



AMA

Privacy Resource Handbook

For all Medical Practitioners
in the Private Sector



AMA

Privacy Resource Handbook

For all Medical Practitioners
in the Private Sector

Published by AMA, Canberra, 2002

© Copyright: The Australian Medical Association, Canberra, ACT, Australia. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means - electronic, mechanical photocopying, recording or otherwise, other than by medical practitioners to whom this is directed and their staff for their professional use, unless the permission of the AMA has been given beforehand.

Disclaimer:

The AMA has made every effort to ensure that, at the date of publication, the information contained in this book 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 the absence of health specific national legislation, the application of general privacy laws to the health sector should enhance rather than hinder 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 AMA has developed this Resource Book to help doctors comply with the Privacy Act 1988 (Cth), as amended, which affects all doctors practicing in the private sector with effect from 21 December 2001.

The book aims to give doctors a sound grounding in the National Privacy Principles (NPPs), so they can more easily implement the changes required to comply with privacy legislation.

We also want to help doctors manage health information ethically and lawfully without hindering them in maintaining high professional standards.

Getting a patient's consent for a doctor to collect health information not merely for current use, but for future use in the course of the patient's ongoing health care, cannot happen without effective two-way communication.

Aligning patient and doctor expectations better will reduce red tape and the costs of complying with the privacy legislation while maintaining quality patient care.

The Government proposes to review the working of the legislation after monitoring the working of the NPPs for the next two years and will consider amendment proposals in light of that review. Doctors have a vital role in making the Government aware of significant issues relating to quality health care arising out of the privacy legislation. With feedback from doctors, the AMA will then be better placed to make effective representations to the Government about making necessary changes to the legislation.

Dr Kerryn Phelps

Federal AMA President

2002

Introduction from the Vice President



Privacy is central to medical practice. As doctors we understand that our patients need to have confidence that we will maintain privacy and confidentiality. If patients are unable to trust us to discuss sensitive matters with us then we will be unable to formulate a diagnosis or a plan of treatment. As patients ourselves we are often concerned about the confidentiality of our own medical information.

As Chair of the Ethics and Medico-Legal Committee I recognised that privacy issues cut across a wide range of areas and to co-ordinate the AMA approach I established and chaired a working party on privacy within the Federal Secretariat across a number of departments.

In the world of electronic health privacy concerns must not be seen as one of the areas that needs to be dealt with along the way but as the central issue which must be adequately addressed before e-health initiatives can go ahead with the confidence of both doctors and patients.

Equally, we need to ensure that privacy guidelines do not interfere with best practice in clinical work and we shall continue to liaise closely with the Privacy Commissioner's office in order to ensure this.

Privacy concerns should be integral to good quality medical practice and not an optional extra. This booklet is an attempt to integrate an approach to privacy in the clinical setting which enhances clinical care and patient confidence. It is as

comprehensive as possible within the constraints of size and readability. I am grateful to all those who have contributed to its development, both directly and indirectly, and in particular to the AMA's legal counsel, Ms Pamela Burton who has been most instrumental in its production.

Our thanks also to the Department of Health and Ageing and the General Practice Computing Group for funding assistance for the printing and distribution of this Resource Kit.

Dr Trevor Mudge

Vice President

Australian Medical Association

Chair

Ethics and Medico-Legal Committee

Contents

FOREWORD	iii
USING THIS RESOURCE BOOK	viii
SECTION ONE	1
INTRODUCTION	1
<i>Background</i>	1
Federal Privacy Legislation	1
Related State and Territory legislation	1
Proposed Federal/State Privacy Code	1
<i>To whom does the new Federal privacy legislation apply?</i>	1
Focus not on medical practitioners alone	1
<i>The National Privacy Principles (NPPs)</i>	2
What are the NPPs?	2
What do the NPPs cover?	2
<i>Compliance with the privacy legislation</i>	2
Privacy and Confidentiality	2
<i>Special Areas of Concern</i>	2
Consent Issues	2
Access to Medical Records	3
<i>What are the consequences of non-compliance?</i>	4
The Privacy Commissioner's powers	4
Medical Indemnity cover for privacy breaches	4
Do doctors need to have a complaint handling process?	4
What should doctors do if the Privacy Commissioner investigates them?	4
SECTION TWO	5
THE PRIVACY LEGISLATION	5
<i>Explaining the National Privacy Principles</i>	5
NPP 1—Collection	5
NPP 2—Use & Disclosure	5
NPP 3—Data Quality	6
NPP 4—Data Security	6
NPP 5—Openness	6
NPP 6—Access & Correction	6
NPP 7—Identifiers	6
NPP 8—Anonymity	6
NPP 9—Transborder Data Flows	7
NPP 10—Sensitive Information	7
<i>Are the NPPs retrospective?</i>	7

SECTION THREE	8
COMPLYING WITH THE NATIONAL PRIVACY PRINCIPLES	8
<i>Collection</i>	8
Do I need my patient's consent to collect their information?	8
What do I tell the patient about the information I collect?	8
Can I collect information from other sources than the patient?	8
Can I collect information from other doctors about a patient without seeing the patient?	9
Can I collect information about other family members when taking a medical history?	9
<i>Consent</i>	9
Is it necessary or advisable to obtain written consent to collect information from patients?	9
Do I need the consent of third parties to collect information about them in the course of taking a family or social history?	9
Can I collect family and social history in order to produce a medico-legal report?	10
<i>Use and Disclosure</i>	10
Can I release patient information to other doctors?	10
Can I share patient information in multi-disciplinary medical teams?	11
Can I record patient information on a Medical Register?	11
Can I disclose patient information to my Medical Defence Organisation?	12
Can I give patient information to a debt collector?	12
Do I have to alter my office layout to comply with the privacy legislation?	12
Can I fax and e-mail medical information?	12
Can I leave telephone messages?	13
What are my obligations when I have to disclose information without the patient's consent?	13
<i>Access</i>	13
How should a request for access be handled? Should it be made in writing?	13
Can I ask a patient why they require access?	13
Do I have to provide a copy of my whole medical file on that patient?	13
How much time do I have in which to process an access request?	13
How much can I charge to provide access to a patient?	13
Do I have to provide access to medical records created before 21 December 2001?	14
Can a parent always get access to their children's medical records?	14
Can a GP provide a patient access to a specialist's report contained on their file?	15
Can I restrict patient access to mental health notes?	15
Do I have to give immediate access to test results?	15
<i>Copyright</i>	16
Who owns the medical records - the doctor or patient?	16
<i>Medico Legal Requests</i>	16
Am I obliged to provide access to the patient of a medico-legal report?	16
Should I forward medical records to a solicitor or a patient's agent?	17
To whom can I disclose a report prepared for a commissioning agent?	17
<i>Transfer of Medical Records</i>	18
I'm retiring - what do I need to do to with my records?	18
A patient wants to change doctors. What am I required to do?	18

SECTION FOUR	19
Meeting Compliance Obligations and Pursuing Best Practice	19
<i>Develop and adopt a privacy policy</i>	19
<i>Implementing the privacy policy</i>	19
Privacy audit	19
Poster and patient information pamphlets	20
Privacy Action Plan	22
Establish a Privacy Manual	22
<i>Some Tips on Developing a Privacy Policy</i>	22
Consent	22
Access and Correction	22
 SECTION FIVE	 23
Privacy Tool Kit	23
<i>Getting Started Checklist</i>	23
<i>Consent Form</i>	24
<i>Staff Information Sheet - Processing Access Requests</i>	25
<i>Tips on providing access</i>	25
<i>Sample Access Request Form</i>	26
<i>Privacy Policy for Back of Accounts</i>	27
<i>Confidentiality Agreement</i>	28
<i>Checklist for IT Privacy of the Practice</i>	29
<i>Website Privacy Statement</i>	31
<i>A Sample Web Site Privacy Policy for Your Practice Web Site</i>	31
<i>Sample Patient Information Poster</i>	33
<i>Sample Patient Information Sheet</i>	34
<i>Sample General Information Sheet</i>	36
 APPENDIX	
NATIONAL PRIVACY PRINCIPLES - IN FULL	38
1 Collection	38
2 Use and disclosure	38
3 Data quality	41
4 Data security	41
5 Openness	41
6 Access and correction	41
7 Identifiers	42
8 Anonymity	43
9 Transborder data flows	43
10 Sensitive information	43

Using This Resource Book

The purpose of this Resource Book is to help doctors to understand how privacy law now affects them and their medical practices.

Section One briefly introduces the *Privacy Act 1988* and National Privacy Principles (NPPs).

Section Two explains and summarises the NPPs then highlights special areas of concern to medical practitioners and explains some new concepts.

Section Three uses questions and answers to discuss the practical application of the NPPs to a clinical practice and to suggest how doctors can comply with them while carrying out best practice in a busy clinical setting. This section covers large and small medical practices, employed and self-employed practitioners, medical researchers, medico-legal workers and clinicians moving between the public and private sectors.

Section Four 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.

Section Five provides some sample forms, tips and checklists, a sample privacy policy poster and patient information sheets.

The Appendix sets out the NPPs in full.

The aim of this Book is to help practitioners meet their privacy compliance obligations and develop privacy compliance policies tailored to suit their own individual practices. It is not intended to be a substitute for the privacy legislation, the NPPs and the guidelines, which doctors should consult when they feel in doubt. Doctors can help in the review of the operation of the legislation after the first two years by telling the AMA when they find the legislation unclear or ambiguous or incomplete or inconsistent, or even unreasonable or unfair.

An Essential Message

Without open and effective communication between doctor and patient, there can be no alignment of the expectations that each has. Doctors are the best conduit for telling patients about their privacy rights, about how their personal information will be managed and what they need to agree if they are to get prompt and holistic medical care. A patient needs to know the possible health consequences of exercising his/her right to withhold personal information from the medical team that is providing the treatment.

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 how the NPPs are to be applied. The Act requires that private sector service providers must comply with the NPPs. The Health Guidelines acknowledge that the principal concern of the health service provider is the health care of the patient. Doctors should keep this in mind when applying the NPPs to the handling of patient information. At the same time, doctors must understand that compliance with the NPPs is a legal requirement. Adherence to privacy rules is expected to enhance, not hinder patient care, the relationship of trust between doctor and patient, and the patient’s confidence in the doctor. It is up to individual doctors to exercise their best professional, ethical and clinical judgment in meeting the NPP obligations consistently with accepted medical precepts and ethics to a standard that can reasonably be expected of a competent and skilled clinician. *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 help members 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

In December 2000, the Commonwealth amended the *Privacy Act 1988 (Cth)* (the Act), previously applicable only to the Commonwealth public sector, to extend its application on and from 21 December 2001 to most of the private sector including all health service providers. The Act, which is not health specific but which was drafted to encompass the health sector, applies equally to other professions and incorporates ten National Privacy Principles (NPPs) with which private sector organisations are obliged to comply in managing personal information which they hold.

What this means for doctors is that:

- they have new obligations to safeguard patient privacy and to give patients some control over how information about them is handled,
- they are required to be more open with patients than before, and
- they are generally required to provide patient access to the information held about them.

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

Related State and Territory legislation

Existing and pending State and Territory privacy and health records legislation requires doctors to comply with specific health information management practices that in some instances differ from what the Commonwealth legislation requires. Against the background of the Constitution, the Commonwealth's intention to create a 'single national

comprehensive scheme' means that laws created by other jurisdictions must be consistent with the Commonwealth legislation. On this understanding, where an act or practice is regulated by the Commonwealth Privacy Act, then it is not regulated by a State or Territory privacy Act.

Proposed Federal/State Privacy Code

The Federal, State and Territory Health Departments are working towards a health specific Privacy Code to apply to both private and public sector health service organisations. The addition of this Code to the existing Federal, State and Territory privacy legislation potentially further complicates the legal situation. However, the aim of the Code is to simplify the application of the privacy principles in the health sector as a whole.

To whom does the new Federal privacy legislation apply?

Focus not on medical practitioners alone

The NPPs 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 activities of people 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.

This means that professional and administrative staff of all private sector organisations providing these types of services, as well as health services that hold health information, have to comply with the NPPs. This includes the people and doctors who work within them, doctors who practise in partnership or alone, in private hospitals, aged care facilities and other private health facilities, and those who undertake medico-legal work. The NPPs 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?

Schedule Three of the Act contains the ten National Privacy Principles that set out the minimum standard of compliance required. These NPPs were designed not only for health service providers but to apply across the broad spectrum of private organisations, 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 virtually the full gamut of information handling practices from collection to disposal of health information, including use and disclosure, storage and maintenance. All health and personal information collected in providing a health service is regarded as sensitive information. It is essential that medical practitioners understand that the individual's consent is generally required for the collection of sensitive information. Exceptions are provided for in NPP 10, for example, in the case of an emergency, or where collection is required by law.

Once the practitioner has obtained consent to collection, 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 further consent from the individual.

The NPPs and the Privacy Commissioner's Health Guidelines 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 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 about how personal information will be handled. This gives rise to issues surrounding consent requirements.

Special Areas of Concern

Consent Issues

When collecting health information or as soon as practicable after that, generally speaking, the practitioner is required to get fully informed and voluntary consent from the patient.

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

Collecting information during a consultation usually implies consent, but the patient must be told what information the doctor is recording and why, how the doctor will use it and to whom the doctor will disclose it.

There may be cases when consent needs to be in writing (though there is no legal requirement that it be in writing), especially if it is being sought for using or disclosing the health information for a secondary purpose such as medical research.

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

When the information collected from the patient is about another person, the consent of that other person might be required. Consent of third parties is not required when their information is collected as part of taking a medical history. See later discussion of TPID.

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 legal professional privilege;
- providing access would be unlawful or the law authorises denial; and
- it might prejudice an investigation of possible unlawful activity.

Handling requests for access

Organisations need to develop a policy about handling access requests. (See Section Five).

Patients do not have to give reasons for requesting access. However, the scope of the request may need clarifying so that the access granted is appropriate, 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. Patients cannot be required to make their requests in writing, though in some cases it may be prudent to ask the patient to do so.

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

Fees that can be charged

Patients should be told about charges for the doctor's time or administrative costs 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 determines 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, of whom some are subject to the Act and some 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 are 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 that are held by the doctor are subject to the Act.

- A doctor who works at a State/Territory health organisation and bills public patients, but takes copies of patient information back to his/her 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 about 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 but 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 there has been a breach, 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. However, the inconvenience, embarrassment and cost of investigation to a doctor 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 most cases simply discussing the issues with the patient should resolve the matter to the patient's satisfaction. The Commissioner will look into a complaint only if that process fails. 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 tell the Federal AMA office about any investigation. 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 (NPPs) setting the minimum standards for privacy that the non-government sector has to follow are embodied in the Act and 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, NPP 1 requires that:

- only information necessary to deliver the health service be collected
- collection be fair, lawful and not unreasonably intrusive
- the person about whom personal information is collected be told:
 - the name and contact details of the organisation collecting their information,
 - 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
 - if there is any law requiring collection of the information.
- a person be told about the main consequences, if any, if the person does not provide all of the information requested.
- the information be collected primarily from the person, but where it is collected from other sources eg. X-rays or specialists' reports, the person should be told this.

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;
- where other provisions under NPP 2 relating to the public interest, such as law enforcement and public or individual health and safety, apply, such as, for example where it is reasonably believed that the use or disclosure is necessary to lessen or prevent "a serious and imminent threat to an individual's life, health or safety" or "a serious threat to public health or public safety". Doctors should familiarise themselves with the terms of the exceptions under NPP 2.

In other words, once a person has given personal information, the health practitioner must get the patient's further consent to use or disclose it. Exceptions to this include use or disclosure of the information for the main reason for which it was originally collected or for other directly related purposes if it would be reasonable for the patient to expect this.

This is perhaps the main concern for doctors who need to share patient information with treating teams, some of

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 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 first issued a Temporary Public Interest Determination (TPID) and subsequently issued an ongoing Determination (PID) that 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.

whom don't see the patient at the time of collection to get consent or discuss purposes of disclosure.

Patient understanding of the purpose of collection is therefore crucial. If the main purpose is for treatment, disclosure, for example, for 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 those 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. Electronic data on computer hard disk drives are often retrievable unless correct procedures are used to "wipe" the drives completely clean. Safe disposal of all kinds of computers must take this into account. The cleaning is not difficult but in cases of uncertainty, the services of an IT professional may be appropriate. 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 the development of e-health records reinforces the need to review and upgrade 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 Sections Four and Five of this Book.

NPP 6—Access & Correction

Generally speaking, individuals have the right to access their own health records and 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 pose a threat to a person's life or cause serious harm to a person's health.

NPP 7—Identifiers

Generally speaking, an organisation must not adopt as their own identifier, Commonwealth government identifiers, such as a Medicare or Veterans Affairs number, and must not use or disclose such identifiers except to fulfil its obligations to the agency which assigned the identifier.

NPP 8—Anonymity

Where lawful and practicable, individuals must be given the option to interact anonymously. In the context of health care this is likely to apply to doctors only in some special circumstances, for example where treatment or counselling is provided on an anonymous basis in the area of HIV/AIDS and sexual health. 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 transfer personal information out of Australia only 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 beyond Australian jurisdiction.

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:

- where 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 collection is necessary for the establishment, exercise or defence of a legal or equitable claim (this may include many medical defence purposes);
- 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, in cases 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 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 personal, sensitive or health information is collected in the course of providing a health service.

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, used or disclosed after that date. If compliance in giving access to information collected prior to 21 December poses an unreasonable administrative burden or expense, then access need not be granted; however, provision of a summary would be an option to consider.

NPP 4 on data security, NPP 5 on openness, NPP 7 on identifiers and NPP 9 on transborder data flows 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.

This Section uses questions and answers to identify and consider issues that might confront medical practitioners in complying with their privacy obligations. The issues fall into the following main groups:

- 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;
- the general right of patients to access information held about them;
- ownership of medical records, medico-legal concerns and transfer of medical records.

Different considerations will apply depending on:

- whether the practice is small or large;
- whether the practice is a general or specialist practice;
- whether the practitioner sees the patient at the time of providing the service;
- whether those who attend the patient provide a health service which allows adequate opportunity for consultation before or after attending;
- whether the practitioner moves between the public and private sector;
- whether information might be required for research.

Collection

Do I need my patient's consent to collect their information?

Generally speaking, 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**.

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 fundamental concept under the Act which doctors must carefully consider 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. This includes:

- that information will be collected;
- the purpose of collection;
- that they may access information collected about them;
- 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 the information will be handled at the time of collecting the health information. Often, when the patient first sees the 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 told that information has been collected, the purpose of collection, that they may access the

information, to whom the information will be disclosed, the identity of, and how to contact, the organisation collecting the information, and any law that requires the information to be collected.

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 without seeing the patient, or 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 telling the patient about how 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?

Yes. See below for consent requirements.

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.

The signing of forms does not provide the assurance doctors would like. People often sign forms although they are not aware of what they are signing or why, but assume they have to sign in order to obtain treatment.

The fact that a patient presents for health care and freely gives the information will generally be evidence of consent. The clinical notes usually tell the best story. If the doctor requires additional information, (for example, to assess whether secondary problems exist, or for ongoing health care) and explains this, 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?

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.

This was addressed early by the Privacy Commissioner's issue of a Temporary Public Interest Determination (TPID) which declared that no organisation is taken to contravene the Act if personal information is recorded by a health service provider in circumstances where:

- (a) *the collection of the third party's information is necessary for [the organisation]*
 - (i) *to provide a health service directly to the individual; and*
 - (ii) *to diagnose, treat or care for the individual; and*
- (b) (i) *the third party is a member of the individual's family or household, or the third party's information is otherwise relevant to the individual's family medical history or social medical history; and*
 - (ii) *[The organisation] collects the information about the third party in either or both of the following circumstances:*
- (c) *without obtaining the consent of the third party; or*
- (d) *without taking reasonable steps under the National Privacy Principle 1.5 to ensure that the third party is or has been made aware of the matters listed in National Privacy Principle 1.3*

A Public Interest Determination (PID) has now been issued in similar terms on an ongoing basis. The PID covers family histories, and 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 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 histories in order to produce a medico-legal report?

The Determination (PID) permits doctors to collect family and social histories in order to produce medico-legal reports.

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 other directly related purposes 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.

Where information is to be used and disclosed for later episodes of care not in the patient's or doctor's mind at the time of collecting it, the situation becomes more difficult. Further patient consent is required, unless the main purpose for collecting the information is 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. It is therefore important that doctors get patients' agreement to collect information 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 to that of the patient's. Further consent is not then required for the consequent sharing of information with other doctors in the course of caring for those 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, 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), for example, to other members of the treating team, if treatment for the condition is required.

However, recording patient health information on medical registers such as diabetics registers raises other issues. Although recall/reminder systems are directly related to the patient's health, if register 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. Depending on how the information will be used and disclosed the patient's agreement is likely to be required if the register is held outside the practice, for example, by GP Divisions. To avoid inadvertently making an unlawful disclosure, the doctor should establish and record the method(s) of recall/reminder to which the patient agrees. 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.

It is important to note that:

- unless the information is de-identified, or consent is obtained, information should be transmitted to General Practice Divisions and the Health Department only for the purpose for which the doctor collected it and not for their own purposes;
- doctors transmitting information electronically must ensure that it is encrypted;
- unique identifiers such as Medicare numbers should not be used or disclosed unless required by Medicare (Health Insurance Commission) or as otherwise necessary for purposes under the Medicare legislation.

Ideally, a general practice 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. Where doctors may be obliged to disclose patient information relating to adverse outcomes to their Medical Defence Organisation, insurer, medical experts or lawyers, and if it is within patients' reasonable expectations, then such disclosures may proceed without seeking patient 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 for which it was collected, namely to provide health care to the patient or for directly related secondary purposes which are in the patient's reasonable expectation. Using the patient's name and address details for billing purposes, or for pursuing non-payment, falls into the category of directly-related secondary purposes which patients might reasonably expect. Thus it is permissible to disclose a patient's name and address to a debt collection agency to recover a bad debt. It is advisable to ensure, perhaps by way of contact with the debt collector, that the personal information disclosed to the debt collector will not be used or disclosed for any other purpose.

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 with receptionists seated behind a counter at 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, possibly including a private interview room, and additional staff to ensure that there is always somebody from the practice in the waiting room. This would not only be inefficient but would generate costs which 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.

The layout of the waiting room should ensure that the reception desk is high enough to protect patient information from unauthorised eyes. Staff should be made aware of the need to position themselves so as to limit the chance of others overhearing their telephone conversations and to avoid making unnecessary identification of patients about whom they are speaking. Similarly, doctors calling in 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.

Care should be taken that individuals cannot see computer screens that show information about other individuals.

Can I fax and e-mail medical information?

Faxing medical reports and health information, for example, 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 out of sight. Appropriate security safeguards need to be in place for the e-mailing of information, including encryption and ensuring the identity of the receiver. Note that unencrypted e-mail is not a secure means of transmitting information.

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 implement a policy of asking patients to tell the practice if they do not want telephone messages left.

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 make a written request. However, most requests are likely to be simply satisfied, for example, by the doctor explaining the medical information or providing a copy of a test result after discussing the result with the patient. The practice should establish a form for use when asking a patient make an access request in writing. The signed form should be placed, or an oral request should be 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 clarifying so that the access granted is appropriate, 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?

Common sense and proper doctor/patient communication will best determine the best form of access provided to patients. 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 but may be happy to receive a summary of the notes or of a specialist's opinion, or an explanation, or simply a copy of a test report. 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 much time do I have in which to process an access request?

Access requests do not have to be responded to immediately. Doctors should 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. In general an access request should be met within 30 days, taking into account the patient's needs.

How much can I charge to provide access to a patient?

Patients cannot be charged application fees to lodge a request for access. They can be charged a reasonable fee to cover administrative costs, the costs of photocopying, and the doctor's time spent perusing the notes or explaining

them to the patient, or rewriting incomprehensible records. 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 to give this during the consultation in accordance with good clinical practice, as part of the normal consultation time and cost.

The doctor and patient may have differing views about what is a reasonable cost for complying with the request for access. Other laws that provide for photocopy costs, for example, Freedom of Information or Health Records legislation, will provide a guide. The doctor and the patient should jointly ascertain the scope of the request and discuss the costs involved.

Do I have to provide access to medical records created before 21 December 2001?

There is a difference between information collected prior to 21 December 2001 and that collected after. The Act generally applies to information collected on or after 21 December 2001. However, there is some retrospectivity to the access provisions. Personal information collected before that date that remains in use after that date forms part of the information 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 to information collected prior to 21 December 2001 not in use. However, a request for access to these records should be handled in accordance with good clinical and ethical practice.

NPP 6.3 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.

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.

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 providing access to mutually agreed intermediaries would be sufficient 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 without my permission". Such a notation is also to be ignored if the patient authorises the release, or the law requires it. However, a 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 author of a report is not an advisable course. A GP might need to consult the specialist about any harm disclosure of the report might pose. However, a specialist is more likely to defer 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 include intimate notes of an interactive doctor/patient relationship. The therapeutic process often requires a verbatim record of a patient's account of events that involve other people, or indeed the doctor, that are not necessarily accurate.

Where access to the notes is requested, doctors should consider questions 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.

If there are grounds for refusing access to all the information, other means of providing access other than copying the complete notes should be considered, including the provision of a summary report.

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 may be 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 usually only a summary of this material is 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 because if a patient does insist on a full copy of the notes after being offered a summary, then the situation has 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 demands 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. Circumstances where releasing uninterpreted test results to a patient could cause life-threatening harm constitute a valid reason under the NPPs not to do so.
- 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 patients' 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.

The goal here is to facilitate access in the most appropriate manner, not to deny access.

Copyright

Who owns the 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. The doctor owns the intellectual property rights in that information. The copyright of specialists' reports held on a GP's file belongs to the specialist who wrote the report.

The High Court case of *Breen v Williams* (1995) 186 CLR 71 confirmed doctors' rights in this regard. The Act is subject to existing law, and that includes court-made law as well as Parliament-made law. Thus, the granting to patients of access to their medical information does not necessarily give patients the right to deal with the information as they wish. The Act restricts doctors as to how they may use and disclose the patient's information. But as well, patients' rights to access their health information may be subject to restrictions on 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 nobody else reproduces the doctor's opinion 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 doctor's 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 doctor examines the patient for the purpose of preparing the report. Where the report, commissioned by a third party, is the subject of legal professional privilege, then it is 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. A doctor might be concerned that a patient might then use the report for other unrelated purposes - in pending litigation, or for some other purpose such as to get a pilot's licence. While under the Act the doctor is not entitled to ask why a patient seeks access, it is reasonable for the doctor to assert copyright over a medico-legal report. In that event the doctor in providing access can stipulate that the report be not further published or reproduced without the doctor's permission and thus ascertain whether the patient is 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 could circumvent its payment by accessing the report through the Act. A doctor concerned that this might happen could ask for payment of the agreed fee before examining the patient and preparing the report and so avoid the problem.

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, and the NPPs.

Should I forward medical records to a solicitor or a patient's agent?

While a doctor is not entitled to ask why access is requested, it is appropriate to seek clarification of the request to enable agreement about the nature of the access and the appropriate cost. When a patient seeks to have notes forwarded to a 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 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 ask for payment of reasonable administrative costs incurred in reviewing the notes and for photocopying 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 for the purpose of or in anticipation 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 and the patient may very likely 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's having applied for a Work Cover benefit covers the consent requirement. If the relevant legislation authorises the release of information, no further consent is required, but good clinical practice would surely dictate that the doctor should tell the patient about the request and 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, which is why the material was collected in the first place. 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 asks whether or 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 to make decisions about management of their health information.

Transfer of Medical Records

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

When a practitioner retires or dies and another doctor within the practice takes over responsibility for the patient records held by the retiring or deceased practitioner, it is appropriate that the practitioner, or the estate, issue a circular announcing the retirement or the death advising that the records will be held by a nominated doctor in the practice. If that is not feasible, then it is appropriate that patients be informed about the new arrangement when they contact the practice giving them the opportunity to have their 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 practice's phone number might have to be retained or redirected to enable patients to be told about 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 the new practitioner gets all papers and records reasonably required to treat the patient adequately.

If the patient has requested transfer of the full medical file, 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 authorship 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 are recommended:

1. **Conduct a privacy audit** of the practice to identify deficiencies in relation to its compliance with the Act (see below).
2. **Display a notice** (perhaps based 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 on request about the handling of patient information. Make an information sheet (or patient information pamphlets containing information set out in samples in Section Five) available to patients who request more information about how their health information will be handled.
3. **Draw an Action Plan** (see below) addressing the deficiencies identified in your audit, working out what is necessary for the ongoing improvement of your procedures, development of privacy policy and compliance with the Act that you propose to implement, and setting target dates for completing each stage in the process.
4. **Create a Practice Privacy Manual** (see below for suggested contents of an office manual)

The practice privacy policy needs to be adjusted and developed as required so that it reflects the particular procedures of the practice.

Implementing the privacy policy

Much of the compliance obligation is in making patients aware of the practice's privacy policy and procedures for handling personal information. Carefully worded waiting room notices or posters, patient information sheets, and a practice privacy policy pamphlet are useful. **Nothing, however, will be a substitute for frank and effective doctor patient communication.**

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.

Take a look at the reception area:

- How might 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 close the data about the previous patient on your computer screen before the next patient comes in?
- When taking telephone calls about a patient in the presence of another person, do you take care 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?

- 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 security—e.g. paper records are kept locked away when not in use?
- For noting—perhaps in red ink - on patient records any restrictions on access, use or disclosure?
- For distinguishing between information collected before and after 21 December 2001 to reflect the different obligations that apply to access, use and disclosure?
- To review personal information regularly, and under secure conditions destroy records no longer needed? Note that for medico-legal purposes, medical records may need to be kept for many years.
- For making your forms clear about which parts a patient is obliged to complete, and which information is voluntary?
- For offering patients a form on which they may apply for a copy of their medical records, in which case, have you considered the issues surrounding this option?
- For security of electronic records? Note that security and privacy issues are to be considered in relation to PCs, laptops, hand-held organisers and commercial patient record software.

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, wherever possible, identifying information from personal health information being used for research and quality assurance activities?

Check the security of patient records

Check the security of storage, transfer and disposal systems for both paper and electronic records.

A full checklist of IT security is provided in Section Five of this Book.

Poster and patient information pamphlets

To comply with NPP 5 - Openness - for ‘getting started’ purposes, the AMA has produced a coloured poster, and two coloured patient information pamphlets either or both of which can be provided to patients who want to know more about how their information is handled. See Section Five for the content of these documents.

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 contained in the samples in Section Five to include information that goes beyond privacy matters and provides other details about the practice.

Privacy Action Plan

Nominate a person in the practice to be its privacy officer

There is no obligation under the Act to appoint a privacy officer, in which case 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 practice managers in a corporate structure. However, it would be prudent to nominate a person to be responsible for ongoing development, implementation, maintenance and observance of the organisation’s policies and its procedures for handling patient information. Depending on the size of the organisation, this person might be a doctor, practice manager, receptionist or someone employed specifically to perform that function.

The person should be responsible for:

- full implementation of the practice's privacy policy
- handling staff and patient privacy questions
- establishing access requests and complaint handling procedures
- establishing and supervising disclosure and complaint registers
- ongoing privacy compliance

What a Privacy Officer should do in performing those functions

(a) Become familiar with the 10 National Privacy Principles (NPPs).

This Book 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, covering such matters as referred to above.

(c) Establish a Disclosure Register.

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.

(d) Examine the 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, see information on IT Privacy contained in Section Five.

(e) Formulate and implement a privacy policy.

Each organisation must have a clearly written privacy policy readily available to whoever requests it. As explained above, by displaying the poster and using the pamphlets provided by the AMA and complying with their contents, (information contained in them is set out in Section Five) you have begun to implement a basic privacy policy.

This material, however, contains general information only and you will need to review and perhaps develop these documents to reflect your own procedures.

The Commissioner has information sheets to help you formulate a privacy policy that suits the needs of your practice. See also some tips below to assist you with this task.

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

It would be prudent to create a register to accurately record complaints and the action taken to respond to them in case of an investigation by the Commissioner of any unresolved complaint. This register will assist in the ongoing reviews of the organisation's practices to ensure adherence with the Act.

(g) 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 help avoid unintentional breaches of privacy. All staff should also be aware of patients' 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 Book of relevance to them.

(h) Staff confidentiality agreements.

It is advisable that all staff sign an appropriately drawn confidentiality agreement. This could be included in contracts of employment. A sample confidentiality agreement is provided in Section Five.

(i) 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.

(j) 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
- advise whether to install additional software to record your privacy policy and your implementation procedures, let you monitor its working, access checklists and conduct privacy audits.

Establish a Privacy Manual

It is suggested that an office manual be compiled containing all relevant privacy information. It should be indexed and made 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 AMA's Website at www.ama.com.au
5. This Book
6. Sample forms from Section Five or as developed by your practice from which further copies can be made as required
7. Your practice's privacy policy, Website policy, information pamphlets etc.
8. The detailed practice procedures in place that cover the handling of patient information.

Some Tips on Developing a Privacy Policy

Consent

Aligning doctor/patient expectations is essential in protecting information and the practice needs to consider the best way of ensuring that. Doctors should tell the patient their vision of how information will be used in caring for the patient's health, whether merely for a particular care episode or providing ongoing care in a more holistic way. Providing written patient information is one basis of communication. But frank and clear oral explanation is also necessary. However the exchange proceeds, the doctor must understand and record any restrictions that the patient places on using or disclosing his/her information.

An established routine procedure for using a particular form of notation on a patient record, to confirm that the doctor has told the patient how the information will be handled and that the patient understands and agrees, provides good evidence of full consent having been given. It is essential in

telling the patient about how their information will be used, that the doctor assures him or herself that the patient understands and agrees. Doctors will appreciate that often patients sign consent forms without fully understanding what they are signing.

Section Five contains a sample consent form for medical practices to adapt in whatever way may be appropriate, if required.

Access and Correction

A medical practice should develop a policy about how it handles access requests. The policy should make clear:

- 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 providing the information in a timely manner.

Practice procedures should be put in place to:

- ensure that the patient's record contains details of oral or written requests for the patient to have access to his/her records and whether the request has been dealt with in accordance with practice time-lines
- indicate that the treating doctor has reviewed the material being requested to ensure no restrictions to access or disclosure apply
- ensure that restricted material is noted on the record.

Section Five

Privacy Tool Kit

Getting Started Checklist

A GETTING STARTED CHECKLIST		
Checklist	Check	Action/comment
1. Have you read the 10 NPPs?		
2. Have you read this Book and disseminated to staff where appropriate?		
3. Have you considered appointing a Privacy Officer?		
4. Do you understand the concepts of 'primary purpose', 'secondary purpose' and 'reasonable expectations' in terms of patient consent for collection, use and disclosure of information?		
5. Have you conducted a privacy audit of your current practices and procedures?		
6. Have you conducted a security review of your current practices and procedures?		
7. Have you formulated or adopted a privacy policy?		
8. Have you developed a policy about handling requests for access to records?		
9. Have you formulated a procedure to handle complaints or incidents regarding breaches of privacy?		
10. Have you trained your staff in relation to your organisation's privacy policy and procedures?		
11. Are you confident your staff are familiar with the privacy legislation and their individual responsibilities under it within the practice?		
12. Have you developed a protocol for the ongoing review of the organisation's adherence to its privacy policy and procedures, and its compliance with privacy legislation?		

Sample Consent Form

Below is an example of a 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. Patients should be invited to discuss or negotiate their needs, and any disclosure not clearly specified on the form.

Privacy Information and Consent Form

The law gives you certain privacy rights in relation to information that you give to this medical practice. We need your consent to collect personal information about you. The fact that you have come here implies that you consent to us knowing about your health situation either for a particular event or generally. This form explains what your rights are over the use we make of the information and how we may disclose it to other medical service providers.

The information we may ask you to give us is deeply personal. But not having it will restrict our capacity to provide you with the standard of medical care that you expect.

Please carefully read the following information about privacy issues then sign this form where indicated below. It will go on your file and you may examine it or change it at any time.

The main reason we collect information from you is so we can assess, diagnose and treat your illnesses properly and be pro-active in your health care. We will also use the information you provide in the following ways:

- Administration of this medical practice
- Billing, including compliance with Medicare and Health Insurance Commission requirements
- Disclosure to others involved in your health care, including doctors and specialists outside this practice who may become involved in treating you. 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.
- Disclosure to others for medical defence purposes if necessary.

{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 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

PATIENT'S ACKNOWLEDGEMENT:

I have read this form and understand why collecting information about me is necessary. 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. I also understand that failure to provide this medical practice with all the information it needs may restrict the practice's ability to provide the quality of health care and treatment that I want.

I am aware that I have the 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 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 about which I notify this practice now or at any future time.

I acknowledge that I have read this form before signing it and that a member of the staff of this practice has at my request clarified any aspects of it that I did not at first understand.

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

Patient

Staff Information Sheet - Processing Access Requests

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

Since 21 December 2001, all patients are entitled to access the information which their health service providers have collected about them. Access may be no more than providing a copy of the latest medical test reports, or viewing some of the information on file. This checklist is designed to help in more complex circumstances.

1. Clarifying the scope of the request may be necessary, for example, whether the whole file is required, or just certain parts. The patient does not have to give reasons for requesting access.

2. Ensure the person seeking access has legal authority to do so or the consent of a person who has that right.

3. Acknowledge the request and indicate likely costs. In most cases, this acknowledgment should be issued within 14 days of receiving the request for access.

4. Refer the request to the treating doctor or privacy officer for approval and action.

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. All deletions should be made from the copy of the information which the patient will get, NOT ON THE ORIGINAL MEDICAL RECORD.

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

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

10. If information is withheld, give reasons. Consider possible other ways of meeting the request. You are obliged to consider the use of an intermediary.

11. Note on the patient file that access has been granted, or refused as appropriate.

Tips on providing access

- *Supervise patient access to originals (rather than copies) to prevent unauthorised removal, deletion or alteration of records. While letting patients photocopy their own records may save staff time and costs, it may also raise public liability and other privacy issues. Whilst the privacy legislation grants patients access to their files, the doctor or medical practice retains ownership of the records.*
- *Administrative staff should clearly understand that they do not have power to decide whether access should be granted. All requests should be referred to the treating doctor or privacy officer. The treating doctor or privacy officer should approve immediate access only for straightforward requests.*
- *If the privacy officer is not a medical practitioner, a medical practitioner should review the record before granting access to it.*
- *The legislation does not require patients to make written requests to see their information. However, in complex cases, it may be prudent to ask that the request be made in writing. Requests for access should be noted on the file.*
- *Access should be given within 30 days of receipt of request, in most circumstances.*

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.

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:

.....

(eg. 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). 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

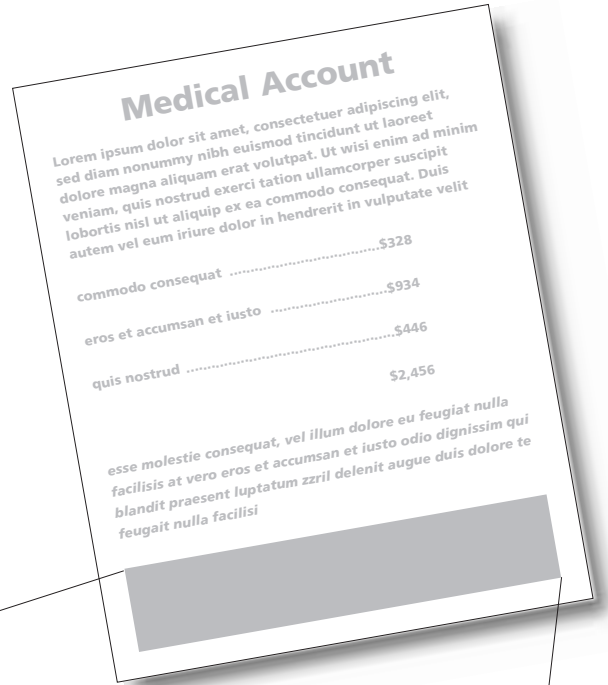
Records provided on / /20 by

Signature of Privacy Officer/Doctor

Note for pathologists and radiologists

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 see their patients only in circumstances 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 an explanation of our information handling policy.

In carrying out the medical services we provide, we may have collected information about you from other members of your treating team, for example, information provided by your referring doctor. We may also have shared information about you with others, for example, by providing (insert as relevant, test results, x-rays, reports) to your referring doctor. We do this only to the extent 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 are 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 the appropriate person in the employer practice or organisation]**

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

- (a) I agree that I shall not, during my period of employment with the organisation, disclose or use any patient files, medical reports or confidential knowledge obtained through my employment with the organisation, other than to perform the usual duties of my employment:
 - a) as set out **[assuming that duty statement is included in employment agreement]** in the agreement to which I am a party and which governs my employment in the organisation or
 - b) which my supervisor has specifically requested me to perform.
- (b) I acknowledge that I may be subject to disciplinary action, which may include immediate termination of my employment, if I commit any breach of the organisation's privacy policy or privacy legislation, whether intentionally or not.
- (c) I acknowledge that clauses (a) and (b) will continue to be binding on me even after the termination of my employment with the organisation, whatever the reason for the termination.
- (d) Upon cessation of my employment with the organisation for whatever reason, I will immediately deliver to the 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 the organisation or its patients past or present.

Signed: Date: / /

Checklist for IT Privacy of the Practice

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

When communicating or transferring information via the telephone, facsimile machine or e-mail, and when it is stored electronically, staff must maintain privacy and confidentiality. The following checklist, largely based on information contained in 'IT Security Guidelines for General Practitioner', asks security-related questions that medical practitioners and their staff should consider and offers a useful guide to compliance with best practice. The full document is available from the General Practitioner Computing Group Website at www.gpcg.org.

Screen-savers

- Are Screen-savers being used? _____
- Do Screen-savers start up automatically after a set period of no PC activity? Is the set period long or short? _____
- Are Screen-savers used with the password protection option enabled? _____

Passwords

- Is the number of attempts allowed to enter an incorrect password limited? _____
- Are the passwords used difficult to guess? _____
- Are passwords changed if other people come into possession of them? _____
- Are default accounts and passwords changed before systems are used? _____
- Are passwords not written down unnecessarily? _____
- Are passwords not shared? _____

Basic security and PC guidelines

- Are computer monitors positioned so that unauthorised persons cannot see them without their behaviour becoming noticed? _____
- Do staff log out of systems while away from PCs? _____
- Have staff attended basic security awareness training? _____
- Have policies and guidelines been developed for the use of computing resources and distributed to all staff? _____

Backups

- Is there is a data backup process in place? _____
- Are backup media rotated before being re-used? _____
- Are backups periodically tested? _____
- Are backup tapes or other media stored securely or destroyed? _____

Anti-virus management

- Do all the organisation's computers have anti-virus software installed and configured to run automatically? _____
- Are all files from external sources checked for viruses before being opened? _____
- Is there a routine for updating anti-virus software that is distributed promptly when available? _____

Accessing the Internet

- Does the organisation have a staff Internet usage policy and it is distributed to all staff?

- Is a stand-alone computer used to access the Internet, alternatively, is there a firewall between the internal network and the Internet?

- Are modems configured to dial-out on demand only?

Communicating by e-mail

- Does the organisation have a staff e-mail usage policy distributed to all staff?

- Is all confidential information sent by e-mail encrypted before sending?

- Do all outgoing E-mails carry a confidentiality and privilege notice?

- Do all staff know the types of E-mail attachments that they should not open if received from unknown senders?

- Is work-related e-mail handled, stored and disposed of in accordance with relevant legislation?

Access controls

- Does the organisation grant access privileges granted only on a 'need to know' basis?

- Does the organisation have an access approval process?

- Have access administration responsibilities been assigned?

- Are access privileges periodically reviewed?

- Have contractors who require access to the system signed confidentiality agreements?

Physical security

- Is all IT equipment stored in secure private areas of the practice?

- Are building security measures in place?

- Have additional measures been taken for laptop/palmtop computers?

Disaster recovery / business continuity planning

- Does the organisation have a Disaster Recovery Plan?

- Does the organisation have maintenance and/or service level agreements in place for equipment and software?

- Does the plan contain business continuity and recovery procedures?

- Is there a device with electrical filtering used to prevent damage to hardware?

- Is there a fail-safe data system in place, such as disk mirroring?

Commercial use

- Does the organisation have protocols in place to protect e-held data from exploitation by organisations that might sell it for commercial purposes?

Data disposal

- 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 on the hard drive even if it has been re-formatted. Consult your IT advisor about how to deal with this.

- Does the organisation have procedures in place for removing, destroying or cleansing electronic data storage devices once they are no longer required (particularly from floppy disks, hard drives, backup tapes, note-book computers and the like when they are no longer in use)?

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 the Website collects personal information, it should tell customers:

- 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.

Website Privacy Statement

This information sheet 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 Sample 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.

Poster and patient information pamphlets

To comply with NPP 5 –Openness– for ‘getting started’ purposes, a sample poster, and two patient information pamphlets either or both of which can be provided to patients who want to know more about how their information is handled, are set out on this and the following 4 pages.

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 purpose only of ‘episodic’ care. Doctors should consider whether this approach suits their particular practice, or whether they should draft their own privacy documents 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.

Sample Patient Information Poster



Your Privacy : Our Policy

The provision of quality health care requires a doctor-patient relationship of trust and confidentiality. Consistent with our commitment to quality care this practice has developed a policy to protect patient privacy in compliance with privacy legislation.

Our policy informs you:

- That we need your consent to collect information about you
- Why we need to collect that information
- How your information will be used by us and to whom we may need to disclose it
- That you may request access to the information that we hold about you
- That you may discuss any concerns you have about how we handle your information

Further information on our policy is available. Talk to your Doctor or ask for a copy of our privacy policy pamphlet.

(Insert Practice Details Here)

Sample Patient Information Sheet



Your Privacy is Our Business

The provision of quality health care is our principle concern. It requires a doctor-patient relationship of trust and confidentiality. Your doctor regards patient health information as confidential and will only collect this information with patient consent.

A patient's personal information is handled in accordance with this practice's privacy policy and consistent with the privacy legislation. Patients are entitled to know what personal information is held about them; how and under what circumstances they may have access to it; why it is held; its use; to whom and under what circumstances it may be disclosed; when consent is required for these purposes; and how it is stored.

Every effort will be made to discuss these matters with patients at the time personal health information is collected from patients attending this practice. Because there will be occasions when it is not practicable to make patients aware of these matters at the time of collection this brochure is designed to outline how this practice endeavours to protect the privacy of patients' personal health information.

Collection, Use and disclosure of your information

Information about a patient's medical and family health history is needed to provide accurate medical diagnoses and appropriate treatment. We will be fair in the way we collect information about our patients. This information is generally collected from the patient, and otherwise with the patient's consent. However, from time to time we may receive patient information from others. When this occurs we will, wherever possible, make sure the patient knows we have received this information.

Medical care requires full knowledge of patient health information by all members of a medical team. To ensure quality and continuity of patient care a patient's health information has to be shared with other health care providers from time to time. Some information about patients is also provided to Medicare, and private health funds if relevant, for billing and medical rebate purposes.

The doctors in this practice are members of various medical and professional bodies including medical defence organisations. There may be occasions when disclosure of patient information is required for medical defence purposes.

There are also circumstances where a medical practitioner is legally bound to disclose personal information. An example of this is the mandatory reporting of communicable diseases.

It is necessary for us to keep patients' information after their last attendance at this practice for as long as is required by law or is prudent having regard to administrative requirements.

Access

A patient has a right to access their information. They may ask to view the information or ask for a copy of a part or the whole record. While not required to give reasons for their request, a patient may be asked to clarify the scope of the request.

There are some circumstances in which access may be denied but in such an event, the patient will be advised of the reason.

A charge may be payable where the practice incurs costs in providing access. This will depend on the nature of the access.

The material over which the doctor has copyright might be subject to conditions that prevent further copying or publication without the doctor's permission.

If a patient finds that the information held on them is not accurate or complete, the patient may have that information amended accordingly.

Upon request a patient's health information held by this practice will be made available to another health service provider.

Parents/Guardians and Children

The right of children to privacy of their health information, based on the professional judgement of the doctor and consistent with the law, might at times restrict access to this information by parents or guardians.

Complaints

It is important to us that your expectations about the way in which we handle your information are the same as ours.

Please do not hesitate to discuss any concerns, questions or complaints about any issues related to the privacy of your personal information with your doctor.

If you are still dissatisfied you can complain to the Federal Privacy Commissioner whose contact details are:

Level 8 Piccadilly Tower
133 Castlereagh Street
Sydney NSW 2000

GPO Box 5218
Sydney NSW 2000
Privacy Hotline: 1300 363 992
Website: www.privacy.gov.au

Further information

Further information about an individual's privacy rights can be obtained from the Office of the Federal Privacy Commissioner.

Sample General Information Sheet



Understanding Privacy - The NPPs at a Glance

The Federal Privacy Act incorporates 10 National Privacy Principles (NPPs) that set out the rules for the handling of personal information in the private sector. In the interests of providing quality health care this practice has developed a privacy policy that complies with the privacy legislation and the NPPs.

Collection

It is necessary for us to collect personal information from patients and sometimes others associated with their health care in order to attend to their health needs and for associated administrative purposes.

Sensitive Information

Health information is 'sensitive information' for the purposes of privacy legislation. This means that generally patients' consent will be sought to collect health information that is necessary to make an accurate medical diagnosis, prescribe appropriate treatment and to be proactive in patient health care.

Use and Disclosure

A patient's personal health information is used or disclosed for purposes directly related to their health care and in ways that are consistent with a patient's expectations. In the interests of the highest quality and continuity of health care this may include sharing information with other health care providers who comprise of patient's medical team from time to time. In addition there are circumstances when information has to be disclosed without patient consent, such as:

- Emergency situations.
- By law, doctors are sometimes required to disclose information for public interest reasons, eg mandatory reporting of some communicable diseases.
- It may be necessary to disclose information about a patient to fulfil a medical indemnity insurance obligation.
- Provision of information to Medicare or private health funds, if relevant, for billing and medical rebate purposes.

In general a patient's health information will not be used for any other purposes without their consent. There are some necessary purposes of collection for which information will be used beyond providing health care, such as professional accreditation, quality assessments, clinical auditing, billing and so forth.

Data quality

All patient information held by this practice relevant to the functions of providing health care will be maintained in a form that is accurate, complete and up to date.

Data security

The storage, use and, where necessary, transfer of personal health information will be undertaken in a secure manner that protects patient privacy. It is necessary for medical practices to keep patient information after a patient's last attendance for as long as is required by law or is prudent having regard to administrative requirements.

Openness

This practice has made this and other material available to patients to inform them of our policies on management of personal information. On request this practice will let patients know, generally, what sort of personal information we hold, for what purposes, and how we collect, hold, use and disclose that information.

Access and correction

Patients may request access to their personal health information held by this practice.

- Where necessary, patients will be given the opportunity to amend any personal information held that is incorrect.
- There are some circumstance in which access is restricted, and in these cases reasons for denying access will be explained.
- A charge may be payable where the practice incurs costs in providing access.
- This practice acknowledges the right of children to privacy of their health information. Based on the professional judgement of the doctor and consistent with the law, it might at times be necessary to restrict access to personal health information by parents and guardians. Upon request a patient's health information held by this practice will be made available to another health service provider.

Identifiers

These are the numbers, letters or symbols that are used to identify patients with or without the use of a name. (eg Medicare numbers). We will limit the use of identifiers assigned to patients by Commonwealth Government agencies to those uses necessary to fulfil the obligations to those agencies.

Anonymity

A patient has a right to be dealt with anonymously, provided this is lawful and practicable or possible for Medicare and insurance rebate purposes. It could also be dangerous to the patient's health.

Transborder data flows

Individual's privacy is protected Australia-wide by privacy laws. We will take steps to protect patient privacy if information is to be sent interstate or outside Australia.

Complaints

Patients should feel free to discuss any concerns, questions or complaints about any issues related to the privacy of their personal information with their doctor. If a patient is dissatisfied the Federal Privacy Commissioner, whose details are below, handles complaints.

Further information

Further information about an individual's privacy rights can be obtained from the Office of the Federal Privacy Commissioner at:

Level 8 Piccadilly Tower
133 Castlereagh Street
Sydney NSW 2000

GPO Box 5218
Sydney NSW 2000
Privacy Hotline: 1300 363 992
Website: www.privacy.gov.au

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
 - (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 subsection 100(2).

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 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.

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.

