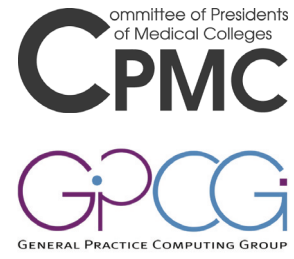




The Royal Australian College
of General Practitioners



Handbook for the Management of Health Information in Private Medical Practice

(Incorporating advice on privacy legislation requirements in Australia)

The Handbook for the Management of Health Information in Private Medical Practice is produced by The Royal Australian College of General Practitioners and the Committee of Presidents of Medical Colleges with the support of the General Practice Computing Group

1st Edition, October 2002

Handbook
for the Management
of Health Information
in Private
Medical Practice

Acknowledgments

Acknowledgments

The Handbook for the Management of Health Information in Private Medical Practice produced by The Royal Australian College of General Practitioners and the Committee of Presidents of Medical Colleges with the support of the General Practice Computing Group.

The publisher gratefully acknowledges the assistance provided by Julie Hamblin of Ebsworth & Ebsworth; Dr Graeme Miller, Medical Director, Family Medicine Research Centre; the members of the RACGP/CPMC Privacy Project Steering Committee; the Office of the Federal Privacy Commissioner; the Office of the Health Services Commissioner (Victoria), and the Office of the NSW Privacy Commissioner.

We also acknowledge the financial support of the Department of Health and Ageing.

The following organisations are also thanked for their input: The Australian Medical Association, the Australian Divisions of General Practice, and the Australian Association of Practice Managers.

Disclaimer

The Handbook has been developed as a best practice model to assist medical practitioners in complying with their legal and ethical obligations in relation to the privacy and confidentiality of personal health information. The various sections of the Handbook have been carefully designed to fit together and form a single model for privacy compliance. Medical practitioners who follow some but not all of the principles set out in this Handbook risk falling short of their minimum statutory obligations.

Copyright

1st edition © The Royal Australian College of General Practitioners 2002.

Apart from any fair dealing for the purposes of study, research, criticism or review, as permitted under the Copyright Act, no part of this work may be reproduced by any process without written permission. Enquiries should be made to the publisher or copyright holder.

ISBN 0 86906 251 4

Published by The Royal Australian College of General Practitioners
College House
1 Palmerston Crescent
South Melbourne
Victoria 3205
Australia

www.racgp.org.au

Printed and bound in Australia by Offset Alpine Printing.

Contents

	Definitions	i
1.	Quality and content of medical records	
	Ensure accuracy and completeness of records	1
2.	Patient consent	2
	2.1 Consent may be implied or expressed	
	2.2 Patients can withhold consent	
	2.3 Group practices	3
	2.4 Use of information must be relevant to consent	
	2.5 Use for teaching purposes	
	2.6 Competence to give consent	
	2.7 Assessing maturity to give consent	
	2.8 Family medical histories	
3.	Advising patients when collecting personal health information	4
	3.1 Written policy important	
	3.2 Considerations before sharing health information	5
	3.3 Health information from third parties	
	3.4 Patient may be anonymous	
4.	Patient access to medical records	6
	4.1 Medical practitioner should discuss the record being accessed with the patient	
	4.2 Fees	
	4.3 Access via a third party can discharge duty	
	4.4 Annotate amendment, do not alter records	7
	4.5 Issues in withholding access	
5.	Using and disclosing personal health information	8
	5.1 Use of information must be within reasonable expectations	9
	5.2 Third party disclosure	
	5.3 Electronic transfer of information	
	5.4 Where use or disclosure lessens or prevents a serious and imminent threat	
	5.5 Change of doctor in the practice	
	5.6 Sale or closure of a practice	
6.	Medical research	10
	6.1 When to obtain Human Research Ethics Committee approval	
	6.2 Considerations in participating in research	
7.	Quality assurance and continuing professional development	11
	Notifying patients of quality assurance activities	
8.	Data security and retention	12
	8.1 Retention of records (timeframes)	
	8.2 Minimum state or territory requirements may apply to record retention	
	8.3 Care of records no longer required	13
	8.4 Transfer of information overseas	
9.	Health provider identified health information	14
	Patient consent required where patient is identified	
10.	Establishing a practice policy on personal health information	15
11.	Further contacts	16
	Appendix	
	Procedures for the security, storage and transfer of personal health information	18

Definitions

Personal health information

In this Handbook, the expression ‘personal health information’ covers:

- information about a patient or a third party obtained by a health service provider from a patient or a third party in the course of providing a health service; or
- an opinion formed by a health 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 includes information on the person’s:

- name, address and contact details
- medical history
- Medicare number
- social circumstances
- health services requested or provided
- expressed wishes about the future provision of health services.

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, 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 issues.

Medical practitioners who work within practices that do not meet these criteria must each take individual responsibility for meeting the minimum privacy standards required by law, and implement an appropriate privacy policy for their individual medical practice.

All information in identifiable form that is received by a medical practitioner in the course of providing a health service should be regarded as personal health information for the purposes of this Handbook. This includes not only medical details but also other personal information, such as the patient's family details, employment and social circumstances.

Personal health information will most commonly be obtained from the patient, but may also be received from third parties, such as specialists or allied health professionals. The term 'personal health information' also extends to information about people other than the patient, such as the patient's family members, that medical practitioners may receive in the course of providing a health service.

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. This means that de-identified health information can be disclosed to third parties more freely and for a range of different purposes. However, 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 an information policy manual and in a practice information leaflet.

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. 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. NH&MRC guidelines specify a minimum of five cases in each cell.

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 (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.

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; and
- use a recall system, subject to patient consent, to provide systematic preventive care and early case detection using scientifically validated guidelines.

Because the primary purpose of keeping medical records is to facilitate better 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 keep and use is accurate, complete and up-to-date.

Ensure accuracy and completeness of 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.

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.

Appendix A provides procedures to assist compliance with this section.

2

Patient consent

The consent of the patient 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 Section 6 Use and disclosure of 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 the following section concerning advice to patients about information use.

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 their 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 the other 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 express 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, medical practitioners may wish 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.

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 teaching purposes

The use of personal health information for teaching purposes raises particular privacy concerns. Patients are often not aware that their health information may be used to assist in teaching, even where the treatment takes place in a teaching hospital. 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.

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 Commonwealth 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 to the use or disclosure of the child's personal health information.¹

2.8 Family medical histories

Where medical practitioners obtain a family medical history from a patient, it is rarely practicable to obtain the consent of the family members to the collection of the personal health information about them. To address this issue, the Commonwealth Privacy Commissioner has issued a Temporary Public Interest Determination under the Privacy Act. The Determination permits medical histories to be collected about the patient's family or about other relevant people without the knowledge or consent of the family member or other third party, where the medical history is necessary for the diagnosis, treatment or care of the patient.²

¹For relevant legislation refer to CCH: Australian Health and Medical Law Reporter: Clinical Practice: Consent: Minors, 17–330, 17–420

²An explanation provided by the Victorian Health Services Commissioner is available on the RACGP website

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; and
- 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.

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 Written policy important

Medical practices must have a written policy for their management of personal health information which is readily available to all patients (refer Section 9). It will assist patients in understanding 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. For example, patients should understand that practice staff may have access to their records for billing or other administrative purposes.

Some patients have particular concerns about computerised records because of a perception that these are less secure. Where the medical record system of a practice is computerised, this should be disclosed to patients. It may be helpful to allay patients' concerns by providing a written information sheet or a sign in the waiting room that explains how computers are used in the record keeping of the practice.

3.3 Health information from third parties

While 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 Patient may be anonymous

Under the Commonwealth 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.

³A model policy is available via the RACGP website

⁴Refer RACGP website for advice of the Victorian Health Services Commissioner

4

Patient access to medical records

Patients have a right to have access to 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 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 or health of any individual;
- providing access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious; or
- 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 Medical practitioner should discuss the record being accessed with the patient

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 a 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.

4.3 Access via a third party can discharge duty

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, for example, who 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 Annotate amendment, do not alter 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 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. 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 a request for access is refused, the medical practitioner must explain this to the patient and document the reasons for the refusal.

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.

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; and
- ‘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; or
- 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; or
- 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); or
- where the medical practitioner has reason to suspect unlawful activities or reasonably believes it is reasonably necessary for certain law enforcement purposes; or
- 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; or
- the use or disclosure is necessary for research or the compilation of statistics, is approved by a properly constituted Human Research Ethics Committee, 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, 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, for example, 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.

Where use or disclosure lessens or prevents a serious and imminent threat

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 able to be implied from the fact that the patient has sought a consultation with the new medical practitioner.

5.5 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.

Appendix A provides minimum procedures to assist compliance with this section.

Personal health information can be used within a practice for the purposes of medical research with the express 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 a Human Research Ethics Committee constituted in accordance with NH&MRC guidelines, and must comply with that committee's requirements.

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

The legal and ethical principles governing medical research using human subjects make it clear that the consent of the research subject 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, express 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.

6.1 When to obtain Human Research Ethics Committee approval

Although the Commonwealth Privacy Act only requires approval to be obtained from a Human Research Ethics Committee (HREC) in the case of medical research using personal health information without the consent of the patient, medical practitioners should 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 NH&MRC funding or is conducted by an organisation that receives NH&MRC 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.

Medical practitioners undertaking medical research should also be aware of and comply with other general guidelines applicable to medical research in Australia, which include the NH&MRC Statement on Ethical Conduct in Research involving Humans and the Commonwealth Therapeutic Goods Administration's Good Clinical Research Practice Guidelines.

Personal health information can be used for quality assurance 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; or
- the patient has given express consent for the use of personal health information for these activities; or
- the personal health information has been de-identified; or
- the activities involve research or the compilation of statistics, have been approved by a properly constituted Human Research Ethics Committee, and are conducted in accordance with that committee's requirements.

Quality assurance or continuing professional development activities involving the transfer of personal health information outside the practice should, in addition, 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.

Quality assurance and continuing professional development activities are essential to promoting and maintaining high quality health care. However, 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.

Notifying patients of quality assurance activities

Particular care must be taken with highly sensitive personal health information, where the patient may wish absolute confidentiality to be maintained. A patient recently diagnosed with HIV infection, for example, 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.

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.

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 6 of this Handbook (and in any event, for any minimum period prescribed by law).

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

- the patient has given express 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.

Measures for protecting the security of personal health information may include physical security (eg. locked filing cabinets, no unauthorised after hours access to the surgery), electronic security (eg. password protection, electronic audit trails, virus protection), and appropriate policies and procedures within the practice to specify who is entitled to have access to personal health information, and under what circumstances. 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.

8.1 Retention of records (time frames)

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 6 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. 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.

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 Care of records no longer required

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

8.4 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, express patient consent should always be sought before transferring personal health information outside Australia.

Appendix A provides procedures to assist compliance with this section. The examples are not exhaustive but are intended to assist medical practitioners achieve appropriate information handling practises.

9

Health 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 health 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.

Patient consent required where patient is identified

Where the health information enables both 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 health 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 health 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.

All medical practices must draw up and implement an 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 to the use or disclosure of personal health information by practice doctors, locums, registrars and other authorised health 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; and
- 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 are aware of appropriate procedures for handling personal health information.

Patients should be made aware of the information policy of the practice and should be entitled to see the policy on request. An outline of the policy could be included in a practice information leaflet.

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.

Appendix A provides procedures to assist compliance with this section.

General practitioners

Royal Australian College of General Practitioners

Best practice advice on health information management.

Website: www.racgp.org.au

Telephone: 03 9214 1414

General Practice Computing Group

Advice on improving your electronic information management.

Website: www.gpcg.org

Telephone: 02 6222 1300

Australian divisions of general practice

For advice regarding the management of health information by your local Division.

Website: www.adgp.com.au

Telephone: 02 6251 3380

Your local division of general practice:

Will be able to assist you with resources and information regarding best practice health information management and compliance with legislation.

Medical colleges

Contact your medical college

For referral and advice on privacy issues.

Australian and New Zealand College of Anaesthetists

Website: www.anzca.edu.au

Telephone: 03 9510 6299

Australasian College of Dermatologists

Website: www.dermcoll.asn.au

Telephone: 02 9879 6177

Australasian College for Emergency Medicine

Website: www.acem.org.au

Telephone: 03 9663 3800

The Royal Australasian College of Medical Administrators

Website: www.racma.org.au

Telephone: 03 9663 5347

The Royal Australian and New Zealand College of Obstetricians and Gynaecologists

Website: www.ranzcog.edu.au

Telephone: 03 9417 1699

The Royal Australian and New Zealand College of Ophthalmologists

Website: www.ranzco.edu

Telephone: 02 9690 1001

Royal College of Pathologists of Australasia

Website: www.rcpa.edu.au

Telephone: 02 8356 5858

Royal Australasian College of Physicians

Website: www.racp.edu.au

Telephone: 02 9256 5444

The Royal Australian and New Zealand College of Psychiatrists

Website: www.ranzcp.org

Telephone: 03 9640 0646

The Royal Australian and New Zealand College of Radiologists

Website: www.ranzcr.edu.au

Telephone: 02 9264 3555

Royal Australasian College of Surgeons

Website: www.racs.edu.au

Telephone: 03 9249 1200

Advice on compliance

Office of the Federal Privacy Commissioner

Website: www.privacy.gov.au

Privacy Hotline: 1300 363 992

Office of the Health Services Commissioner (Victoria)

Website: www.health.vic.gov.au/hsc

Telephone: 03 8601 5200

Community and Health Services Complaints Commissioner (ACT)

Telephone: 02 6205 2222

Office of the NSW Privacy Commissioner

Website: www.lawlink.nsw.gov.au/pc.nsf

Telephone: 02 9268 5588

Australian Medical Association

Email: privacy@ama.com.au

Telephone: 02 6270 5400

See: *AMA Practitioners' Privacy Resource Kit*

Appendix

Guidelines for security, storage and transfer of personal health information

Guideline procedures for handling personal health records, whether manual or computerised, are described under the major security requirements of patient consent, medical record quality, and disclosure of personal health information. Minimum procedures are provided, and also optional additional safeguards.

The appropriateness of a particular procedure may vary in different circumstances, but should be determined according to the general principles set out in these guidelines.

These procedures relate to personal health information as defined in the first guideline, but may equally apply to information that has been de-identified.

1. Patient consent

	Objective	Record type	Minimum procedures	Additional procedures
(i)	Patient consent is obtained and documented	Manual	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 any changed restriction	The practitioner provides an information sheet/consent for the patient to read and sign
		Electronic	Record in the patient's record their consent and any restrictions to this consent 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 any changed restriction	The practitioner provides an information sheet/consent form for the patient to read and sign

2. Medical record quality

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

3. Disclosure of personal health information

	Objective	Record type	Minimum procedures	Additional procedures
(i)	Patient has consented to third party disclosure	Manual	Ensure that patient consent has been obtained	Develop and use proformas for recording data
		Electronic	Ensure that patient consent has been obtained	<p>Establish an on-screen prompt for obtaining consent prior to disclosure</p> <p>Establish a default condition of 'no consent'</p>
(ii)	Transfers and disclosures are authorised by the medical practitioner	Manual	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	
		Electronic	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	Medical practitioner reviews audit trail of all transferred data ensure appropriate authorisation was given

3. Disclosure of personal health information (continued)

	Objective	Record type	Minimum procedures	Additional procedures
(iii)	Personal health information is de-identified when necessary	Manual	<p>The medical practitioner or authorised person should manually delete or mask any identifying data in records</p> <p>Assign patient identification numbers using, for example, randomly generated identifiers. (Do not base identification numbers on patient identity. Examples of unacceptable numbers include those based on birth dates or Medicare numbers)</p>	
		Electronic	<p>Identifying fields must be capable of deletion or masking prior to disclosure</p> <p>Assign patient identification numbers using, for example, randomly generated identifiers. (Do not base identification numbers on patient identity. Examples of unacceptable numbers include those based on birth dates or Medicare numbers)</p>	Ensure software program de-identifies all personal health information transmissions where appropriate
(iv)	Authorised disclosures of personal health information include only necessary information	Manual	The medical practitioner or authorised person should mask or delete unnecessary information, eg. reformat records.	Flag sensitive records
		Electronic	Establish a prompt to withhold information, and/or procedures to ensure only necessary data is selected prior to transmission or release of data	<p>Establish a classification system to assist identification of levels of data</p> <p>Link authorisation and access controls to this classification system</p> <p>Establish a mechanism to block or mask unnecessary information</p>
(v)	Only authorised people have access to personal health information	Manual	<p>Hold records in an area that is not readily accessible to people other than medical practitioners and authorised practice staff</p> <p>Locate facsimile machines, printers and documents etc. in an area not readily accessible other than to medical practitioners and authorised practice staff</p> <p>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, held in locked car, or stored in a secure off-site location</p>	<p>Store records in a locked room or secure filing cabinet</p> <p>Use physical or electronic locks for after hours protection</p>
		Electronic	Use at minimum a two-level logical access control system, eg. with user ID and password. 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	<p>Use physical or electronic locks, cards, fingerprint readers etc.</p> <p>Periodic review of log of computer access and data transmissions</p> <p>Periodic compliance audit with security procedures</p>

3. Disclosure of personal health information (continued)

	Objective	Record type	Minimum procedures	Additional procedures
(v)	(continued)	Electronic	<p>Terminals displaying medical data should not be accessible to unauthorised persons</p> <p>Communication controllers/modems should be subject to controlled use eg. password protection or units left 'off' except when authorised transmission occurs</p> <p>Permanent internet connections (eg. ADSL or cable modems) require additional security, eg. a firewall</p> <p>Restrict the performance of sensitive functions, such as transmission, to authorised personnel</p> <p>Ensure hard copies of personal health information are not accessible to unauthorised persons</p> <p>Locate facsimile machines, printers, documents etc. in an area that is not readily accessible other than to medical practitioners and authorised practice staff</p> <p>Records taken outside the practice, eg. for home consultations, should be held under the direct control of the medical practitioner. Eg. laptops and backup media should be securely carried, held in a locked car or stored in a secure offsite location</p> <p>Ensure backup copies of patient medical data are not accessible to unauthorised persons</p>	<p>Use dial-out only or dial-back modems</p> <p>Restrict availability of modem numbers by using silent numbers</p> <p>Authenticate remote users, senders and receivers of data by, for example, hardware or software authentication of valid terminal/user</p>
(vi)	Records awaiting disposal are not accessible prior to destruction	<p>Manual</p> <hr/> <p>Electronic</p>	<p>Shred or dispose of records using a secured disposal system</p> <hr/> <p>Dispose of records using a secure disposal system</p> <p>Delete records and any copies that are held on tape, diskette or other media as appropriate</p> <p>Reformat or destroy all disks prior to disposal, ie remove data. Note: deleting data does not necessarily destroy it</p>	
(vii)	Personal health information remains confidential	<p>Manual</p> <hr/> <p>Electronic</p>	<p>Ensure that persons authorised to access data maintain confidentiality. For example, they should understand and sign confidentiality agreements</p> <hr/> <p>Ensure that persons authorised to access data maintain confidentiality. For example, they should understand and sign confidentiality agreements</p>	<p>Store sensitive data in a secure location with restricted access, eg. in a locked cupboard within the practice</p> <hr/> <p>Use encryption to securely store sensitive data</p>

3. Disclosure of personal health information (continued)

	Objective	Record type	Minimum procedures	Additional procedures
(viii)	(continued)	Manual	<p>Store personal health information in a secure area and return it to the secure location after use</p> <p>Number any loose pages and on each page identify the patient</p> <p>Ensure off-site storage is secure</p> <p>Transfer copies of documents, not the originals</p> <p>Establish a tracking system to monitor the location of records at all times. Records in use could be replaced with a sheet indicating date of removal and who has possession. This is particularly appropriate when records have been removed from the practice (eg. home visits, legal matters, reports or permanent external storage)</p> <p>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</p>	<p>Store critical paper records in a fireproof cabinet</p> <p>Ideally records should be retained forever</p>
		Electronic	<p>Establish a formal policy for data backups, eg. daily backups of all data or changes; weekly backups of the entire system; and a 4-week rolling cycle of backups</p> <p>Ensure data backups are performed by adequately trained personnel</p> <p>Establish secure offsite data storage facilities</p> <p>Regular data backups should be stored in a protected and fireproof location accessible only to authorised personnel</p> <p>Use off-site storage for data and software backups by means of physical transfer or electronic download</p> <p>Perform regular (monthly) test restores</p> <p>Securely retain old software and ensure you have hardware that supports access to these files, to allow ongoing access to any older data</p>	<p>Automatically save data during input sessions</p> <p>Locate all computers with data a stored on their hard disks in physically secure area</p> <p>In order to duplicate data and provide greater security against loss, mirror data storage</p> <p>Use a secure third party to hold system source code</p> <p>Securely store backups in a fireproof safe</p>
(ix)	Data transmitted externally is complete and accurate	Manual	<p>Use a secure method of transfer, eg. courier, express post or registered mail</p> <p>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, such as for critical incident reporting</p>	<p>Confirm that records sent have been received</p> <p>Ensure that all pages were transmitted and to the correct number, by checking fax transmission reports</p>

3. Disclosure of personal health information (continued)

	Objective	Record type	Minimum procedures	Additional procedures
(ix)	(continued)	<p>Manual</p> <p>Establish an audit trail of transmissions, including recipient, date, time, and records handled</p>		
		<p>Electronic</p> <p>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</p> <p>Establish error reporting to identify failed or incomplete transmissions</p> <p>Establish an audit trail of transmissions, including recipient, date, time, and files handled</p>		<p>Confirm that data has been received by the intended receiving party</p> <p>Confirm that data has been received by the intended receiving party</p> <p>Establish an electronic signature check of transmitted files, eg. Public key infrastructure (PKI) to ensure messages are confidential, authenticated, integrity is maintained, and cannot be repudiated</p>
(x)	Transferred data remains confidential	<p>Manual</p> <p>Identify the intended recipient on all data transmissions (mail/fax/courier etc.)</p> <p>Mark all transmissions 'confidential'</p> <p>Use a cover sheet for all faxes</p>		<p>Use voice messages where the medical practitioner is satisfied as to the authenticity of the receiving party</p> <p>Obtain confirmation from the receiving party that the data has been received and is secure</p>
		<p>Electronic</p> <p>Prior to transmission, verify the receiving party, either manually or by computer</p>		<p>Use dedicated lines over provider (local or wide area) network where all nodes are authorised</p> <p>Use data encryption, eg. PKI to ensure messages are confidential, authenticated, integrity is maintained, and messages cannot be repudiated</p>