. Use and disclosure, subclause 2.1
10. Government related health identifiers

A healthcare identifier is a unique number assigned to healthcare consumers, healthcare providers and organisations that provide health services. These identifiers are assigned by and administered via the Healthcare Identifiers Service (HIS) which has been established to carry out this work. The Department of Human Services (Medicare Australia) has the responsibility of operating this service.

10.1 Healthcare identifiers service

The HIS provides a nationally consistent way of identifying all who are involved in the documentation associated with a healthcare event. It provides confidence that the right health information is associated with the right individual at the point of care and when exchanging information electronically.

Healthcare identifiers are one of the foundations of the national e-health system and part of the core infrastructure needed to support secure electronic communications across Australia’s healthcare system. The three types of national identifiers:

1. Individual Healthcare Identifier (IHI) is automatically allocated to all persons enrolled with Medicare and anyone who is issued with a Department of Veteran’s Affairs (DVA) entitlement and available to all others who seek healthcare in Australia.
2. Healthcare Provider Identifier – Individual (HPI-I) is allocated to registered or registrable healthcare providers involved in providing patient care.
3. Healthcare Provider Identifier – Organisation (HPI-O) can be allocated to organisations that deliver healthcare such as general practices, community health services and hospitals.

The legislation to support the HIS includes:

- Healthcare Identifiers Act 2010
- Healthcare Identifiers (Consequential Amendments) Act 2010

A healthcare service provider may only use, disclose or keep a record of these identifiers where necessary to meet any obligations to the relevant agency; or where there are overriding legal or public interest considerations; where these activities occur for ‘prescribed’ circumstances relating to a regulation made subject to the Privacy Act.\(^\text{10}\)

10.2 National e-health record system

The national personally controlled electronic health record (PCEHR) system aims to place the patient at the centre of their own healthcare by enabling access to important pieces of health information when and where it is needed by patients and their healthcare providers. A PCEHR will be a secure, electronic summary of the health record stored and shared in a network of connected systems. The PCEHR will not be the whole patient health or medical record. The PCEHR will hold significant health information and aims to assist with safety and continuity of care.\(^\text{11}\)

For further information visit www.ehealthinfo.gov.au.

Relevant NPPs:

7. Identifiers, subclause 7.1
11. Establishing a practice policy on personal health information

A general practice must take steps to implement policies, procedures and systems relating to practice functions and activities that ensure the practice complies with the Australian NPP and that will enable a practice to deal with inquiries and complaints from consumers about the practice’s compliance with the NPPs.

All medical practices must have a clearly expressed and up-to-date information policy for their practice, setting out procedures for the management of personal health information held by the practice. The policy must explain how personal health information is collected and used within the practice, and the circumstances in which it may be disclosed to third parties. It must also lay down procedures for:

- ensuring that the collection of personal health information, whether by interview, observation or in writing, is conducted in a setting which provides privacy and protects the information from access by unauthorised people
- obtaining the patient’s consent for the use or disclosure of personal health information by practice doctors, locums, registrars and other authorised healthcare service providers to the practice, and for the purposes of practice research and quality assurance and improvement
- providing patients with access to their personal health information upon request
- de-identifying personal health information where necessary
- ensuring that personal health information is disclosed to third parties only where consent has been obtained
- classifying personal health information so that any disclosure of the information to third parties is limited to that which is authorised or required
- protecting against unauthorised access to information while stored and transmitted in any form (eg. paper, electronic, verbal)
- security against loss of data
- retention of individual medical records until the patient has reached the age of 25 or for a minimum of seven years from the time of last service, whichever is the longer.

The policy should make specific provision for staff training and education in relation to privacy laws and confidentiality so that all staff is aware of appropriate procedures for handling personal health information.

A practice must take such steps as are reasonable in the circumstances to make its privacy policy available free of charge and easily accessible to its patients upon request. An outline of the policy could also be included in a practice information leaflet.

Establishing a practice policy on personal health information will enable the medical practitioner to deal with enquiries or complaints from patients about their compliance with the NPP.

The precise content of the information policy will depend upon the personnel structure of each practice and the record keeping system used. In each case, however, the important point is to ensure acceptable minimum standards of privacy protection and data integrity are achieved, consistent with applicable privacy legislation.

Relevant NPPs:

5. Openness, subclauses 5.1, 5.2
Resources

RACGP resources:
- Computer and information security standards available at www.racgp.org.au/ehealth/ciss
- Telehealth standards available at www.racgp.org.au/standards/telehealth

Advice on compliance:
- Office of the Australian Information Commissioner
  Telephone: 1300 363 992

- Office of the Privacy Commissioner – New South Wales
  Telephone: 02 8019 1600

- Office of the Information Commissioner – Queensland
  www.oic.qld.gov.au
  Telephone: 07 3234 7373

- Office of the Information Commissioner – Northern Territory
  www.infocomm.nt.gov.au
  Telephone: 1800 005 610

- Office of the Victorian Privacy Commissioner – Victoria
  Telephone: 1300 666 444

- Human Rights Commission – ACT
  www.hrc.act.gov.au
  Telephone: 02 6205 2222

- Privacy Committee South Australia – SA
  Telephone: 08 8204 8773
References


Appendix: Guidelines for the consent, quality security, storage and transfer of personal health information

### 1. Patient consent

<table>
<thead>
<tr>
<th>Objective</th>
<th>Record type</th>
<th>Minimum procedures</th>
<th>Additional procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i) Patient consent is obtained and documented</td>
<td>Manual</td>
<td>Annotate in the patient’s record their consent and any restrictions, eg. information is not to be used for medical research. When there is a change to the conditions of consent, update the patient’s record, noting the date and changed restriction.</td>
<td>The practitioner provides an information sheet/consent form for the patient to read and sign.</td>
</tr>
<tr>
<td>Electronic</td>
<td>Record in the patient’s record their consent and any restrictions, eg. information is not to be used for medical research. When there is a change to the conditions of consent, update the patient’s record, noting the date and changed restriction.</td>
<td>The practitioner provides an information sheet/consent form for the patient to read and sign.</td>
<td></td>
</tr>
</tbody>
</table>

### 2. Medical record quality

<table>
<thead>
<tr>
<th>Objective</th>
<th>Record type</th>
<th>Minimum procedures</th>
<th>Additional procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i) Complete and accurate data</td>
<td>Manual</td>
<td>The treating medical practitioner enters personal health information at the time of consultation or when data becomes available. Treating medical practitioners review and identify any records that have personal health information that have not been updated for accuracy (ie. when they have not personally entered the data themselves). Train medical support staff in record keeping procedures. Note name of the treating medical practitioner who is responsible for the entered data.</td>
<td>Develop and use proformas for recording data. Match medical records to the daily consultation record to identify any records that have entered data and have not been updated.</td>
</tr>
<tr>
<td></td>
<td>Electronic</td>
<td>The treating medical practitioner should enter personal health information at the time of consultation or when data becomes available – where practical. Train medical support staff in computer procedures and record keeping. Record name of the treating medical practitioner who is responsible for the entered data.</td>
<td>Establish tracking procedures for medical data (audit trail) including description of the nature of changes and identification of the user making the changes. Match medical records to the daily consultation record to identify any records that have entered data and have not been updated.</td>
</tr>
</tbody>
</table>
### 3. Disclosure of personal health information

<table>
<thead>
<tr>
<th>Objective</th>
<th>Record type</th>
<th>Minimum procedures</th>
<th>Additional procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i) Patient consented to third party disclosure</td>
<td>Manual</td>
<td>Ensure that patient consent has been obtained and annotated.</td>
<td>Develop and use proformas for recording consent.</td>
</tr>
<tr>
<td></td>
<td>Electronic</td>
<td>Ensure that patient consent has been obtained and recorded.</td>
<td>Establish an onscreen prompt for obtaining consent prior to disclosure. Establish a default condition of ‘no consent.’</td>
</tr>
<tr>
<td>(ii) Transfer disclosures are authorised by the medical practitioner</td>
<td>Manual</td>
<td>Ensure medical practitioner authorisation prior to any release of data, eg. medical practitioner personally initiates, notes and signs transfer/disclosure, or authorises a delegated staff member to do so.</td>
<td>Medical practitioner reviews audit trial of all transferred data to ensure appropriate authorisation was given.</td>
</tr>
<tr>
<td></td>
<td>Electronic</td>
<td>Ensure medical practitioner authorisation prior to any release of data, eg. medical practitioner personally initiates, notes and signs transfer/disclosure, or authorises a delegated staff member to do so.</td>
<td></td>
</tr>
<tr>
<td>(iii) Personal health information is de-identified when necessary</td>
<td>Manual</td>
<td>The medical practitioner or authorised person should manually delete or mask any identifying data in records. Assign data identification numbers using, eg. randomly generated identifiers (do not base identification numbers on patient identity). Examples of unacceptable numbers include those based on birth dates or Medicare numbers.</td>
<td>Ensure software program de-identifies all personal health information transmissions where appropriate.</td>
</tr>
<tr>
<td></td>
<td>Electronic</td>
<td>Assign patient identification numbers using, eg. randomly generated identifiers (do not base identification numbers on patient identity). Examples of unacceptable numbers include those based on birth dates or Medicare numbers.</td>
<td></td>
</tr>
<tr>
<td>Objective</td>
<td>Record type</td>
<td>Minimum procedures</td>
<td>Additional procedures</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| (iv) Authorised disclosure of personal health information includes only necessary information | Manual      | The medical practitioner or authorised person should mask or delete unnecessary information, eg. reformat records, in accordance with the patient’s specified consent.                                                                                                             | Flag to notify the presence of ‘privileged care’ data.  
Ensure the use of a ‘confidential envelope’ that forms a discrete part of the client’s paper record, which houses sensitive health data.                                                                                             |
|                                                                          | Electronic  | Establish a prompt withhold information, and/or procedures to ensure only necessary data is selected prior to transmission or release of data consistent with the patient consent obtained.                                                                                                           | Establish a classification system to assist identification of levels of data.  
Link authorisation and access controls to this classification system.  
Establish a mechanism to block or mask unnecessary information.  
Alert other providers via a technical ‘flag’ mechanism that data is stored under a ‘privileged care’ section.  
When sensitive health information is locked, the healthcare provider implementing the lock must notify the receiving individual provider that a lock was applied when the individual provider believes the information is important to the individual patient’s care plan. |
| (v) Only authorised people have access to personal information            | Manual      | Hold records in an area that is not readily accessible to people other than medical practitioners and authorised practice staff.  
Locate fax machines, printers and documents in an area not readily accessible other than to medical practitioners and authorised practice staff.  
Records taken outside the practice (eg. for home consultation) should be held under the direct control of the medical practitioner, eg. carried at all times, transported securely, or stored in a secure off-site location. | Store records in a locked room or secure filing cabinet.  
Use physical or electronic locks for after hours protection.                                                                                                                                                                            |
|                                                                          | Electronic  | Use at minimum a two-level logical access control system, eg. with user identification and password.                                                                                                                                                                                                                           | Use physical or electronic locks and cards, fingerprint readers.                                                                                                                                                                            |
### Disclosure of personal health information

<table>
<thead>
<tr>
<th>Objective</th>
<th>Record type</th>
<th>Minimum procedures</th>
<th>Additional procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support this with good security administration procedures, eg. passwords which are changed monthly, and automatic log-off of terminals or password protected screen savers after a period of inactivity, eg. 10 minutes.</td>
<td></td>
<td></td>
<td>Periodically review log of computer access and data transmissions.</td>
</tr>
<tr>
<td>Terminals displaying medical data should not be accessible to unauthorised persons.</td>
<td></td>
<td></td>
<td>Periodically conduct a compliance audit with security procedures.</td>
</tr>
<tr>
<td>Communication controllers/modems should be subject to controlled use, eg. password protection or units left “off” except when authorised transmission occurs.</td>
<td></td>
<td></td>
<td>Restrict availability of modem numbers by using silent numbers.</td>
</tr>
<tr>
<td>Permanent internet and network connections eg. hardware or (eg. ADSL or cable modems) require additional security, eg. a firewall.</td>
<td></td>
<td></td>
<td>Authenticate remote users, senders and receivers of data, by for example, hardware of software authentication of valid terminal/user.</td>
</tr>
<tr>
<td>Restrict the execution of sensitive functions, such as transmission, to authorised personnel. Ensure hard copies of personal health information are not accessible to unauthorised persons.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locate fax machines, printers, documents in an area that is not readily accessible other than to medical practitioners and authorised practice staff.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records taken outside the practice, eg. for home consultations, should be held under the direct control of the medical practitioner. For example, laptops and back-up media should be encrypted securely, transported or stored in a secure off-site location.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure backup copies of patient medical data are encrypted and are not accessible to unauthorised persons.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(vi) Records awaiting disposal are not accessible prior to destruction</td>
<td>Manual</td>
<td>Shred or dispose of records using a secured disposal system.</td>
<td></td>
</tr>
</tbody>
</table>
## Disclosure of personal health information

<table>
<thead>
<tr>
<th>Objective</th>
<th>Record type</th>
<th>Minimum procedures</th>
<th>Additional procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Dispose of records using a secure disposal system. Securely delete records and any copies held backup media such as removal hard disk, tape, diskette or other media. Securely delete or destroy all disks prior to disposal, i.e. remove data. Note: deleting data does not necessarily destroy it.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(vii) Personal health information remains confidential Manual Ensure that persons authorised to access data maintain confidentiality. For example, they should understand and sign confidentiality agreements.</td>
<td>Store sensitive data in a secure location with restricted access, e.g. in a locked cupboard within the practice. Use encryption to securely store sensitive data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Ensure that persons authorised to access data maintain confidentiality. For example, they should understand and sign confidentiality agreements.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(viii) Secure storage of personal health information Manual Store personal health information in a secure area and return it to the secure location after use. Number any loose pages and on each page identify the patient. Ensure off site storage is secure. Transfer copies of documents, not the originals. Establish a tracking system to monitor the location of records at all times. Records in use should be replaced with a sheet indicating date of removal and who has possession. This is particularly important when records have been removed from the practice (e.g. home visits, legal matters, reports or permanent external storage). Retain individual patient medical records until the patient has reached the age of 25 years or for a minimum of 7 years from the date of last contact, whichever is the greater.</td>
<td>Store critical paper records in a fireproof cabinet. Where possible, records should be retained longer than legislative and jurisdictional requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objective</td>
<td>Record type</td>
<td>Minimum procedures</td>
<td>Additional procedures</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Electronic</td>
<td>Establish a formal policy for data backups, eg. daily backups of all data or changes; weekly back-ups of the entire system; and a 4 week rolling cycle of backups.</td>
<td>Automatically save data during input sessions.</td>
<td>Locate all computers with data stored on their hard disks in a physically secure area.</td>
</tr>
<tr>
<td></td>
<td>Ensure data backups are performed by adequately trained personnel.</td>
<td>In order to duplicate data and provide greater security against loss, mirror data storage.</td>
<td>Use a secure third party to hold system storage code.</td>
</tr>
<tr>
<td></td>
<td>Establish secure offsite data storage facilities.</td>
<td>Securely store backups in a fireproof safe.</td>
<td>Ensure all backups are encrypted.</td>
</tr>
<tr>
<td></td>
<td>Regular data backups should be stored in a protected and fireproof location accessible only to authorised personnel.</td>
<td>Use off-site storage for data and software backups by means of physical transfer or electronic download.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use off-site storage for data and software backups by means of physical transfer or electronic download.</td>
<td>Perform regular (monthly) test restores.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perform regular (monthly) test restores.</td>
<td>Securely retain old software and ensure you have hardware that supports access to these files, to allow ongoing access to any older data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Securely retain old software and ensure you have hardware that supports access to these files, to allow ongoing access to any older data.</td>
<td>Confirm that records sent have been received.</td>
<td>Confirm that records sent have been received.</td>
</tr>
<tr>
<td></td>
<td>Each transmission should include the identity of the originating medical practitioner, except when the patient is not identified or anonymity of the medical practitioner is required, such as for critical incident reporting.</td>
<td>Ensure that all pages were transmitted and sent to the correct number, by checking fax transmission reports.</td>
<td>Ensure that all pages were transmitted and sent to the correct number, by checking fax transmission reports.</td>
</tr>
<tr>
<td></td>
<td>Establish an audit trail of transmissions, including recipient, date, time and records handled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(ix) Data transmitted externally is complete and accurate</td>
<td>Manual</td>
<td>Use a secure method of transfer, eg. courier, express post or registered mail.</td>
<td>Confirm that data has been received by the intended receiving party.</td>
</tr>
<tr>
<td></td>
<td>Each transmission should include the identity of the originating medical practitioner, except where the patient is not identified or anonymity of the medical practitioner is required.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Disclosure of personal health information

<table>
<thead>
<tr>
<th>Objective</th>
<th>Record type</th>
<th>Minimum procedures</th>
<th>Additional procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic</td>
<td>Establish error reporting to identify failed or incomplete transmissions.</td>
<td>Establish an electronic signature handled check of transmitted files, eg. public key infrastructure (PKI) to ensure messages are confidential, authenticated, integrity is maintained and cannot be repudiated.</td>
<td></td>
</tr>
<tr>
<td>Manual</td>
<td>Identify the intended recipient on all data transmissions (mail/fax/courier).</td>
<td>Use voice messages where the medical practitioner is satisfied as to the authenticity of the receiving party.</td>
<td></td>
</tr>
<tr>
<td>Manual</td>
<td>Mark all transmissions ‘confidential’. Use a cover sheet for all faxes.</td>
<td>Obtain confirmation from the receiving party that the data has been received and is secure.</td>
<td></td>
</tr>
<tr>
<td>Electronic</td>
<td>Prior to transmission, ensure the data is able to be received either manually or by computer – on the other end.</td>
<td>Use dedicated lines or virtual private network (VPN) connections over provider (local or wide area) computer network where all nodes are authorised.</td>
<td></td>
</tr>
<tr>
<td>Electronic</td>
<td></td>
<td>Use data encryption, eg. PKI to ensure messages are confidential, authenticated, integrity is maintained and messages cannot be repudiated.</td>
<td></td>
</tr>
</tbody>
</table>