AMA

Privacy Resource Handbook

For all Medical Practitioners
in the Private Sector

Published by AMA, Canberra, 2010

Disclaimer:
The AMA has made every effort to ensure that, at the date of publication, the information contained in this Resource kit is free from errors and omissions and that all opinions, advice and information drawn upon to compile it have been provided by professionals in good faith.

The information and recommendations contained within it are considered to be consistent with the law and applicable Guidelines at the time of publication. However, they do not constitute legal advice. The information provided is not intended to be comprehensive. Medical practitioners concerned about their legal rights and obligations in relation to Federal, State or Territory privacy legislation may wish to seek their own independent legal advice.

Foreword

The AMA supports overarching health privacy legislation.

In absence of such legislation at the Federal level, it is important that the application of general privacy laws to the health sector enhances – not hinders – the provision of quality health care.

We have worked closely with the Federal Privacy Commissioner to ensure that compliance with the privacy legislation and the guidelines is not at the expense of good clinical practice.

The aim of this Handbook is to provide doctors with a sound understanding of the National Privacy Principals (NPPs), making it easier to implement the changes required to comply with privacy legislation.

We also want to help doctors manage health information in an ethical and lawful way, consistent with the maintenance of high professional standards.

Effective two-way doctor-patient communication is crucial to obtain patient consent for the collection of patient health information for any subsequent use and any future disclosure of that information that might be needed for the patient's ongoing health care.

A better alignment of patient and doctor expectations will reduce red tape and limit the financial costs incurred in complying with the privacy legislation in the course of providing quality patient care.

In May 2008 the Australian Law Reform Commission completed a review of privacy law and in October 2009 the Commonwealth Government released its response. In this response the Commonwealth Government has indicated that it is planning to amend the Privacy Act 1988 to incorporate many of the changes recommended by the Law Reform Commission.

At the time of publication the Commonwealth Government had released for comment an exposure draft of proposed Australian Privacy Principles legislation. The AMA will update this Handbook to reflect these changes once they are finalised as well as any significant changes to the Privacy Act 1988.

Dr Andrew Pesce
Federal AMA President
July 2010

A GUIDE TO THE USE OF THIS RESOURCE HANDBOOK

The purpose of this Resource Handbook is to provide assistance to doctors in understanding privacy law.

The first section of the Resource Handbook is a brief introduction to the *Privacy Act 1988* and National Privacy Principles (NPPs).

The second section explains and summarises the NPPs. Some special areas of concern to medical practitioners are then highlighted and some new concepts are explained.

The third section deals with the practical application of the NPPs to a clinical practice and how doctors can comply with them in the course of carrying out best practice in a busy clinical setting. This section covers large and small medical practices, the employed and self-employed practitioner, medical research, medico-legal work, and clinicians moving between the public and private sector. This material is in question and answer form.

The fourth section provides "getting started" advice on privacy compliance, how to use the AMA's privacy kit material, how to develop a privacy policy to suit the needs of individual practices, and how to move from basic privacy compliance to best privacy practice.

The final section provides the AMA's Privacy Kit and sample forms. The NPPs are set out in full in the Appendix to this Handbook.

This Resource kit is not intended to be comprehensive and is not a substitute for a thorough reading of the privacy legislation, the NPPs and the guidelines. Its aim is to assist practitioners with their privacy compliance obligations and to develop their own privacy compliance policies tailored to suit the nature of their practice.

An Essential Message

If there is one overall message to doctors it is the need to ensure open and effective communication between doctor and patient. Effective communication will in turn ensure that the expectations of both doctor and patient are aligned, and that patients have knowledge of their privacy rights, know how their personal information will be managed, and know what they need to agree to if they are to receive prompt and holistic health care. Patients should be made fully aware of any health consequences that might flow if they exercise their right to withhold personal health information from their treating medical team.

The Federal Privacy Commissioner has issued general *Guidelines to the National Privacy Principles* as well as health specific guidelines entitled, *Guidelines on Privacy in the Private Health Sector* (the Health Guidelines) which outline the way in which the NPPs are to be applied. The Health Guidelines acknowledge that the health service provider's principal concern is the health care of the patient. Doctors should keep this in mind when applying the NPPs to the handling of patient information. Adherence to privacy rules is expected to enhance, not to hinder, patient care, the relationship of trust between doctor and patient, and the patient's confidence in the doctor. It is up to the individual doctor to exercise his or her best professional, ethical and clinical judgment to a standard reasonably expected of a competent and skilled clinician to ensure that the NPP obligations are met in a manner consistent with accepted medical precepts and ethics. The *Privacy Act 1988* (as amended), the Health Guidelines, the NPPs themselves and information sheets can be accessed at the Office of the Privacy Commissioner's website at www.privacy.gov.au.

Federal AMA's website at www.ama.com.au provides information to assist its members to become privacy perfect. In addition Federal AMA members with questions about the application of the privacy legislation can e-mail privacy@ama.com.au or contact their local AMA branch.

SECTION ONE
INTRODUCTION

Background

Federal Privacy Legislation

The *Privacy Act 1988 (Cth)* ("the Act"), applies to most of the private sector including all health service providers on and from 21 December 2001. The legislation is not health specific, and its focus is not only on the medical profession. The Act incorporates 10 National Privacy Principles (NPPs) that impose compliance obligations on private sector organisations in relation to the management of personal information held by them. For medical practitioners it means that they are:

- obliged to safeguard patient privacy and to give patients some control over the way information about them is handled,
- required to be open with patients, and
- generally required to provide patient access to the information held about them.

Federal privacy legislation was enacted to reflect the privacy principles developed internationally, and in particular, the Organisation for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980). It was enacted to bring Australia into line with many other countries, including New Zealand, Hong Kong, Canada and many European nations, and, as far as possible, to establish a nationally consistent approach to handling of personal information in the private sector across industries.

In the period since it was extended to private sector health providers in 2001, the Federal legislation has undergone some limited changes in response to the emergence of genetic information as a medical technology with ethical and privacy implications and a more concerted government response to the possibility of national emergencies. Nevertheless the day-to-day operation of the Act remains substantially unchanged.

Related State and Territory legislation

Understanding privacy legislation in Australia is made difficult by reason of the fact that there is existing State and Territory privacy and health records legislation that requires doctors to comply with specific health information management practices. Legislation in NSW, Victoria, and the ACT includes privacy principles that apply to private sector health services providers. In most respects those principles are similar to the National Privacy Principles in the Federal Privacy Act. But there are differences and, in a particular case, the difference may be significant. Because of the complexities of overlapping laws it is important to seek advice from your local AMA Branch or a legal practitioner if a contentious privacy issue arises.

E-Health Initiatives

Developments under the general heading of E-Health hold out the promise of significant health care benefits. However electronic storage and transmission of patients' health information has obvious implications for patient privacy. The Federal Government's initiatives in this area are being pursued with privacy and security as key considerations. Some changes in privacy legislation are also being considered.

National Emergencies

There are now special provisions of the Privacy Act that authorise wide-ranging exceptions to privacy obligations if the Federal Government declares a national emergency.

To whom does the new Federal privacy legislation apply?

Focus not on medical practitioners alone

The NPPs incorporated in the Act apply to all private organisations with an annual turnover in excess of $3m and to all private organisations that provide health services, irrespective of their size. *Health service* is defined in the Act to include persons who:

- assess, record, maintain or improve the individual's health;
- diagnose or treat the individual's illness or disability or suspected illness or disability; or
- dispense a prescription drug or pharmaceutical prepared medicine.

Thus, compliance with the NPPs is required by all private sector organisations that provide these types of services and health services that hold health information. This applies to the people and doctors who work within them, doctors practicing in partnership or alone, in private hospitals, aged care facilities and other private health facilities, and those who undertake medico-legal work. They also apply to VMOs who work in public hospitals and who retain health records in private clinics.

The National Privacy Principles (NPPs)

What are the NPPs?

These are the ten privacy rules contained in Schedule Three of the *Privacy Act* (the Act) that set out the minimum standard of compliance required. The NPPs are applicable across the board of private organisations and not designed specifically for health service providers. However they offer privacy protection to patients and balance this with the need for doctors to maintain doctor-patient confidentiality and to provide quality health care.

Application of the NPPs to clinical medical practices might pose some difficult ethical and legal dilemmas. Privacy decisions have to be made in conjunction with good clinical practice. Ethical codes of conduct may assist in resolving some of these dilemmas.

What do the NPPs cover?

The NPPs cover a wide range of information handling practices from collection to disposal of health information, including use and disclosure, storage and maintenance. It is important for medical practitioners to understand that the individual's consent is required for the collection of sensitive

information. All health and personal information that is collected in providing a health service is regarded as sensitive information.

Consent to collection having been obtained, there are then restrictions on how the information will be used (within the practice) and disclosed (to people outside the practice, such as others in the treating team), without the further consent of the individual.

The NPPs and the Privacy Commissioner's *Guidelines on Privacy in the Private Health Sector* cover:

- what comprises proper consent;
- what to tell individuals when their personal information is collected;
- what to consider before disclosing that health information to others;
- what details should be included in a health service provider's privacy policy;
- how to secure and store information; and
- the provision of access to individuals to personal information held about them, including their health records.

Compliance with the privacy legislation

Privacy and Confidentiality

Doctors might believe that, so long as they continue good clinical practice and respect patient confidentiality, they are not at risk of breaching the privacy legislation. For compliance purposes this is not necessarily so. Confidentiality underlies the doctor-patient relationship of frankness and trust. It forms an essential part of patient privacy. However, the concept of privacy is wider. It limits what information can be collected and how it can be collected. It includes a person's right to know what information is held about them, a right to access it, and to have some control over its use and disclosure to others. Importantly, it also entails an alignment of expectations between the doctor and the patient on how personal information will be handled. This gives rise to issues surrounding consent requirements.

Special areas of concern

Consent Issues

Fully informed and voluntary consent is required at the time of or as soon as practicable after collection of health information.

Consent is also required for the use and disclosure of information for purposes not directly related to that for which the information was collected.

When a doctor collects information directly from the patient during a consultation, consent is usually implied, so long as it is clear to the patient what information is being recorded and why, how it will be used and to whom it will be disclosed.

Consent might need to be in writing, particularly if consent is sought for the use or disclosure of health information for secondary purposes such as for medical research.

The patient is usually the person to give consent but in some circumstances it may be given by a parent or guardian on a patient's behalf.

There are occasions where the information collected from the patient is about another person, in which case the consent of that other person might be required.

Access to Medical Records

Patients have a general right to access all health information held about them. Some exceptions exist, eg where:

- It would pose a serious threat to anyone's life or health;
- It would have an unreasonable impact on someone else's privacy;
- The request is frivolous or vexatious;
- The information relates to existing or anticipated legal proceedings between the organisation and the individual and the information is the subject of professional legal privilege;
- It would be unlawful to provide access, or denial is authorised by law; and
- It might prejudice an investigation of possible unlawful activity.

Handling requests for access

Organisations need to develop a policy to outline how they will handle access requests. (See Section Five).

Patients do not have to give reasons for requesting access. However, the scope of the request may need to be clarified in order to provide appropriate access, which may not necessarily involve providing a copy of the whole of the patient file. The patient might only want to look at the notes during a consultation or may want copies of documents on their file. Generally a patient should be allowed access in the form requested. Patients cannot be required to make their requests in writing, though in some cases it may be prudent to request the patient to do so.

A patient's request for access should be noted on the patient's file and all requests should be referred to the treating doctor, and the request should be completed within a reasonable time, taking into account the patient needs, and should not ordinarily exceed 30 days.

Fees that can be charged

Patients should be made aware of the costs charged where the doctor's time or administrative costs are involved and of the alternative less costly forms of access to the photocopying of a large file. (See Section Three under *Access*).

Location of Patient Information

The Act does not concern itself with who owns the health records, but applies to individuals and organisations that hold personal and health information. In other words, who controls the records is the determining factor as to whether the records fall under the Act or not. It is possible for medical records as they move around to be covered by the Act at some times, and not at others. It is also possible that the same set of notes can be shared by a number of people, some of whom are subject to the Act and some who are not. To assist in understanding this movement of records, consider the following situations.

- A doctor who works for a state/territory health organisation and bills public patients – the medical records held by the public entity, and are exempt from the Act but may be subject to relevant state/territory privacy or health records legislation.
- A doctor who works at a state/territory health organisation and with a right to see private patients – the medical records are held by the doctor and subject to Act.
- A doctor who works at a state/territory health organisation and bills public patients, but takes copies of patient information back to their private rooms – the medical records held by the public entity are exempt from the Act but are subject to any relevant state/territory health records or privacy legislation. However, once the doctor takes possession of a copy of the records then those records are subject to the Act.
- A doctor who works in private rooms and bills patients privately – the medical records are covered by the Act.

If there is any doubt as to the control of any patient records, a doctor in private practice should comply with the Act.

What are the consequences of non-compliance?

The Privacy Commissioner's powers

The enforcement process is generally complaint driven. The Federal Privacy Commissioner has no judicial powers. However, that office has wide powers of investigation. The approach to enforcement is one of conflict resolution. At first instance the individual complaint is to be made to the organisation or doctor. If it is not resolved at that stage, the Commissioner may investigate. The Commissioner can dismiss a complaint at any stage. If the Commissioner finds that a breach has occurred, the Commissioner can make an enforceable determination that the conduct is not to be repeated, that the doctor or organisation should do 'any reasonable act' to redress loss or damage suffered, and that a specific amount of compensation be paid. If, for example, the inadvertent disclosure of a patient's HIV status found its way to an employer, and the individual was sacked, a large damage award could result. Such a worst scenario is unlikely, and the Commissioner has vowed to tread softly in the first year of the operation of the legislation taking into account the effort an organisation has made to develop and implement a privacy policy in accordance with the legislation. However, the inconvenience, embarrassment and cost of investigation to a doctor that arises from an investigation should not be underestimated.

Medical Indemnity cover for privacy breaches

Doctors are advised to check whether their professional medical indemnity arrangements cover awards and/or the costs of investigations and representation.

Do doctors need to have a complaint handling process?

Yes. In the majority of cases the matter should be able to be resolved to the patient's satisfaction by simply discussing the issues with the patient. Only on failure of that process will the Commissioner look into a complaint. An investigation could be time consuming and costly to the practice.

What should doctors do if the Privacy Commissioner investigates them?

Doctors are advised to obtain their own independent legal advice and/or notify their MDO. In addition, AMA members are invited to notify the Federal AMA office of any investigation by the Commissioner. Doctors and their staff should comply with any direction given by the Commissioner, as monetary fines or imprisonment may result from non-compliance (see Section 46 of the Act).

Section Two
The Privacy Legislation

Explaining the National Privacy Principles

The National Privacy Principles (the NPPs) incorporated into the Act are the privacy rules to be followed by the private sector. They set the minimum standards for privacy that organisations must meet. They are summarised below.

NPP 1 - Collection
This principle sets out what a person has to be told when information is collected about them. As applied to a doctor or any provider of a health service, and taking into account NPP 10 (sensitive information), the NPPs require:

- A person's consent in order to collect health and other personal information about them
- Collection only of information necessary to deliver the health service
- Collection to be fair, lawful and not intrusive
- A person about whom personal information is collected to be told:
  - the name of the organisation collecting their information and its contact details,
  - why their health information is being collected,
  - how it will be used,
  - to whom it may be given, and
  - that they can access information held about them if they wish.
- A person to be informed of the main consequences, if any, if the person does not provide all of the information requested.
- Collection to be primarily from the person, but where collected from other sources eg. X-rays or specialists' reports, the person should be informed of this.

> ***Note: Taking of family histories without family members' consent***
> *As information is often collected from patients about others in the course of taking a family or social work history, good clinical practice would be hindered if NPP 1 and NPP 10 had to be strictly complied with. In recognition of this, the Federal Privacy Commissioner has issued a Public Interest Determination (PID), which remains in force until 10 December 2011. It applies to private sector health care providers generally. The PID relieves health service providers from the obligation of obtaining the other person's consent, and explaining to them how the information about them will be handled when taking histories from a patient.*

NPP 2 – Use & Disclosure

This principle sets out how health information once collected can be used (in your practice) and disclosed (to others outside the practice, say members of a treating team), and the consent requirements for such use and disclosure. A health organisation should only use or disclose information:

- for the 'primary purpose' (and there is to be only one such purpose) for which it was collected; or
- for directly related secondary purposes which are within the person's reasonable expectations; or
- for use and disclosure for which the person has given consent,
- unless other provisions under NPP 2 relating to the public interest, such as law enforcement and public or individual health and safety, apply.

Thus, once personal information is collected, the patient's further consent is generally required for its use and disclosure unless the information is being used or disclosed for the main reason it was collected or for another directly related purpose if the person would reasonably expect this.

This is perhaps the main concern for doctors who need to share patient information with treating teams, some of whom don't see the patient at the time of collection to get consent or discuss purposes of disclosure.

The problem is compounded by the Privacy Commissioner's narrow view of a medical practitioner's primary purpose of collecting personal information. The Privacy Commissioner has taken the view that the collection of information has to pertain to the particular episode of diagnosis or treatment. 'Primary purpose' does not extend to the broad concept of health services as caring for a patient's general health and well-being.

Patient understanding of the purpose of collection is therefore crucial. If the main purpose is for treatment disclosure, for example, medical research is a secondary use. Obtaining informed consent to collect information for a holistic approach to patient care – that is care not restricted to the immediate circumstances, but for the patient's general health - can obviate the need to obtain consents for handling the same information on subsequent occasions. It is therefore important for efficient clinical practice that doctors clearly identify the primary purpose of collecting information and align their expectations with that of the patient.

NPP 3 – Data Quality

This principle sets standards for keeping health information accurate, complete and up-to-date. Good clinical practice requires this. Doctors are now obliged to take reasonable steps to ensure this is done.

NPP 4 – Data Security

This principle sets standards for protecting and securing health information from loss, misuse and unauthorised access. Again, health service providers must take reasonable steps to achieve this. Paper and electronic records must be properly secured, safely stored and maintained.

This includes safe disposal of data no longer in use. The safe disposal of lap top computers, for example, must take into account the retrievability of deleted electronic data on it. The safe daily disposal of waste paper bins must take into account identifiable health information on paper scraps. Doctors are probably doing this responsibly, but with the development of e-health their records might need to review and upgrade their security measures.

NPP 5 – Openness
Health service providers must develop a policy document that clearly explains how the organisation handles health information and make the policy available to anyone who asks. This is a new compliance obligation, help with which is provided in this resource kit in Sections Four and Five.

NPP 6 – Access & Correction
Generally speaking, individuals have a right to access their own health records and a right to have information corrected, if it is inaccurate, incomplete or out of date. This right includes access to factual and opinion material, including specialists' reports whether or not a report states that it is not to be shown to the patient without the specialist's consent. This is a new legal requirement effecting a change in practice, and requires new understanding and procedures.

Access can be restricted or denied in certain circumstances specified in the Act, for example, where access might cause serious harm to a person's life or health.

NPP 7 – Identifiers
Generally speaking, an organisation must not adopt, use or disclose Commonwealth government identifiers, such as a Medicare or Veterans Affairs number, except for the purposes for which it has specifically been assigned.

NPP 8 – Anonymity
Where lawful and practicable, individuals must be given the option to interact anonymously. In the context of health care this is unlikely to have much applicability to doctors. Providing a safe health service, and for billing and rebate purposes doctors are required to record the identity of the patient.

NPP 9 – Transborder Data Flows
An organisation can only transfer personal information out of Australia to countries bound by similar privacy protection laws or schemes, unless the individual otherwise consents. This principle is to ensure continued privacy of patient information outside the jurisdiction of Australian law.

NPP 10 – Sensitive Information
An organisation must not collect sensitive information without the individual's consent, unless the collection is required by law, or falls within some specified limited circumstances. Health information is 'sensitive information'. Exceptions include circumstances:

- where the collection is necessary to prevent a serious and imminent threat to the life or health of an individual and the individual is physically or legally incapable of giving consent or is physically unable to communicate consent;
- where the collection is necessary for medical defence purposes or for the establishment of a legal or equitable claim
- where the information is necessary to provide a health service to that individual and is collected as required by law or in accordance with binding rules established by competent health or medical bodies that deal with professional confidentiality;
- where the information is collected for research relevant to public health or public safety where the purpose cannot be served by de-identification, obtaining consent is impracticable, and the information is collected in accordance with the law or approved rules of certain bodies or in accordance with guidelines approved by the Commissioner under section 95A of the Act for this purpose.

It is important here to note that:

Sensitive information means information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, or criminal record, as well as health information about the person.

Health information includes personal information collected to provide, or in providing, a health service.

Personal information means information or an opinion, including information or an opinion forming part of a database, "whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".

This means that consent of the individual is required before any information is collected in the course of providing a health service, unless it comes under one of the strictly defined exceptions.

Are the NPPs retrospective?

NPP 6 relating to an individual's access to information applies to information collected on or after 21 December 2001, and also to information collected before 21 December, which is referred to or used after that date. If compliance in giving access to old records poses an unreasonable administrative burden or expense, provision of a summary would suffice.

NPP 4 on data security, NPP 5 on openness, NPP 7 on identifiers and NPP 8 on anonymity also apply to information collected before 21 December 2001. Otherwise the rest of the NPPs apply to information collected after 21 December 2001.

SECTION THREE

COMPLYING WITH THE NATIONAL PRIVACY PRINCIPLES

All doctors in the private sector must develop and apply a privacy policy to comply with privacy legislation. How to 'get started' and attend to the practicalities that this implies is the subject of Sections Four and Five.

The purpose of this Section is to identify and consider problems that might be encountered by particular medical practitioners. The information contained in this section is provided in question and answer format, which may assist doctors in complying with their privacy obligations. The Questions and Answers cover:

- The issues surrounding the collection of information in the course of providing a health service
- Consent requirements
- The use and disclosure of collected information, including the sharing of information with other members of a treating team and for administrative purposes
- Consideration of 'primary' or 'directly related secondary purposes within the patient's reasonable expectation' and what are 'secondary purposes for which further consent is required
- The general right of patients to access information held about them
- Ownership of medical records, medico-legal concerns and transfer of medical records

Different consideration will apply depending on whether the practice is small or large, is a general or specialist practice, whether the practitioner sees their patients at the time of providing the service, and whether those who attend their patients provide a health service which allows them adequate opportunity for consultation before or after attending them, whether the practitioner moves between the public and private sector, and whether information might be required for research.

Collection

Do I need my patient's consent to collect their information?
Yes, but this is generally implied by the patient presenting for medical attention and giving the doctor the relevant medical history for that purpose. See also **Consent.**

There are exceptions to the requirement for consent, such as where it is necessary to deal with a threat to the life or health of an individual who is physically or legally incapable of giving the consent. The exceptions are set out in NPP 10.

What do I tell the patient about the information I collect?
The patient must be told and agree to the main purpose for which the information is collected. The main (or 'primary') purpose is a crucial concept under the Act, and has to be carefully considered by doctors when collecting health information from patients. Unless the doctor's and patient's expectations about the main purpose for which the information is required are aligned, a myriad of consents might be required for later use and disclosure of the information in the course of the patient's health care. See **Use and Disclosure.**

The patient has to be advised how their information will be handled. The patient should be informed that information will be collected, the purpose of collection, that they may access information collected about them, and to whom the information will be disclosed. General information about this can be set out in a patient information brochure or pamphlet (see Section Five for samples). If possible, the patient should be told how their information will be handled at the time of collecting the health information. Often, when the patient first sees their doctor, the advice can be given during usual communications. The patient might be handed an information sheet or pamphlet and also be given information orally during the consultation.

Can I collect information from other sources than the patient?
Collection should primarily be from the patient, but may come from other sources, for example, x-rays and specialists' reports. Sometimes information about a patient is volunteered from family or other sources. Unless it would be a serious threat to the life or health of any individual, the patient should be informed that information has been collected, the purpose of collection, that they may access the information and to whom the information will be disclosed.

Amendments to the Federal *National Health Act 1953* also allow health service providers to collect health information about a patient from the Prescription Shopping Information Service, without the patient's consent, as long as the information is necessary to provide a health service.

Can I collect information from other doctors about a patient without seeing the patient?
Radiologists, pathologists and in some circumstances anaesthetists often collect patient information either without seeing the patient, on attending them in circumstances not conducive to informing the patient about the collection, use and disclosure likely to occur in relation to their personal information. They sometimes might rely upon the diligence of the referring doctor to ensure collection of health information complies with the privacy legislation.

If the referring doctor has sufficiently explained the purpose of collecting a medical history at the time of taking it, and the patient understands that the information would be used for this type of ongoing health care, members of the treating team could reasonably proceed without the need for further specific consents.

Radiologists and pathologists, and other specialists might also comply with the Act by informing the patient of the way in which their information was handled, say, by including an appropriately drafted statement on the back of the patient's account. An example of such a statement is available in Section Five.

Can I collect information about other family members when taking a medical history?
While consent for this is required under the privacy legislation, the Federal Privacy Commissioner has issued a Public Interest Determination that exempts compliance with this requirement. For details of the exemption see **Family History Collection**.

Consent

Is it necessary or advisable to obtain written consent to collect information from patients?
The Act is not prescriptive. The doctor has to be satisfied that a person genuinely consents to the collection of their personal information.

Consent can be express, oral or implied. It is implied, for example, where a patient gives a medical history to the doctor when presenting for treatment. What is important is that the consent be voluntary and informed.

The signing of forms may not necessarily provide the assurance doctors would like. This because people sometimes sign forms without being aware of the nature of the form they are signing or why they are signing it, and may simply be assuming that they have to sign in order to obtain treatment.

The fact that a patient presents for health care and freely gives their information will generally be evidence of consent. The clinical notes usually tell the best story. If the doctor requires additional information, say for purpose of assessing whether any secondary problems exist, or for ongoing health care, and explains this to the patient, the patient's agreement should be noted at the time.

If this becomes the doctor's usual practice, then the notation can be brief, as later reference to it will show that the usual practice was followed. Contemporaneous notes usually provide the best evidence of what has occurred.

Where the doctor has any doubts, express consent should be obtained and noted. Consent forms are not obligatory, but may be necessary in some situations. Obtaining written consent is advisable, for example, where the use of patient information is requested for secondary purposes, such as scientific or market research. A sample consent form is provided in Section Five.

Do I need the consent of third parties to collect information about them in the course of taking a family or social history?
While this is required under the Act, the Federal Privacy Commissioner has issued a Public Interest Determination that exempts compliance with this requirement. For details of the exemption see **Family History Collection**.

Use and Disclosure

Can I release patient information to other doctors?
A patient must give implied or express consent for their personal information to be collected. Once the doctor has collected patient information it may be used or disclosed for the main reason it was collected or for another directly related purpose if the person would reasonably expect this. Otherwise, further consent is required for its use or disclosure.

If the main purpose of collecting patient information is to assess, diagnose and treat a patient, then the use or disclosure of that information to others in the treating team for that particular episode of care, is a directly related secondary disclosure that is likely to be within the reasonable expectation of the patient, and further consent is not required. This should have been explained to the patient at the time of the collection. On the other hand, its disclosure, say, for the purposes of medical research, is clearly an unrelated secondary use that requires patient consent.

Posing more difficulty is the situation where the information is to be used and disclosed for later episodes of care not in the patient's or doctor's mind at the time the information was collected. Further patient consent is required, unless the main purpose for collecting the information was at the outset agreed between the patient and doctor to be for the purpose of providing ongoing holistic care of the patient.

The main purpose of collection is therefore a crucial concept. Reaching an understanding about this with the patient when medical histories are being taken is essential. Otherwise the Privacy Commissioner's narrow view of a medical practitioner's primary purpose of collecting personal information poses bureaucratic obstacles to efficient clinical practice.

It is therefore important that doctors obtain their patient's agreement to collect information from them for the broader purpose of caring for their health as a whole, if that accords with their general practice, and ensure that they have aligned their expectations in that regard with those of the patient. Further consent is not then required for the consequent sharing of information with other doctors in the course of caring for the patient's health needs.

Can I share patient information in multi-disciplinary medical teams?

The multi-factorial nature of some medical conditions, such as psychiatric disorders, usually requires multi-disciplinary involvement with management and hence communication between various organisations for whom the involved health professionals work. The need for consent at each and every instance of 'extra-organisational therapy' is impractical and can be avoided if at the outset the patient understands, and consents to the sharing of information between the treating team for the holistic care of the patient.

The doctor-patient relationship is not a 'series of isolated incidents', but a holistic link dependent on frank exchanges. Having to seek consent for every information usage should not be the default situation. Doctors need to align the expectations of patients with their own as to what is being done with information. Then the patient can say "I don't want so and so to know about this", and the doctor can note the restriction placed on the use of the notes.
Dr Trevor Mudge, former Vice President of Federal AMA

Can I record patient information on a Medical Register?

If a doctor suggests a diabetes test and the patient agrees, then consent to collect relevant information about this condition is implied. The use to be made of the information and to whom the information is likely to be disclosed and why, should be explained at the time of collection. The information, once collected, can be used (within the practice) and disclosed (outside the practice) say to other members of the treating team in the event that treatment for the condition is required.

However, an issue arises as to the recording of patient health information on medical registers, such as diabetic's registers. Although recall/reminder systems are directly related to the patient's health, if registers are used for this purpose, as the information is being recorded somewhere other than on the patient's file, and particularly if the register system is to be used to facilitate government practice incentive payments, the purpose of the register should be explained to the patient. The patient's agreement is required if the register is held outside the practice, such as registers held by GP Divisions. The doctor should ensure that the patient agrees to the method of recall/reminder. That is, whether it is in order for a phone call to be made and a message left with the person who answers the phone, or a recorded message, or whether the reminder should be by way of letter only. Otherwise, an unlawful disclosure might inadvertently be made.

It is important to note that:

- General Practice Divisions and the Health Department can only use the information for the purpose for which it was collected by the doctor, and not for their own purposes, unless the information is de-identified, or consent is obtained.
- Doctors transmitting information electronically must ensure that it is encrypted.
- Unique identifiers, such as the Medicare numbers should not be used or disclosed unless required by Medicare or is otherwise necessary for purposes under the Medicare legislation.

Ideally, general practices might prepare a patient information sheet or pamphlet promoting its health prevention and care plan that sets out the practice's policy to provide patients with a recall/reminder system. The information should refer to the government practice incentive program and the practice's desire to ensure the privacy of its patients' personal information. It might go on to explain the minimum requirements of a health care program, the additional levels of care that might be needed, and the frequency of the care activities.

Can I disclose patient information to my Medical Defence Organisation?
Patients are more likely to reasonably expect this, if it is set out in an information sheet supplied to them. However, the Privacy Commissioner has acknowledged that doctors may be obliged to disclose patient information relating to adverse outcomes to their Medical Defence Organisation, insurer, medical experts or lawyers without the patient's consent.

Can I give patient information to a debt collector?
Names and addresses recorded by doctors form part of the patient's health information, and thus must be afforded the highest level of privacy. Generally, such information should only be used for the primary purpose of collection, namely to provide health care to the patient or for a directly related secondary purpose which is in the patient's reasonable expectation. Using the patient's name and address details for billing purposes, and for the purpose of chasing up non-payment, falls into the category of directly related secondary purposes within the patient's reasonable expectation. Patients would reasonably expect doctors to chase unpaid accounts. Thus it is permissible to disclose a patient's name and address to a debt collection agency to recover a bad debt.

Do I have to alter my office layout to comply with the privacy legislation?
Accidental disclosure of patient information can occur if discussions between the receptionist and patient can be overheard.

Most medical waiting rooms are set up in a fashion so that the receptionist can sit behind a counter behind which they work, take telephone calls, attend to approaching patients, and keep an eye on waiting patients. If for example, an ill patient had an epileptic fit, they could be appropriately assisted. Conversations can often be overheard. Some patients have hearing impairments, and speaking to them softly is not appropriate. To ensure no conversation is overheard would require substantial changes to waiting room layout and staff practices, to include a private interview room, and additional staff to ensure a person is in attendance in the waiting room at all time. This would be both inefficient and costly and such costs would inevitably be passed on to the consumer.

Doctors are expected under the Act to do their best to protect their patients' privacy without compromise to other patient needs, or incurring excessive costs.

Doctors should ensure the reception desk is high enough to protect patient information from unauthorised eyes, make staff aware of the need to position themselves in such a way that telephone conversations are not likely to be overheard and that unnecessary identification of patients about whom they are speaking is not made. Similarly, doctor's calling in their patients by name should refrain from extraneous comments about the patient's health. Patients might also be given the option of completing a form rather than answering questions asked by the receptionist.

Can I fax and e-mail medical information?
Faxing medical reports and health information, say to other members of a treating team, is permissible. It is important that the receiving medical practices ensure that the fax machine is secure and away from the public eye. In relation to the e-mailing of information, doctors should ensure that appropriate security safeguards are in place.

Can I leave telephone messages?
Unwitting breaches of patient privacy can occur by a medical practice leaving a message with a person or on an answering machine when a patient is not available. Medical practices should put a policy in place whereby no telephone messages are left that include sensitive information, unless that is authorised by the patient on a case by case basis.

What are my obligations when I have to disclose information without the patient's consent?
If disclosure is permitted or required by law, for example, the notification of a communicable disease, where practical the patient should be informed of that having occurred. Doctors are required to keep a register of disclosures made to an authorised enforcement body (see NPP 2.1(h)).

Access

How should a request for access be handled? Should it be made in writing?
A patient can not be *required* to put a request for access in writing. Medical practices should develop a policy for the handling of access requests, which could be set out in a patient information pamphlet that can be given to patients who have complicated access requests. A patient can be asked to put their request in writing. However, most requests are likely to be simply satisfied, say, by the doctor's explanation of some medical information, or the provision of a copy of a test result after the patient has discussed the result with the doctor. If the patient is asked to make the request in writing an access request form should be provided. The written request should be placed, and an oral request noted, on the patient's file. All requests should be referred to the doctor who is likely to want to go through the patient's notes to ensure that nothing in them is likely to cause serious harm to the patient, or anyone else, or unduly infringe someone else's privacy. The nature of the access required and the cost to the patient of the type of access requested should be explained in advance.

Can I ask a patient why they require access?
Patients do not have to give reasons for requesting access. However, the scope of the request may need to be clarified in order to provide appropriate access, which may not necessarily involve providing a copy of the whole of the patient file. The patient might only want to look at the notes during a consultation. They may want to take some notes of their own, or have a copy of a particular report.

Do I have to provide a copy of my whole medical file on that patient?
As to what form of access is to be provided to patients, common sense and proper doctor/patient communication applies. What the patient requires should be clarified, and the appropriate format in which it should be provided should be discussed. A patient may not want the whole of the record. They may be happy to receive a summary of the notes or of a specialist's opinion, or receive an explanation,

or simply want a copy of a test report. Generally access should be provided in the form requested. That may mean providing a copy of the document or documents containing the information, rather than just an opportunity to view the file or to attend for a consultation about the information. It is not sufficient to provide illegible notes or incomprehensible computer print outs. The cost of any elaboration or rewriting should also be made clear prior to providing the documents to the patient.

How long do I have to process an access request?
Access requests do not have to be responded to immediately. Doctors should take the time required to go through the notes to ensure that access is not likely to cause serious harm to the patient or some other person and that test results and so forth have been discussed in a clinical situation with the patient. Access requests should be met within a reasonable time, taking into account the patient's needs. In general an access request should be met within 30 days.

How much can I charge to provide access to a patient?
Patients cannot be charged application fees to lodge a request for access, or for legal advice obtained by the doctor relating to a request for access. They can be charged a reasonable fee to cover administrative costs, the costs of photocopying, retrieving information, etc. But that work should be done by administrative staff and charged accordingly. The doctor's time taken in perusing the notes or explaining them to the patient, or rewriting incomprehensible records can be charged at the doctor's usual consultancy rate. The cost cannot be charged to Medicare or to health funds. However, if the patient is seeking an explanation of, or access to, limited information as part of a normal medical consultation, then it may be appropriate for this to be given during the consultation in accordance with good clinical practice, and included as part of the normal consultation time and cost.

What the doctor and patient may consider to be a reasonable cost for complying with the request for access may differ. Guidance can be sought from other relevant legislation, that provides for photocopy costs, such as might be contained in Freedom of Information or Health Records legislation.

The costs that may be charged for providing access to information, is a matter that can be specified in the practice's Consent Form and Access Request Form. That one way of ensuring that there are no unpleasant surprises that may lead to a request for access becoming contentious.

In each case, discussion should take place between the doctor and the patient to ascertain the scope of the request for access, and to discuss the costs involved. In some cases allowance may have to be made for the patient's capacity to pay.

Do I have to provide access to medical records created before 21 December 2001?
There is a difference between records created prior to 21 December 2001 and those created after. The Act generally applies to information collected on or after 21 December 2001. However, there is a retrospective aspect to the access provisions. That is, any personal information collected before that date that is still in use forms part of the post-21 December 2001 record, to which the patient has access.

Past records are 'still in use' if they relate to a condition still being treated, or they are referred to in the course of continuing health care. This applies to records used within the practice (referred to by the doctor) or disclosed (to specialists or others outside the practice), whether they comprise factual or opinion information. If providing access to past records causes an undue financial or administrative burden, then a summary of the relevant part of the records will suffice.

There is therefore no obligation on a doctor to provide access to a patient of past records not in use. However, a request for access to these records should be handled in accordance with good clinical and ethical practice.

Can a parent always get access to their children's medical records?
The Act does not specify an age at which a child is considered of sufficient maturity to make his or her own privacy decisions. Doctors need to address each case individually, having regard to the child's maturity, degree of autonomy, understanding of the relevant circumstances and the type and sensitivity of the information sought to be accessed.

In the case of a baby the circumstances are likely to be rare where there are real concerns for the child's health that can't be disclosed to the accompanying parent or which did not warrant outside intervention.

In the case of a young teen, the doctor might quite properly take the view that access to the records without the child's consent would be a breach of confidentiality. The request for access should then be treated as a parental request for disclosure, and denying the parent access requires no reason other than confidentiality having to be maintained.

NPP6.3 should also be noted. That is, where grounds exist to deny access, consideration should be given to whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

However, if a doctor suspects that **parents are using the child's health for their own domestic purposes**, the doctor will need to ask the accompanying parent which parent is entitled to receive information about the child. If the matter can't easily or quickly be resolved and the child has health needs that require attention, it would be prudent to advise the absent parent of the disclosure necessarily made to the accompanying parent. A doctor should assess each situation in a clinical and privacy context.

Can a GP provide a patient access to a specialist's report contained on their file?
Patient access to a GP's medical records includes access to specialists' reports on the GP's files, notwithstanding that they may be marked "not to be released to the patient". A notation "not to be released to a third party without my permission" is also to be ignored if the patient authorises the release, or the law requires it. However, specialist notation of this kind may alert the referring doctor to something in the report that might cause serious harm to the patient or another person, and thus provide a reason for restricted release. Otherwise the specialist's consent to patient access is not required.

The specialist retains copyright over reports he/she writes and the opinions contained in them. Simply referring the patient to the specialist who is the author of the report is not an advisable course. A specialist has more reason to refer the patient to the GP, who is generally better placed to assess whether the release of the report is likely to cause serious harm to the patient (or another person) – the main reason under the Act to restrict access to health information.

Can I restrict patient access to mental health notes?
Some GPs and specialists such as psychiatrists collect information during counselling sessions and make process notes that often includes, intimate notes of an interactive doctor/patient relationship. The therapeutic process often requires a verbatim record of a patient's account of events that involves other people, and indeed the doctor, that are not necessarily accurate.

Where access to the notes is requested, doctors should consider issues such as, whether providing access would pose a serious threat to the patient or to any other person, or whether providing access would have an unreasonable impact upon the privacy of another, including the doctor.

Other means of providing access than copying the complete notes may be considered, including the provision of a summary report. However generally access should be provided in the form requested.

A psychiatrist or psychotherapist might find it helpful to let patients know in advance (or in a patient information pamphlet) that most of the material collected from the patient will be in the form of psychotherapy 'process notes', rather than factual material, and that it is often the case that patient access to such notes is restricted on the grounds that access and correction of the notes might impede the therapeutic process and cause serious harm to the patient. It could be explained that a summary only of this material is usually provided in response to a patient request for access. Up front open communication with patients is to be encouraged. However, no agreement should be reached to this effect as a matter of course as, in the event that a patient does insist on a full copy of the notes after being offered a summary, then the situation ought to be revisited to see if a restriction is warranted under the Act.

Do I have to give immediate access to test results?

If a patient pre-empts a medical appointment and requests access to test results before discussing the report with the doctor the access should be deferred until the consultation has taken place. By way of contrast, if a patient asks for a copy of a report of say, 12 months ago, after appropriate clinical interventions have occurred, the practice's procedures for access requests (which may still include reference to the doctor) should be followed.

The Quality Use of Pathology Committee (QUPC) has given consideration to how pathologists should handle a situation where a patient demanded test results which the referring doctor, their GP, had withheld.

The QUPC protocol takes account of the fact that doctors are not expected under the legislation to hand over "raw" notes and results immediately upon being asked. The QUPC recommends:

- Consult the referring doctor, since the GP is best placed to interpret test results to the patient, in the context of clinical history. There are certain conditions where it could cause life-threatening harm to release uninterpreted test results to a patient, a valid reason under the NPPs not to release the information.
- Having contacted the referring doctor to ascertain why test results were being withheld, the pathologist should give the patient a written response, explaining why results are being reserved if he or she concurs with the patient's GP. A copy of the response should go to the referring doctor.
- If the GP has not had the opportunity of discussing the results, the patient having pre-empted the appointment, then the specialist can tell the patient that access to the test results will be deferred until after that appointment.

Family History Collection

Do I need the consent of family members when taking a family history?
Best clinical practice requires collecting a full family and social history from patients.

NPP 10.1 states that 'sensitive information' (which by definition includes all personal information collected for the purpose of providing a health service) about an individual is not to be collected unless the individual has consented. This causes difficulties for doctors taking family or social histories from patients without the consent of relevant family and other third parties.

The Privacy Commissioner has addressed this by issuing a Public Interest Determination (TPID) of 6 December 2007 (which is in force until 10 December 2011) which declares that no organisation is taken to contravene NPP 10.1 if health information is collected by a health service provider from a patient about another person ('the third party') in circumstances where:

(a) the collection of the information relates to the patient's social, family or medical history and is necessary for the health service provider to provide a health service directly to the patient; and

(b) the third party is a member of the patient's family or household or the third party's information is otherwise relevant to the consumer's family, medical or social history; and

(c) the health service provider obtains the information without the consent of the third party.

The Determination provides that in that situation the public interest outweighs the interest in upholding the third party's privacy.

The PID focuses on family histories, but it also covers personal information taken from patients about non-family members, recorded in the context of the patient's relevant interpersonal relationships. Thus, GPs, psychiatrists, and other mental health practitioners who may be treating stress, anxiety conditions and other mental health issues can safely record verbatim information about third parties in order to assess, diagnose, treat or care for a person's health.

Can I collect family and social history in order to produce a medico- legal report?
The PID is intended to allow doctors to collect family and social history in order to produce medico-legal reports. The terms of the PID allows this where doctors are carrying out medico-legal assessments (other than for the limited medico - legal purposes allowed by NPP 10.1(e)). Doctors are performing a 'health service' for the purpose of the Act in that they are assessing, recording or diagnosing an individual's actual or suspected illness or disability. The PID also applies where the health service provided is one of assessment only and where the doctor is commissioned by a third party where the service is not provided directly to the individual.

Copyright

Who owns my medical records – the doctor or patient?
The Act gives patients a general right of access to information held about them. It does not necessarily give a patient the right of ownership of that information. As a general rule the doctor who holds patient information owns and controls it. Doctors retain their legal rights in relation to copyright of their own work. Access to this information is a separate issue.

Included in the health information a doctor often holds about a patient are diagnostic notes, perhaps a medical protocol tailored to a patient's particular needs, letters written by the doctor, clinical notes taken about the patient, as to which the doctor owns the intellectual property rights. The copyright of specialists' reports held on a GP's file belongs to the specialist who wrote the report. The way in which the doctor takes notes, records patient management and so forth form part of the doctor's intellectual property.

The High Court case of *Breen v Williams* (1995) 186 CLR 71 confirmed a doctor's right in this regard. The courts have held that enactment of the Privacy Act did not alter that position (*Mid-City Skin Cancer & Laser Centrev Zahedi-Anarak* [2006] NSWSC 844). Thus, the granting of access to patient's of their medical information does not necessarily give patient's the right to deal with the information as they wish. It restricts doctors as to the way in which they are to use and disclose the patient's information, but also a patient's right to access their health information may be subject to restrictions as to its reproduction and use subject to the doctor's permission. In practice this would be hard to enforce or explain, and there is probably little reason to do it. However, in relation to medical reports it is important, because there is a question of ensuring that the doctor's opinion is not reproduced by someone for commercial purposes without the doctor's permission, and there is the question of the right to charge a fee for reports.

There is nothing to stop a doctor from asserting copyright over the material that indicates that the doctors' consent is required for further reproduction of the material. However, the doctor should ensure that this does not breach his/her ethical duty, by preventing relevant material being made available to another doctor or medical treatment team member.

Medico Legal Requests

Am I obliged to provide access to the patient of a medico-legal report?
The Act provides patients with a general right to access personal information held about them. Opinions expressed in medical reports prepared at the request of lawyers on behalf of clients form part of the health record to which the Act applies. The intellectual property rests with the author of the report. But, subject to certain exemptions, a person is entitled to know and see what information is held about them. Sometimes a person requests a copy of a medico-legal report written about them before the agreed fee for the preparation of the report is paid.

Three distinct situations must be appreciated:

1. Where a doctor, other than a treating doctor of the patient, is requested by a third party – say the insurer of a defendant to a legal proceeding – to prepare a medico-legal report. The patient's consent is required before the patient is examined by the doctor for the purpose of preparing the report. The report, commissioned by a third party, is the subject of legal professional privilege, and exempt from the access requirements under the Act.

2. Where a third party commissions the report – say for insurance purposes rather than for legal proceedings – where no legal professional privilege applies. The patient is, subject to other restricted exemptions under the Act, entitled to access that report. Doctors might be concerned that a patient might then use the report for other unrelated commercial purposes – for pending litigation, or for some other commercial purpose such as to obtain a pilot's licence. While under the Act the doctor is not entitled to ask a patient why access is required, in the case of a medico-legal report, it is reasonable for the doctor to assert copyright over it. In that event the doctor can provide access on the condition that the report not be further published or reproduced without the doctor's

permission. In this way the doctor can then ascertain whether the patient was attempting to use the Act to avoid paying the appropriate fee.

3. Where the treating doctor has been asked to provide a report for medico-legal or other commercial reasons, on behalf of the patient - though a commercial fee for the preparation of the report is agreed, the patient accessing the report through the Act could circumvent its payment. Where a doctor has concerns about this occurring, the problem might be avoided by the doctor asking for the agreed fee to be paid before the patient is examined and the report prepared.

The Federal Privacy Commission has plans to include in its public education program the need for the public to make sensible and honest use of the Act.

Doctors performing medico-legal assessments are performing a "health service" for the purpose of the Act in that they are assessing, recording or diagnosing an individual's actual or suspected illness or disability. They must, therefore, comply with the Act, but similarly are able to take family and other personal histories under the PID as it stands.

Should I forward medical records to a solicitor or a patient's agent?
While a doctor is not entitled to ask the reason why access is requested, it is appropriate to seek clarification of the request so that the nature of the access and the appropriate cost can be agreed. Where a patient seeks that their notes be forwarded to their solicitor it is likely that the material is to be used for medico-legal purposes. It is improper for lawyers to use the Act as a back-door method of obtaining access to medical opinions. It would be appropriate to ask the patient to clarify what part of the notes is required. The doctor then, as in every case where copies of the whole or part of a file are required, should go through the notes to identify any information as to which access should be restricted (such as information about other people collected in the course of history taking). Then, whether part or all of the notes are required, the doctor should request that the reasonable administrative costs incurred in the doctor reviewing the notes and the photocopying costs be paid before their release to the solicitor.

To whom can I disclose a report prepared for a commissioning agent?
If you are not the treating doctor, and you are commissioned by a third party, the report, if requested in anticipation of, or for the purpose of **litigation**, is the subject of legal professional privilege, and while the patient has no right of access to it, it can be disclosed to the commissioning party. The patient has consented to an examination and the report being prepared and would reasonably expect it to be used and disclosed for the purpose it was prepared.

If the report was commissioned for other purposes, say for production to a **Mental Health Tribunal**, or **Parole Board**, the disclosure is authorised or permitted by law, whether or not the patient has consented to the disclosure. Generally speaking, the patient is likely to be able to access the report.

In some states **Work Cover legislation** authorises the release of information to a statutory board and requests are made to doctors for information without providing the patient's consent. Generally, the patient having made application for some benefit under the Work Cover legislation covers the consent requirement. If the release of information is authorised by the relevant legislation, no further consent is required, but good clinical practice would surely dictate that the doctor should inform the patient of the request and of the fact that it has been met.

If an **insurance company** or **employer** commissions the report, so long as the person has given authority for the report to be prepared, then it follows that the report can be disclosed to the

commissioning agent, the purpose for which the material was collected. However, if an employer seeks information from a doctor to verify a sickness certificate, the doctor should obtain the patient's consent before dealing with this inquiry. Similarly, if a family member makes an inquiry as to whether of not a patient has made an appointment to see the doctor, this information should not be given without the patient's consent, if the patient has capacity or maturity it is up to them to make their own decisions about the management of their health information.

Transfer of Medical Records

I'm retiring – what do I need to do to with my records?

Where a practitioner retires and another doctor within the practice takes over responsibility for the patient's records of the retiring practitioner, it is appropriate for a circular to be sent out notifying of the retirement and to include notice that the records will be held by the nominated doctor in the practice. If that is not feasible, then it is appropriate to inform each patient as they contact the practice of the new arrangement so as to allow a patient the opportunity of having the records transferred to another doctor or practice.

If no arrangements can be made to transfer the records to another doctor, then suitable storage arrangements should be made so that they can be easily accessed if required, and the practices' phone number might have to be retained or redirected to ensure patients can be informed of the new arrangements.

A patient wants to change doctors –what am I required to do?

A doctor should always do what accords with best clinical practice and relevant codes of ethics, to ensure that all papers and records the new practitioner would reasonably require to adequately treat the patient are provided.

If the patient has requested the full medical file to be transferred, then the patient's wish should be met, with copies of the file being provided to the nominated doctor. The transferring doctor should retain all original documents on his/her own file and archive for medico-legal purposes.

The author of material on the doctor's file is irrelevant, as the practitioner who holds the material is responsible for complying with the request for access/transfer.

It may be appropriate to clarify the scope of the patient's request, to understand the needs of the patient and the new treating practitioner.

SECTION FOUR

MEETING COMPLIANCE OBLIGATIONS AND PURSUING BEST PRACTICE

Develop and adopt a privacy policy

The first obligation under the Act is to develop a privacy policy in compliance with the Act. For 'getting started' purposes, a medical practice might initially adopt the policy as set out in the sample patient information pamphlets in Section Five. The following steps should be undertaken:

1. Display a notice (perhaps by drawing on the sample poster in Section Five) in the waiting room informing patients that the practice has a privacy policy which complies with the privacy legislation and that more information is available about the handling of patient information on request. Make available an information sheet (or patient information pamphlets such as those set out in Section Five) to patients who request more information about the way in which their health information will be handled.
2. Conduct a privacy audit of the practice to see where deficiencies in compliance with the Act by the practice lie (see below).
3. Draw a *Act*ion *Plan* (see below) that addresses the deficiencies identified in your audit and that ensures ongoing improvement of your procedures, development of privacy policy and compliance with the Act.
4. Adjust the adopted privacy policy as required to ensure the policy reflects the particular procedures of the practice.
5. Nominate a person in the practice as privacy officer who is responsible for:
    - full implementation of the policy;
    - the handling of staff and patient privacy questions;
    - the setting up access request and complaint handling mechanisms; and
    - ongoing privacy compliance.

Implementation

Much of the compliance obligation is to ensure that a patient is aware of the practice's privacy policy and procedures for handling personal information. This can be achieved by carefully worded waiting room notices or posters, patient information sheets, and a practice privacy policy pamphlet. **Nothing, however, will be a substitute for frank and effective doctor patient communication**.

Poster and patient information pamphlets

To comply with NPP 5 – Openness - for 'getting started' purposes, the AMA has provided a poster, and two patient information pamphlets as to which either or both can be provided to patients who want to know more about how their information is handled (see Section Five). This material can be used by any practice after the insertion of the practice's details in space provided.

These documents have been designed to encourage patient expectation that information collected about them will be managed to facilitate a holistic approach to their health care rather than for the purpose only of 'episodic' care. Doctors should consider whether this approach suits their particular practice, or whether they should draft their own privacy policy tailored to suit their particular needs.

Practices might also want to expand the patient information pamphlets to include information that goes beyond privacy matters and provides other details about the practice.

Privacy audit

Take a look at the reception area:

- Can the risk of telephone conversations being overheard be minimised?
- What can be done to minimise the risk of patients being overheard when giving oral information?
- Are computer screens and patient records out of view of other people?
- Are screen-savers fitted to block unauthorised viewing?
- Is access to patient data restricted to those who require it?

Take a look at your consulting habits:

- Do you keep patient information – files, medical reports, mail or scripts bearing patient names – out of the view of other patients?
- Do you remove data displayed on a computer screen relating to a previous patient before the next patient comes in?
- Do you take care when taking telephone calls relating to a patient in the presence of another patient not to identify the patient when health information is discussed?
- Do you ensure that staff, registrars, students, non-treating doctors or nurses in training are not present during consultations without the prior permission of the patient?

Take a look at your existing forms for patient completion:

- Do they ask only for information necessary to be collected for the provision of the health service and associated administrative purposes?
- Do they state that the patient is not obliged to provide any information, and set out the consequences, if any, that may result if the information is not provided (e.g., that the service can not be provided).
- Do they require written consent to the collection of the information, and if so, is sufficient information provided to ensure that the patient's consent is fully informed, and are procedures in place to ensure that the consent is genuinely given.

Take a look at Patient Records

Are there procedures in place:

- For noting – say in red ink – on patient records any restrictions on access, use or disclosure?

- For noting when anyone else accesses sensitive information?
- For distinguishing between information collected before 21 December 2001, and that collected after that date, to reflect the different obligations that apply to access, use and disclosure?
- To review personal information regularly, and to securely destroy records no longer needed? Note that for medico-legal purposes, medical records may need to be kept for many years.
- Is it clear on the face of your forms which parts a patient is obliged to complete, and the giving of which information is voluntary?
- Do you intend to offer patients a form for completion for the purpose of an application for a copy of their medical records, and have you considered the issues surrounding this option?

Research and Quality Assurance Programs

Where research projects are conducted in the practice under the approval of an institutional ethics committee:

- Are staff aware of the requirement to obtain consent specified in the research protocol?
- Are consents properly obtained?
- Are patients informed when the practice is undertaking research and quality improvement activities?
- Are procedures in place to remove where possible identifying information from personal health information being used for research and quality assurance activities?

Disclosure and Complaint Registers

A medical practice should create a disclosure register to record disclosure of patient information made without the consent of a patient to an authorised enforcement body under NPP 2.1(h) in compliance with NPP2.2. It would be prudent to create a complaint register, so that if any unresolved patient complaint lead to an investigation by the Privacy Commissioner, an accurate record of the complaint and action taken can be produced.

Start a Practice Privacy Manual

Compile a manual of relevant information, index it, and make it available to all staff. It might consist of:

1. Full NPPs (see Appendix)
2. Health Guidelines accessible on the Privacy Commissioner's website at www.privacy.gov.au
3. Any useful fact sheets issued by the Privacy Commissioner, accessible on the above website
4. Other material produced from time to time for AMA members accessible on the AMAs website at www.ama.com.au
5. This Privacy Resource Handbook
6. Sample forms from Section Five or as developed by your practice from which further copies can be made as required
7. Yours practice's privacy policy, website policy, information pamphlets etc.

See also Tips on Developing Privacy Policy below.

Privacy Action Plan

Do you need to appoint a privacy officer?

There is no obligation under the Act to appoint a privacy officer and all staff need to be involved if best practice is to be achieved. The ultimate responsibility lies with the practice principals be they doctors or practices managers in a corporate structure. However, it would be prudent to consider nominating a person to be responsible for the ongoing activities related to the development, implementation, maintenance and adherence of the organisation's policies and procedures relating to the handling of patient information. This person may be a doctor, practice manager, receptionist or someone employed specifically to perform that function. The person chosen may depend on the size of the organisation.

The person should be responsible for:

- full implementation of the practice's privacy policy;
- the handling of staff and patient privacy questions;
- the establishment of procedures to handle access requests and complaints;
- the establishment of disclosure and complaint registers.

How to perform the functions of a Privacy Officer

(a) Familiarise yourself with the 10 National Privacy Principles ('the NPPs').

This resource kit contains relevant information about the NPPs and obligations. The Office of the Federal Privacy Commissioner has publicly released various summaries and health guidelines relating to the NPPs, which you will find useful.

(b) Conduct a privacy audit.

This is a review of your organisation's current practices to identify what information is collected, how it is collected, how it is used and disclosed and where it is stored. The results should be compared with the NPPs in order to identify the changes that you will need to make to your current practices to ensure compliance with the Act.

(c) Examine your security arrangements.

Ensure that information held by your organisation is protected from misuse, loss, unauthorised access, modification or disclosure. This can be done by making sure that your storage, transfer and disposal systems for both paper and electronic records are secure. Paper shredders should be used for daily waste. For assistance with security of computer systems, please see information on IT Privacy contained in this resource kit.

(d) Formulate and implement a privacy policy.

Each organisation must have a clearly written privacy policy, which is readily available to anyone who requests it.

By displaying the poster and using the pamphlets provided by the AMA, you have implemented a basic privacy policy.

These documents, however, contain general information only, and you will need to review and perhaps develop your own procedures in relation to the points contained in the documents.

You will also need to provide further information about the procedures used by your organisation in the implementation of privacy policy.

You may wish to develop a more detailed privacy policy. The Federal Privacy Commissioner has information sheets which will assist you in formulating a privacy policy that suits the needs of your practice.

The key issues to cover include the kinds of information the practice collects and holds, the reasons for holding it, how it is collected and used and who it may be disclosed to and why. The policy should underline the importance of consent to collecting and disclosing health information.

However a privacy policy cannot substitute for direct communication between the doctor and patient about the information the doctor needs, why and how it might be used or disclosed to others.

(e) Develop a procedure for resolving patient complaints about your handling of their personal information

- This should include establishing:
- An 'incident and complaints record' for recording complaints about the handling of personal information.
- A 'disclosure registry' for recording disclosures made to others required under or authorised by the law without the consent of the patient.
- These records will assist in the ongoing reviews of the organisation's practices to ensure adherence with the Act.

(f) Train staff about your privacy policy and their obligations under the privacy legislation.

All staff should be familiar with the organisation's privacy policy and procedures to ensure that there are no unintentional breaches of privacy. All staff should also be aware of the patient's right to access their own information, although there may be restrictions to access. Professional staff should also have an understanding of the concepts of 'primary' and 'secondary purpose' of collection in relation to patient consent for use and disclosure of their information. You may wish to provide staff members with copies of information in this resource kit of relevance to them.

(g) Staff confidentiality agreements.

It is advisable that all staff sign an appropriately drawn confidentiality agreement. This could be included in contracts of employment. It might include words to the effect of, '*I agree that I shall not, during the period of my employment or after its termination (however caused), disclose or use in any manner whatsoever any patient files, medical reports, or confidential knowledge gained through my employment with [name of practice]. I acknowledge that any*

such disclosure is in breach of privacy legislation'. A sample confidentiality agreement is provided in Section Five.

(h) Monitor ongoing privacy procedures to ensure compliance.

The privacy officer should regularly review and evaluate the organisation's privacy policy, and whether staff are complying with it. There may need to be changes to the policy or procedures as a result of the review, or perhaps as the result of a complaint or incident report.

(i) Consider the need for external advice.

Some organisations may require the assistance of external providers to:

- Conduct the privacy audit, develop policy and procedures, and assist in the ongoing adherence by staff; and / or
- Advice as to whether additional software should be installed that records your privacy policy and your implementation procedures, allows you to monitor its working, access checklists and conduct privacy audits.

Check the IT Privacy of the Practice

Privacy of health information applies to all communications, not just paper records.

Whether communicated or transferred via the telephone, facsimile machine or e-mail, and whether stored electronically, staff must maintain privacy and confidentiality. The following checklist, a summary drawn from ' *IT Security Guidelines for General Practitioner'*, offers a valuable compliance guide to medical practitioners and their staff. The full document is available from the General Practitioner Computing Group website at www.gpcg.org

IT Security Coordinator

- Practice has appointed and defined the role of an IT Security Coordinator
- Training in IT security has been provided to the IT Security Coordinator

Screen-savers

- Screen-savers are being used.
- Screen-savers are initiated automatically after a set time period of no PC activity.
- Screen-savers are used with the password protection option enabled.

Passwords

- The number of attempts allowed to enter an incorrect password is limited.
- Difficult to guess passwords being used.
- Passwords are changed if they become known to other people.
- Default accounts and passwords are changed before systems are used.
- Passwords are not written down unnecessarily.

- Passwords are not shared.

Basic security and PC guidelines

- Computer monitors are positioned to help maintain privacy.
- Staff log out of systems while away from PCs.
- Staff attend basic security awareness training.
- Policies and guidelines have been developed for the use of computing resources and distributed to all staff.

Backups

- There is a data backup process in place.
- Backup media is rotated before being re-used.
- Backups are periodically tested.
- Backup tapes or other media are stored securely or destroyed.

Anti-virus management

- Anti-virus software is used for all computers with automatic updates.
- Files from external sources are checked for viruses before being used.
- Anti-virus updates are obtained and distributed promptly when available.

Accessing the Internet

- There is a staff Internet usage policy and it is distributed to all staff.
- A stand-alone computer is used to access the Internet, alternatively, hardware and / or software firewalls are used between the internal network and the Internet.
- Modems are configured to dial-out on demand only.

Communicating by e-mail

- There is a staff e-mail usage policy and it is distributed to all staff.
- Confidential information is not sent by e-mail unless encrypted.
- E-mails are sent with a confidentiality and privilege notice.
- E-mail attachments are not opened from unknown senders.
- Work-related e-mail is handled, stored and disposed of in accordance with relevant legislation.

Access controls

- Access privileges are granted only on a ‘need to know’ basis.
- There is an access approval process.
- Access administration responsibilities are assigned.

- Access privileges are reviewed on a periodic basis.
- Contractors who require access to the system have signed confidentiality agreements.

Physical security

- IT equipment is stored in secure private areas of the practice.
- There are building security measures in place.
- Additional measures are taken for laptop/palmtop computers.

Disaster recovery / business continuity planning

- There is a Disaster Recovery Plan.
- There are maintenance and/or service level agreements in place for equipment and software.
- The plan contains business continuity and recovery procedures.
- A device with electrical filtering is used to prevent damage to hardware.
- Place, such as disk mirroring.

Commercial use

Protocols are in place to protect e-held data from exploitation by organisations that might sell it for commercial purposes.

Data disposal

Procedures are in place to ensure that data is removed, destroyed or cleansed once it is no longer required (particularly from floppy disks, hard drives, backup tapes, note-book computers and the like when they are no longer in use).

Information can be deleted "but still dangerous" where a computer itself is disposed of. Data can be recovered from computers despite efforts to destroy it. Information may not be visible on the PC but it remains in the hard drive.

Does your practice have a website?

The NPPs and the organisation's Privacy Policy and other terms and conditions for use of the website are to be clearly displayed in an obvious place such as boxes or tabs on the home page entitled 'Terms and Conditions of Use' and 'Privacy Policy'. If personal information is collected the website customer should be informed:

- Who is collecting their personal information.
- How their personal information is being used.
- How their personal information is stored.
- To whom their personal information is being disclosed.
- A sample website statement is contained in the Appendix in Section Five.

Tips on Developing a Privacy Policy

Consent to collection, use and disclosure of information
Consent by a patient to the collection of personal information by a medical practice is generally implied by the patient's request for a medical service. However, consent to the use and disclosure of that information is required if it is to be used and disclosed for any broader or other purpose than the main purpose for which it was collected (or any directly related purpose and within the reasonable expectations of the patient). Where information is collected in the course of providing medical care, a meeting of minds between doctor and patient is therefore required in relation to the breadth of the care envisaged.

Consideration needs to be given to how best the practice can ensure that doctor/patient expectations are aligned. Doctors should make it clear to patients how they envisage the information will be used and disclosed in the course of caring for their patient's health – whether merely for a particular episode of care, or for a more holistic approach to the patient's ongoing care. Doctors need to establish procedures for communicating this to their patients. This might be partially achieved by the provision of written patient information. In addition clear and frank oral communication is required. In the course of the exchange doctors must be aware of and record any restrictions placed by the patient on the use and disclosure of any particular personal information.

An established routine procedure to record by a particular form of notation on a patient record, that a patient has had explained and understands and agrees to how their information is handled, is perhaps the best evidence that full consent was obtained. Doctors will appreciate that often patients sign consent forms without fully understanding what they are signing.

However, a sample consent form is provided in Section Five for adaption where appropriate by medical practices, if it is required.

Access and Correction
Medical practices need to develop a policy to outline how they will handle access requests. It should include:

- Who within the practice will be responsible for handling access requests
- The fees (if any) the practice will charge for various types of access
- The quality standards which will be adopted in relation to proving the information in a timely manner.

Internal Privacy Manual
An internal practice manual should detail the procedures that are in place that ensure:

- Access requests, whether oral or in writing are noted in the patient's record and dealt with in accordance with practice time-lines
- A method to note that the treating doctor has reviewed the material to ensure no restrictions to access or disclosure apply
- Systems that ensure restricted material are noted on the record

Section Five

Privacy Kit Material – Tips & Sample Forms

Getting Started Checklist

A GETTING STARTED CHECKLIST		
Checklist	**Check**	**Action / comment**
1. Have you read this Resource kit and disseminated to staff where appropriate?		
2. Have you considered appointing a Privacy Officer?		
3. Have you read the 10 NPPs and understood the concepts of 'primary purpose', 'secondary purpose' and 'reasonable expectations' in terms of patient consent for collection, use and disclosure of information?		
4. Have you conducted a privacy audit of your current practices and procedures?		
5. Have you conducted a security review of your current practices and procedures?		
6. Have you formulated or adopted a privacy policy?		
7. Have you developed an access request to records handling policy?		
8. Have you formulated a procedure to handle complaints or incidents regarding breaches of privacy?		
9. Have you trained your staff in relation to your organisation's privacy policy and procedures, and are they familiar with the privacy legislation?		
10. Have you developed a protocol for the ongoing review of the organisation's adherence to its privacy policy and procedures, and with privacy legislation?		

Consent Forms

The following is an example of Consent Form that may be drawn on to suit the needs of your practice. It does not replace effective oral communication between doctor and patient.

Dear (Patient Name)

COLLECTION OF PERSONAL INFORMATION, PRIVACY ACT 1988

We require your consent to collect personal information about you. Please read this information carefully, and sign where indicated below.

This medical practice collects information from you for the primary purpose of providing quality health care. We require you to provide us with your personal details and a full medical history so that we may properly assess, diagnose and treat illnesses and be pro-active in your health care. We will also use the information you provide in the following ways:

- Administrative purposes in running our medical practice
- Billing purposes, including compliance with Medicare and Health Insurance Commission requirements
- Disclosure to others involved in your health care, including treating doctors and specialists outside this medical practice. This may occur through referral to other doctors, or for medical tests and in the reports or results returned to us following the referrals. If necessary, we will discuss this with you.

{if the practice undertakes training of students, or research activities, then the following clauses may be adopted}

- Disclosure to other doctors in the practice, locums and by Registrars attached to the practice for the purpose of patient care and teaching. Please let us know if you do not want your records accessed for these purposes, and we will note your record accordingly.
- Disclosure for research and quality assurance activities to improve individual and community health care and practice management. You will be informed when such activities are being conducted and given the opportunity to "opt out" of any involvement

I have read the information above and understand the reasons why my information must be collected. I am also aware that this practice has a privacy policy on handling patient information.

I understand that I am not obliged to provide any information requested of me, but that my failure to do so might compromise the quality of the health care and treatment given to me.

I am aware of my right to access the information collected about me, except in some circumstances where access might legitimately be withheld. I understand I will be given an explanation in these circumstances. I understand that if I request access to information about me, the practice will be entitled to charge me fees to cover

- time spent by administrative staff to provide access at the employee's hourly rate of pay plus 20%,
- time necessarily spent by a medical practitioner to provide access at the practitioner's ordinary sessional rate and
- for photocopying and other disbursements at cost.

I understand that if my information is to be used for any other purpose other than set out above, my further consent will be obtained.
I consent to the handling of my information by this practice for the purposes set out above, subject to any limitations on access or disclosure that I notify this practice of.

Signed:..... Date:.....
Patient

Processing Access Requests Information Sheet

This information sheet may be used as a checklist to process requests to access medical records by your patients.

All patients are entitled to access the information collected about them by their health service providers.

Access may be as simple as providing a copy of the latest medical test reports, or viewing some of the information on file. However, access may involve more than just providing a print out or photocopy, and this checklist is designed to assist in those more complex circumstances.

1. Clarify scope of request if necessary. Reasons for requesting access do not have to be given, but clarification may be sought as to whether the whole file is required, or just certain parts.

2. Ensure the person seeking access has legal authority or consent to do so.

3. Acknowledge request, including providing an indication as to costs. In most cases, this acknowledgment should be done within 14 days of receiving the request for access.

4. Refer request to treating doctor or privacy officer for approval and action. The treating doctor or privacy officer should consider NPP 6 in considering request for access. If approval is granted, proceed with checklist. If approval is not granted at this stage, proceed to point 10, and provide reasons for refusal and consider other options.

5. Collate requested information.

6. Treating doctor or privacy officer to assess information to make sure that no part should be withheld due to any provisions under NPP 6.

7. Delete or remove any information, which should be withheld under NPP 6. Under no circumstances should deletions be made on the original medical file.

8. Consider copyright implications of doctor's work, and note any restrictions on further publications.

9. Once cleared for access, provide information in most appropriate form, taking into account wishes of individual. Ensure person receiving information has legal authority or consent to do so.

10. If information is withheld, provide reasons for this decision. Consider other options, which may be available to meet request, eg discussion with patient, use of intermediary etc.

11. Notate patient file that access has been granted, or refused as appropriate.

Tips on Access

- Patient access should be supervised, to ensure no unilateral removal, deletion or alteration of records. They should not photocopy their own records, although this may be time/cost saving to staff, it may raise public liability and other privacy issues. Whilst patients are granted access to their files under the privacy legislation, ownership of the records remains with the doctor or medical practice.
- Access to patient records should not be granted, without specific authorisation from the treating doctor or privacy officer. Immediate access should only be given with the approval of the treating doctor or privacy officer for straightforward requests.
- If the privacy officer is not a medical practitioner, a medical practitioner should review the record before granting access to it.
- Generally access should be granted in the form requested.
- Administrative staff should not make the decision whether access should be granted. All requests should be referred to the treating doctor or privacy officer.
- Written requests are not required by the legislation. However, in complex cases, it may be prudent to require that the request be made in writing, as the request should be noted on file for future reference.
- Access should be given within 30 days of receipt of request, in most circumstances.
- Administrative charges to cover the cost of complying with the request should be reasonable. Routine tasks such as photocopying should be done by administrative staff and charged accordingly.

Sample Access Request Form

This form may be used when individuals request access to medical records. It should be used in conjunction with the Processing Access Requests Information Sheet contained in this Resource Handbook.

Access Request Form

Name of Person seeking Access:……..

Name on Medical Record/Name of Patient:……

Relationship between person seeking access and patient:……

Medical Records required:……..……

……

……

(e.g. pathology test results, whole file, records relating to treatment for (insert condition), records between (insert relevant dates) etc)

Form of Access required:…….

……..

……..

(for example: photocopy, summary, viewing, explanation etc)

Records to be: collected on _____/_____/20 ___.

posted to: ……..

……

……..

Costs

No charge will be made to lodge this request for access. However, in providing access to you, this practice may incur charges arising out of: retrieval of records from archives, doctor's time to peruse the records, photocopy charges and doctor's time for explanation (which is not Medicare or private health insurance funded).

The practice may charge fees to cover

- *time spent by administrative staff to provide access at the employee's hourly rate of pay plus 20%,*
- *time necessarily spent by a medical practitioner to provide access at the practitioner's ordinary sessional rate and*
- *for photocopying and other disbursements at cost.*

If you have any queries regarding the costs of your request for access, please discuss these with us.

Please Note: In some cases, access to medical records may be restricted due to specified circumstances in the Privacy Act. If your request falls within one of these stated exceptions, we will provide you with an explanation as to why access could be granted, and to discuss if there is another alternative that will meet your requirements

_____

Office Use Only

Acknowledgment of access request provided
Costs of access discussed
Access granted / denied
Records provided on _____/_____/20____ by ……

Signature of Privacy Officer/Doctor

Privacy Policy for Back of Accounts

The following is a suggested form of words for doctors who do not necessarily see their patients when they first collect information about them (such as pathologists, radiologists), and doctors who seek their patients where it is impractical to discuss information handling policies (specialists in emergency situations, anaesthetists).

Consistent with our commitment to quality care this practice has developed a policy to protect patient privacy in compliance with federal privacy legislation. You can contact our office for more information about our information handling policy.

In the course of carrying out the medical services we provide we may have collected information about you from other members of your treating team. This might include, for example, information provided by your referring doctor. We might also have shared your information about you with others, for example, by providing (**insert as relevant, test results, x-rays, reports**) to your referring doctor. This will be done only as is necessary for your proper health care.

You are generally able to access the personal information we hold about you by contacting us at the above telephone number. We would be happy to discuss any concerns you have about our handling of your personal information.

Confidentiality Agreement

This is an example of a Confidentiality Clause that might be included in or accompany a contract of employment of staff of a medical practice.

Privacy Clause

Dear **[Insert name of employee]**

As an employee of **[insert name of employer practice or organisation]** I agree that I will abide by the privacy policy, privacy legislation and privacy procedures, which apply to this **[practice or organisation]**. In particular, I agree that:

(a) I shall not, during my period of employment with **[insert name of employer practice or organisation]**, disclose or use any patient files, medical reports or confidential knowledge obtained through my employment with **[insert name of employer practice or organisation],** other than to perform my usual duties of employment as authorised and detailed above **[assuming that duty statement is included in employment agreement]** or specifically requested by my supervisor to perform.

(b) Any breach of this **[practice or organisation]**'s privacy policy or privacy legislation, caused by me, whether intentional or not, may result in disciplinary action, including immediate termination.

(c) The obligations contained in clauses (a) to (b) will continue even after the termination of my employment with **[insert name of employer practice or organisation]**, whatever the reason for the termination.

(d) Upon termination of my employment with [insert name of employer practice or organisation], for whatever reason, I will immediately deliver to **[name of practice or organisation]** all patient files, medical reports or other documents which are in my possession or under my control which in any way relate to the business of **[insert name of practice or organisation]** or its patients past or present.

Signed: …….. Date: ……/……/……

Website Privacy Statement

This is an information sheet which contains an example of a Website Privacy Policy to use on your practice website.

Questions to ask your Internet service provider

1. Full name of Internet service provider for inclusion in website statement.

2. What information does your Internet service provider record for statistical purposes, eg. date and time of visit, pages accessed, server address etc?

3. How often is statistical information provided to you, and in what form?

4. Whether there are any security measures, such as encryption, secure sockets layer etc, and if so, what level of security is available, to allow for secure communication via the Internet?

5. Are cookies used on your site, and if so, how are they used? Are they persistent or session based?

What must website privacy statement tell site visitor?

1. That the practice has developed a policy to protect patient privacy in compliance with privacy legislation;

2. What personal information is being collected;

3. Who is collecting their personal information;

4. How their personal information is being used;

5. To whom their personal information is being disclosed; and

6. How their personal information is being stored.

A Web Site Privacy Policy for Your Practice Web Site

You may need to collect certain information and/or assurances from your Internet service provider in order to complete this statement

This practice has developed a policy to protect patient privacy in compliance with privacy legislation. Our policy is to inform you:

1. What personal information is being collected;
2. Who is collecting your personal information;
3. How your personal information is being used;
4. To whom your personal information is being disclosed; and
5. How your personal information is being stored.

Information Collected

- When you look at this web site, our Internet Service Provider {insert name of ISP here} makes a record of your visit and logs the following information for statistical purposes:
- Your server address
- Your domain or top level domain name (eg practice.com, .gov, .au, etc)
- The date and time of your visit to the site
- The pages you accessed and documents downloaded
- The previous site you visited
- The type of browser you are using

{your ISP may collect more or less information for you}

Our Internet Service Provider provides this information to us ***{insert details of how information is provided and on what basis eg regularity etc}***

This non-identified information is used to monitor usage patterns on our site in order to improve navigation and design features – helping you to get information more easily.

Access to information collected

We will not make an attempt to identify users or their browsing activities. However, in the unlikely event of an investigation, a law enforcement agency or other government agency may exercise its legal authority to inspect our Internet Service Provider's logs, and thus gain information about users and their activities.

Use of information collected

We will only collect your e-mail address if you send us a message. Your e-mail address will only be used for the purpose for which you have provided it, and it will not be added to a mailing list or used for any other purpose without your consent. We may however, use your e-mail address to contact you to obtain your consent for other purposes, but will give you the option of having your address deleted from our records at that time.

Personal health Information

{If there are no specific security measures in place use this clause}

In the interests of your privacy, and given the inherent insecurity of information passed over the Internet, we do not currently support the transmission of personal health information to or from our patients over the Internet. If you send any personal health information to us via the Internet, we cannot guarantee its security.

{If there are specific security measures in place use this clause}

We have deployed the following security measures to support more secure communication of sensitive information across the Internet.

{insert details of the security measures that you have adopted/deployed, such as encryption, secure sockets layer etc}

Cookies

This web site only uses session cookies and only during a search query of the web site. Our Internet Service Provider has assured us that no cookies are employed on this web site except for those associated with the search engine. The web site statistics for this site are generated from the web logs as outlined above.

Upon closing your browser the session cookie set by this web site is destroyed and no personal information is maintained which might identify you should you visit our web site at a later date.

Cookies can either be persistent or session based. Persistent cookies are stored on your computer, contain an expiry date, and may be used to track your browsing behaviour upon return to the issuing web site. Session cookies are short lived, are used only during a browsing session, and expire when you quit your browser.

Sample Information Pamphlet, General Information Pamphlet & Patient Information Poster

Instructions for 'Getting Started' Use
The following two double sided pages can be detached and cut to create two sheets. Insert your practice details in the blank spaces provided on both sheets. Fold each sheet inwards into thirds to create six-panel privacy policy pamphlets for patients. Photocopy as many as required. These are samples only pending development of its own privacy information pamphlets.

Following the pamphlets is a sample privacy policy poster, which for 'getting started' use, insert practice details in the space provided and display in a prominent place in your waiting or reception area.

Appendix

National Privacy Principles – in full

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:

(i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under s.95AA for the purposes of this subparagraph; and

(iii) in the case of disclosure – the recipient of the genetic information is a genetic relative of the individual; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the ***carer***) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

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

4 Data security

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

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsections 100(2) and (3).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an ***identifier***.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required or authorised by or under law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.