



Privacy Policy in Community Pathology

Sydney, January 2002
Revised version 1.2: 13 May 2002

TABLE OF CONTENTS

1	INTRODUCTION	3
1.1	Scope, audience and intent of this document	3
1.2	Privacy legislation for community pathology	3
1.3	Status of this document	4
1.4	Other laws, codes and guidelines	4
2	THE PATHOLOGY PROCESS	6
2.1	Requester	6
2.2	Patient	6
2.3	Collection	6
2.4	Courier	7
2.5	Registration	7
2.6	Analysis	7
2.7	Consultation	7
2.8	Report	7
2.9	Account	8
2.10	Other regulation of the pathology process	8
3	THE PATHOLOGY INFORMATION LIFE CYCLE AND NPPS	10
3.1	Overview	10
3.2	Collecting information	12
3.2.1	NPP 1 - Collection	12
3.2.2	NPP 10 - Sensitive information	13
3.2.3	NPP 8 – Anonymity	15
3.3	Storage and Maintenance	16
3.3.1	NPP 3 – Data quality	16
3.3.2	NPP 4 – Data security	16
3.4	Use of information and disclosure	17
3.4.1	NPP 2 – Use & disclosure	17
3.4.2	NPP 9 – Transborder data flows	20
3.4.3	NPP 7 – Identifiers	21
3.5	Access by the individual	22
3.5.1	NPP 6 – Access and correction	22
3.6	Openness	24
3.6.1	NPP 5 – Openness	24
4	COMPLAINTS HANDLING	25
	APPENDIX 1 - NATIONAL PRIVACY PRINCIPLES	26
	APPENDIX 2 - DEFINITIONS FROM THE PRIVACY ACT	35
	APPENDIX 3 – REFERENCES AND OTHER SOURCES OF INFORMATION	36

1 INTRODUCTION

Australians believe privacy is important especially in relation to information concerning their health. This has been reaffirmed in recent work on community attitudes by the Office of the Federal Privacy Commissioner.

When there is good communication between health service providers and their clients there are fewer complaints. Experience has shown this to be true of pathology providers and their patients. It applies no less in the area of privacy.

When pathology practices are open about the health information they hold, and how they use and disclose it, surprises are unlikely. With fewer surprises there are likely to be fewer complaints.

This document aims to facilitate that communication and as a consequence fulfil many of the obligations that pathology providers have to their patients in the area of privacy.

1.1 Scope, audience and intent of this document

This policy document has been produced by the Australian Association of Pathology Practices (AAPP) for its members and their clients. The AAPP is the principal industry body for private pathology practice in Australia.

The intention of the document is to explain the application of the Federal Privacy Commissioner's "*Guidelines on Privacy in the Private Health Sector*" as it applies to community pathology and to fulfil the requirement of National Privacy Principle 5 to have a Privacy Policy.

Each employee and contractor of a pathology practice needs to be aware of their obligations and those of the organisation in respect of privacy. This document aims to assist in this regard.

1.2 Privacy legislation for community pathology

The Privacy Amendment (Private Sector) Act 2000 (Commonwealth) extends the operation of the *Privacy Act 1988* (the Act) to cover the private health sector throughout Australia and so covers all private pathology practices regardless of their size or nature of operation. The legislation came into effect on the 21st December 2001.

The Privacy Commissioner writes: "*The Act ... gives important privacy rights to individuals but also recognises the rights of business to achieve its objectives in an efficient way. The Federal Privacy Commissioner ... is required to uphold this ideal and to work with all stakeholders, in a balanced manner, to ensure that the privacy rights of individuals are protected while enabling business to continue to operate efficiently.*"

1.3 Status of this document

It is intended that this document be an industry standard and that it should be read in conjunction with “*Guidelines on Privacy in the Private Health Sector*” published by the Federal Privacy Commissioner.

The document is explanatory in nature and does not purport to be an independent “guide” as that term is used in the legislated co-regulatory privacy scheme.

Members of the AAPP intend complying with the National Privacy Principles (NPPs). The complaint handling procedure used will be that described by the Commissioner and there is no intention to establish an independent industry adjudicator.

The standards described here do not go beyond the legislative requirements of the NPPs and are not intended in any way to restrict competition.

1.4 Other laws, codes and guidelines

Community pathology in Australia is highly regulated with many sometimes competing requirements for operational standards (see 2.10). This is also true in the area of privacy.

The new provisions and the associated guidelines do not cover Commonwealth, State and Territory public sector health service providers where other laws can and often do apply.

Many private pathology practices also provide services to the public sector. This can be:

- Private patients whose testing is performed by private laboratories (within public hospitals)
- Private Laboratories performing public hospital patient testing
- Private laboratories referring tests to public facilities

Records of public patients kept in a private practice are considered by the Federal Privacy Commissioner to be covered by the Privacy Act.

In addition to this complexity though there are also State privacy laws that apply to private pathology practices.

In Victoria on 1 July 2002 the Health Privacy Principles and subsequent determinations associated with the *Health Records Act 2001 (Vic)* will become legally binding on private pathology practices. This will be administered by the Victorian Health Services Commissioner.

In NSW *The Privacy and Personal Information Protection Act 1998* gives enforceable remedies in relation to privacy breaches only by public sector agencies but the Act gives the NSW Privacy Commissioner the power to investigate and conciliate complaints about breaches of privacy by organisations and individuals who are not public sector agencies.

There may be others. The only practical approach for a pathology practice is to adopt the most rigorous of the laws that apply with the expectation that this will meet the requirements of the others. Clearly over time there must be harmonization of these laws and standards and it is the policy of the AAPP to promote this.

References to documents that may be relevant are made in Appendix 3.

2 THE PATHOLOGY PROCESS

Pathology is a specialist medical service. A description of the pathology process is provided here to aid the understanding of all parties in how information is collected, handled and used in community pathology.

2.1 Requester

The requester is the person who makes an order (request) for pathology testing. In most cases this is a referring doctor looking to manage a patient's medical condition or to form a diagnosis.

Dental practitioners, nurse practitioners and others also order pathology on behalf of a patient. In some cases, although rarely, patients self refer

A request often contains some medical history to aid in the selection and interpretation of tests. In some cases especially where associated with genetic testing this includes information about relatives.

There are certain other pieces of information required by legislation and regulation required with a request some of which is to allow for claiming under Medicare.

2.2 Patient

In pathology the subject, client or individual having the pathology test is generally referred to as the patient. In practice there may be no direct contact between the pathology practice and the patient. The pathology practice may only ever receive a sample and request.

There is an assumed consent to the collection and use of personal information when an individual consents to the collection of a specimen.

2.3 Collection

The collection of pathology specimens can occur at the requester's surgery, in hospital, at home or at an Approved Collection Centre. All specimens are identified and labelled to avoid mix-up.

Some tests require preparation before collection and this may depend on information from the patient.

Most collections are invasive by their nature. In some circumstances a test or procedure may be added or deleted based on the information taken at the collection centre.

2.4 Courier

Most specimens are transported from where they have been collected to the laboratory by trained drivers in dedicated vehicles.

2.5 Registration

Information from the request is recorded in the laboratory information system and the specimen is prepared for testing. Specimens are allocated unique identifiers

Some requests may be faxed or sent as electronic messages to the laboratory. Standards describe the security and confidentiality requirements for these transmissions.

2.6 Analysis

A laboratory is often divided into sections and it is common to have more than one group working on a patient's sample(s) at the same time.

No laboratory in Australia can do every test that is requested of it and so requests and specimens may be referred to other laboratories. In some cases a pathologist may seek advice from a pathologist in a different practice to help form their opinion. In both circumstances, although rare, this may be outside Australia.

2.7 Consultation

Discussion can take place between members of the pathology practice and the requester. This happens when a requester rings for a result, when the results require urgent action or where there is a significant result that warrants further consideration of the patient's history.

2.8 Report

A pathology report is produced. This includes results and may contain advice on management and/or further testing. This report almost always goes to the requester, copies of the reports are kept by the pathologist and copies may also be directed to others as directed by the requester or patient.

Most reports are printed and delivered by pathology courier or post. Reports may be phoned, faxed or sent as electronic messages. Standards describe the security and confidentiality requirements for these transmissions.

2.9 Account

Most community pathology in Australia is paid for directly or indirectly by the Commonwealth under Medicare. There are requirements for certain information under the Health Insurance Act. The bulk of community pathology is billed direct to Medicare. There are circumstances however where bills are sent to individuals or organisations as directed on the request form or by other agreement. Debt recovery action is required in some cases.

2.10 Other regulation of the pathology process

While the description above is true for most community pathology in Australia there are many exceptions. Where they are recognised as relevant in terms of considerations for privacy these are discussed in the next section.

Privacy is just one element of the pathology process that is subject to regulation. Some of those involved in that regulation are shown against each of the steps in the pathology process in the diagram below.

PATHOLOGY REGULATION



Pathology Processes

Requester Patient Requester's Staff Hospitals & Nursing homes Commercial	Marketing Sales	Doctor Collect Self Collect Practice Collect	Client APCC Laboratory	Receipt Registration Preparation Distribution	Microbiology Biochemistry Haematology Anatomical	Results Inquiry Client Consultation Client Mgmt	Report Delivery	HIC Patients Insurers Commercial
---	--------------------	--	------------------------------	--	---	---	--------------------	---

Government, Laws and Standards Setters

Medical Registration Board	Medicare Private Health Insurance Legislation	NPAAC / NATA / RCPA accreditation	NPAAC / NATA /RCPA accreditation	NPAAC / NATA / RCPA accreditation	NPAAC / NATA / RCPA accreditation	NPAAC / NATA / RCPA accreditation	NPAAC / NATA / RCPA accreditation	HIC -APA HIC - Professional Review
Medicare Participation Review Panel	Health Complaints Commissioners	HIC - APCC inspection	IATA State Transport Act EPA		TGA HIC - APL	RCPA HIC - APP	Privacy Act AS4400, AS4444	Health Insurance Complaints Commissioner
Colleges Divisions Scientific Societies	ACCC	Local Government - planning & health regulations			MSAC NHMRC Vic PSAB	AMC - AMEB Medical Boards Professional Indemnity	NHMRC Registrations	Electronic Transaction Legislation
QUPC		Nurses Registration Board			AQIS			PCC/ PSTC
NHMRC		Poisons Act Human Tissues Act Public Liability			Scientific and Technical Training Accreditation Board EPA OH&S Acts Professional Indemnity			ACCC- pricing Private Health Insurance Legislation (including simplified billing)

3 THE PATHOLOGY INFORMATION LIFE CYCLE AND NPPS

The Privacy Act only applies to ‘personal information’. That is, information about an individual who can be identified, or whose identity could be reasonably ascertained, from the information.

Personal information must relate to a natural, living person. A ‘natural person’ is a human being as opposed to an entity recognised by the law as a ‘legal person’, such as a company.

The National Privacy Principles(NPPs) do not apply to de-identified information or statistical data sets, which would not allow individuals to be identified.

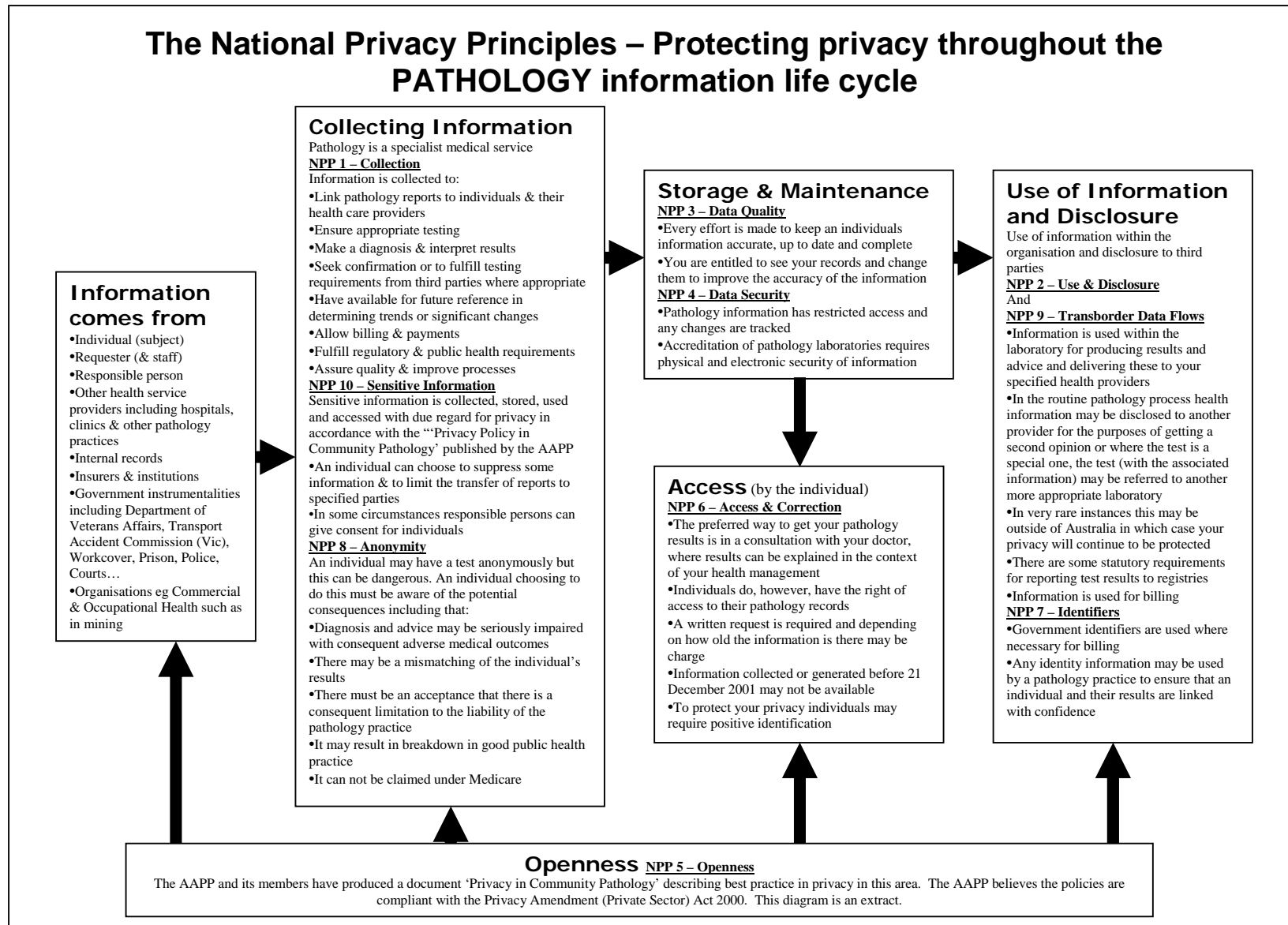
Definitions of the different kinds of information referred to in the Act are given in Appendix 2. For practical purposes any information collected from a patient by a pathology practice should be considered health information and so sensitive, regardless of how it is collected and stored.

3.1 Overview

To assist patients in understanding why information is collected and how it is used a brochure has been developed. The brochure contains the following advice to patients:

- We need your consent to collect information about you.
- We need information from you to be able to provide you with reliable results and your doctors with helpful advice.
- We will be fair in the way we collect information.
- Most information is collected at the time that a pathology request is written out by your doctor. Your doctor will generally explain why he or she is recording the information and where it is going to.
- Where you visit a pathology collection centre and more information is sought you will be asked if it is OK to collect that information.
- Pathology practices have their record systems inspected for laboratory accreditation and they must be reliable and secure.
- The best way to get your results is in consultation with your doctor so they can be explained in the context of your health care.
- You may, however, request access to information we hold about you.
- You may discuss any concerns you may have about how we handle your information. You should speak to your pathology practice first (Contact information is provided).

Also shown in the brochure is a diagram giving a summary of how the NPPs apply to community pathology and this is shown below.



Using the same structure as shown in the previous diagram, the National Privacy Principles (NPPs) are provided below along with pertinent annotations relating them to pathology where appropriate.

3.2 Collecting information

3.2.1 NPP 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.

In pathology only necessary information is collected and it is used to:

- Link pathology reports to individuals & their health care providers
- Ensure appropriate testing
- Make a diagnosis & interpret results
- Seek confirmation or to fulfil testing requirements from third parties where appropriate
- Have available for future reference in determining trends or significant changes
- Allow billing & payments
- Fulfil regulatory & public health requirements
- Assure quality & improve processes

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

AAPP members undertake to do this. In particular the Standard for Approved Collection Centres goes to the physical facilities to ensure privacy in conversations between Collectors and their patients. Inspection against these standards forms part of the laboratory accreditation scheme

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;*
- (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.*

The brochure “Privacy and Pathology” produced by each member practice gives contact details for the organisation and its privacy officer. Each of the other issues is also addressed.

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

In addition to information coming directly from an individual, information relevant to a pathology request may come from:

- Requester (& staff)
- Responsible person
- Other health service providers including hospitals, clinics & other pathology practices
- Internal records
- Insurers & institutions
- Government instrumentalities including Department of Veterans Affairs, Transport Accident Commission (Vic), Workcover, Prison, Police, Courts...
- Organisations eg Commercial & Occupational Health such as in mining

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.

The Privacy Commissioner has issued a Temporary Public Interest Determination that ensures family history taking by health service providers is not prevented by the Privacy Act in the following circumstances:

An organisation collects health information from an individual about another individual (a third party) 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) *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*

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 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.*

3.2.2 NPP 10 - Sensitive information

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

- (a) *the individual has consented; or*

For pathology there is an implied consent when a request is written and a specimen collected that information necessary to provide the service is collected and that it will be handled and used as set out in this document.

(b) *the collection is required by law; or*

As described elsewhere some of the information collected is because of law.

(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.*

Most of the information collected from patients and others for pathology testing is collected under this provision.

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.*

Many pathology laboratories are involved in clinical trials and research. Where that is so it is done in accordance with NHMRC and other guidelines for human research which themselves address privacy considerations. In some cases information is collected by law for registries. For some of these such as Pap Smear registers it is possible for the patient to opt out of their involvement in others especially those related to Public Health and Disease Surveillance (eg Cancer Registries) collection and reporting is mandatory.

- 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*

Where this is possible this is done.

- 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.*

3.2.3 NPP 8 – Anonymity

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

In pathology an individual may have a test anonymously but this can be dangerous. An individual choosing to do this must be aware of the potential consequences including that:

- Diagnosis and advice may be seriously impaired with consequent adverse medical outcomes
- There may be a mismatching of the individual's results
- There must be an acceptance that there is a consequent limitation to the liability of the pathology practice
- It may result in breakdown in good public health practice
- It cannot be claimed under Medicare

3.3 Storage and Maintenance

3.3.1 NPP 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.

In pathology every effort is made to keep an individual's information accurate, up to date and complete. Except where it might be a danger to a patient they are entitled to see their records and change them to improve the accuracy of the information

3.3.2 NPP 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.

Accreditation of pathology laboratories requires physical and electronic security of information. Pathology information has restricted access and both access and changes are tracked. It is very rare for a pathology practice to close but not at all uncommon for there to be a change of ownership. Where there is a change in ownership the obligations in respect of health information are transferred. Where a pathology practice does cease business then patients are to be notified through appropriate advertising and suitable arrangements made for transfer or destruction of records.

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.

Most of the information collected and produced by pathology practices is needed for very long periods. In certain circumstances such as with request forms there is a requirement imposed by law. In other cases the material may be required for defence at law. The National Pathology Accreditation Advisory Committee (NPAAC) has published a standard on the "Retention Of Laboratory Records And Diagnostic Material". At a minimum pathology practices must comply with these requirements or lose accreditation. These are considered minimum requirements for good laboratory practice to ensure patient safety and good outcomes.

3.4 Use of information and disclosure

3.4.1 NPP 2 – Use & 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*

As described earlier pathology practices are routinely required to send reports to registries.

- (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.

Pathology practices are routinely subpoenaed to provide pathology reports.

- 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*

When reports are produced from a pathology system a record is made showing where the report was sent.

- 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).*

It is not uncommon for pathology reports to be made available under this provision for patients in hospitals and nursing homes.

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*

In general for pathology:

- Information is used within the laboratory for producing results and advice and delivering these to the specified health providers
- In the routine pathology process health information may be disclosed to another provider for the purposes of getting a second opinion or where the test is a special one, the test (with the associated information) may be referred to another more appropriate laboratory
- There are some statutory requirements for reporting test results to registries
- Information is also used for billing and debt recovery

In addition information may be used for:

- A pathology practice's management, funding, service monitoring, complaint-handling, planning, evaluation and accreditation activities – for example, activities to assess the cost of a particular service
- Disclosure to a medical expert (only for medico-legal opinion), insurer, medical defence organisation, or lawyer, solely for the purpose of addressing liability indemnity arrangements, for example in reporting an adverse incident.
- Disclosure to a lawyer for the defence of anticipated or existing legal proceedings.
- A pathology practice's quality assurance or clinical audit activities, where they evaluate and seek to improve the delivery of a particular treatment or service
- For training of staff within the laboratory

3.4.2 NPP 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 NPPs; 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 NPPs.*

Specialised testing or second opinions may be sought outside Australia in rare circumstances. This should only be where there is a reasonable belief that the recipient is subject to a comparable information privacy scheme and that the transfer of data is necessary for the performance or completion of a pathology request.

3.4.3 NPP 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**.*

Government identifiers are used where necessary for billing as required by law. In addition, however, in pathology any identity information may be used by a pathology practice to ensure that an individual and their results are linked with confidence.

3.5 Access by the individual

3.5.1 NPP 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.*

For good health care the preferred way to deliver pathology results to a patient is for the treating practitioner to provide them in the context of a consultation where results can be explained in the context of overall health management

Individuals do, however, have the right of access to their pathology records except in the circumstances described above.

A written request is required and depending on how old the information is, there may be a charge. Information collected or generated before 21 December 2001 may not be available.

To protect privacy individuals may require positive identification.

3.6 Openness

3.6.1 NPP 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.*

This document and the brochure entitled “Privacy and Pathology, Our Policy to Protect You” issued by AAPP member practices describe the policies of the AAPP and its members.

- 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.*

These documents are available from the AAPP web site (www.aapp.asn.au) or from the AAPP member practices. Brochures are routinely available from the Collection Centres of AAPP member practices and from many Doctor’s surgeries.

4 COMPLAINTS HANDLING

Each pathology practice has appointed a Privacy Officer. In the first instance any concerns from an individual in respect of privacy should be addressed to them. Contact details are given on the back of the brochure entitled “Privacy and Pathology, Our Policy to Protect You” issued by AAPP member practices.

If an individual thinks a health service provider has interfered with their privacy they can however, complain to the Privacy Commissioner but when the Privacy Commissioner receives a complaint, the individual must in most cases be referred back to the provider to give the provider a chance to resolve the complaint directly (see s.40(1A) of the Privacy Act).

If the individual and the provider cannot resolve the complaint between themselves, the Office of the Federal Privacy Commissioner conciliates the complaint using letters and phone calls, or in some cases, face-to-face meetings. In the majority of cases, the complaint is resolved this way.

As a last resort, the Privacy Commissioner can make a formal determination. If a health service provider does not comply with the determination either the Privacy Commissioner or the complainant can seek to have it enforced by the Federal Court. The Privacy Commissioner may also investigate an act or practice that may be a breach of privacy even if there is no complaint (see s.40(2) of the Privacy Act).

The Federal Privacy Commissioner’s Hotline is 1300 363 992.

APPENDIX 1 - NATIONAL PRIVACY PRINCIPLES

Extracted from the Privacy Act (without annotation).

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

- 2.2 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 NPPs; 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 NPPs.

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.

APPENDIX 2 - DEFINITIONS FROM THE PRIVACY ACT

Health information means:

- (a) information or an opinion about:
 - (i) the health or a disability (at any time) of an individual; or
 - (ii) an individual's expressed wishes about the future provision of health services to him or her; or
 - (iii) a health service provided, or to be provided, to an individual; that is also personal information; or
- (b) other personal information collected to provide, or in providing, a health service; or
- (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.

Health service means:

- (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
 - (i) to assess, record, maintain or improve the individual's health; or
 - (ii) to diagnose the individual's illness or disability; or
 - (iii) to treat the individual's illness or disability or suspected illness or disability; or
- (b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

<p>The term health service provider as used in these Guidelines means a provider of a health service. The term 'health service provider' is not separately defined in the Privacy Act.</p>

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.

Sensitive information means:

- (a) information or an opinion about an individual's:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association; or
 - (vii) membership of a trade union; or
 - (viii) sexual preferences or practices; or
 - (ix) criminal record;that is also personal information; or
- (b) health information about an individual.

APPENDIX 3 – REFERENCES AND OTHER SOURCES OF INFORMATION

The Federal Privacy Commissioner has an active web site at www.privacy.gov.au and for health in particular at www.privacy.gov.au/health/index.html. The site includes copies of the “Guidelines on Privacy in the Private Health Sector” and “Health Information and the Privacy Act 1988 -A short guide for the private health sector”.

The Australian Medical Association (AMA) has produced a “Privacy Kit for Medical Practitioners in the Private Sector” for members. This includes a patient information pamphlet, a poster and information and tools for implementing requirements of the Privacy Act in a Medical Practice. (www.ama.com.au)

Standards Australia publishes a number of general standards which may be relevant

- AS 3806 *Compliance Programs*
- AS 4269 *Complaints Handling*
- AS/NZS ISO/IEC 17799:2001 *Information Technology – Code of Practice for Information Security Management*
- AS/NZS 4360 *Risk Management*

There are also health informatics standards that may be relevant

- AS 4700 Series – HL7 Implementation in Australia, in particular
- AS 4700.2 Pathology Orders and Results
- HB 262 : 2002 Pathology Electronic Messaging – Guidelines for pathology messaging between pathology providers and health service providers
- A handbook is being prepared on the application of AS 17799 in the health sector.

The National Pathology Accreditation Advisory Council (NPAAC) has published numerous standards that are used in accrediting pathology laboratories many of which stipulate requirements in relation to health information. These are available at <http://www.health.gov.au/npaac>

The AAPP provided feedback to the Federal Privacy Commissioner in a document entitled “*Draft Health Privacy Guidelines – A Response to a Request for Consultation by the Office of the Federal Privacy Commissioner made by the Australian Association of Pathology Practices Inc. July 2001*”. It has also produced a brochure used by the member practices called “*Privacy and Pathology, Our Policy – To Protect You, December 2001*”

State based legislation and commentary can be found at:

Victoria - www.dhs.vic.gov.au/privstat.htm

NSW -The Privacy and Personal Information Protection Act 1998
www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/