

1. Introduction

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.*”

This document outlines the 10 National Privacy Principles (NPPs), their application to Coastal Pathology, and Coastal Pathology’s policies relating to our patients’ rights and our legal responsibilities in terms of privacy issues dealt with by the Act.

2. The 10 National Privacy Principles

Ten NPPs form the core of the private sector provisions of the Privacy Act. These principles set the minimum standards for privacy that organisations must meet.

The principles cover the whole information handling lifecycle – from the collection of health information, to its storage and maintenance, as well as its use and disclosure.

The principles, as they apply in the **health** sector, are **summarised** below. For more details see the Federal Privacy Commissioner’s *Guidelines on Privacy in the Private Health Sector*.

NPP 1 – Collection and NPP 10 – Sensitive Information

These principles apply to the collection of health information. In general, they require a health service provider to:

- collect only the information necessary to deliver the health service;
- collect lawfully, fairly and not intrusively; and
- obtain a person’s consent to collect health information about them.

Providers also need to ensure that consumers are informed about why their health information is being collected, who is collecting it, how it will be used, to whom it may be given and that they can access it if they wish.

NPP 2 – Use and Disclosure

This principle sets out how providers can use and disclose health information.

‘Use’ refers to the handling of information *within* an organisation.

‘Disclosure’ is the transfer of information to a third party *outside* the organisation.

A health service provider may use or disclose health information:

- for the main reason it was collected (the primary purpose); or
- for directly-related secondary purposes, if the consumer would reasonably expect these; or
- if the consumer gives consent to the proposed use or disclosure; or
- if one of the other provisions under this principle applies.

The key is to make sure that there is alignment between the expectations of the health service provider and those of the consumer about what will be done with the health information.

NPP 3 – Data Quality

Health service providers are required to take reasonable steps to keep health information up-to-date, accurate and complete.

NPP 4 – Data Security

This principle requires that health service providers take reasonable steps to protect and secure health information from loss, misuse and unauthorised access. Information that is no longer needed should be destroyed. As health information may be needed for future care of the individual or for public health reasons, the priority should be to secure the data properly.

NPP 5 – Openness

Health service providers need to be open about how they handle health information. A provider must develop a document for consumers which clearly explains how their organisation handles health information. The document must be made available to anyone who asks for it.

NPP 6 – Access & Correction

Consumers have a general right of access to their own health records. Access can only be denied in certain circumstances - for instance where access can pose a serious risk to a person's life or health. Also, consumers can ask for information about them to be corrected, if it is inaccurate, incomplete or out-of-date. The provider will need to take reasonable steps to correct the information.

NPP 7 – Identifiers

There are restrictions on how Commonwealth government identifiers, such as the Medicare number or the Veterans Affairs number, can be adopted, used or disclosed. At present, a health service provider is not permitted to adopt these identifiers for their own record keeping systems. These identifiers may only be used or disclosed for the reasons they were issued or if other provisions under this principle apply.

NPP 8 – Anonymity

Where lawful and practicable, consumers must be given the option to use health services without identifying themselves.

NPP 9 – Transborder data flows

If health information needs to be transferred out of Australia, this may occur if laws (or a scheme) with similar privacy protection to these principles bind the recipient. Otherwise, health information should only be transferred with the consumer's consent, or if other provisions under this principle apply.

3. The 10 National Privacy Principles and Coastal Pathology

Each of the NPPs (as extracted from the Act) are listed below, along with pertinent annotations relating them to pathology practices in general, and Coastal Pathology specifically, where appropriate.

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.

At Coastal 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.

Coastal Pathology undertakes to do this. In particular, the Standard for Approved Pathology Collection Centres (2006) goes to the physical facilities to ensure privacy in conversations between Collectors and their patients. Inspection against these standards forms part of the laboratory's accreditation.

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.*

Coastal Pathology's brochure "Privacy Law and Coastal Pathology" gives contact details for our organisation and 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 to Coastal Pathology 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 etc
- 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 Determination that ensures family history taking by health service providers (such as Coastal Pathology) 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.

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 practices, including Coastal 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 testing by Coastal Pathology 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, Notifiable Diseases Registries), collection and reporting is **mandatory**. Coastal Pathology abides by these principles.

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.

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 Coastal Pathology advises that **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
- Samples cannot be tested in parallel or reported in cumulative fashion
- 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

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.

Coastal Pathology makes every effort 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. Where an individual requests a significant change to his or her stored health information, there may be important medical and legal reasons for retaining a complete record. Consequently, the requested changes will be appended, but the original information may also be retained in the record.

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 Coastal Pathology requires physical and electronic security of information. Pathology information has restricted password-protected access, and both access and changes are tracked. Back-up systems are in place to prevent loss of data.

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. Coastal Pathology will ensure these arrangements are made, if closure or change of ownership occurs.

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 such as Coastal Pathology, 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”, with which Coastal Pathology complies. These are considered minimum requirements for good laboratory practice to ensure patient safety and good outcomes.

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. Coastal Pathology will comply with any lawful commands in this regard.

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 our pathology information 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 Coastal Pathology reports to be made available under this provision eg 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 Coastal Pathology:

- Information is used within the laboratory for producing results and advice and delivering these to the specified health providers
- 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 our 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 (eg in reporting an adverse incident.)
- Disclosure to a lawyer for the defence of anticipated or existing legal proceedings.
- Our practice's quality assurance or clinical audit activities, where we evaluate and seek to improve the delivery of a particular treatment or service
- For training of staff within the laboratory

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 will only be done 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.

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 eg Medicare numbers are used where necessary for billing as required by law. In addition, Coastal Pathology uses any identity information to ensure that an individual and their results are linked with confidence.

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.

Coastal Pathology retains the right to deny individual's access to their information if:

- providing access would pose a threat to the life or health of any person
- providing access would have an unreasonable impact on the privacy of other individuals
- the information relates to existing or anticipated legal proceedings between the laboratory and the individual, and the information would not be accessible during those proceedings
- the information is otherwise subject to legal professional privilege
- providing access would reveal the intentions of the organisation in relation to negotiations (other than about the provision of a health service) with the individual, exposing the organisation unreasonably to disadvantage
- providing access would be unlawful
- denying access is required or authorised by or under law
- providing access would be likely to prejudice an investigation of possible unlawful activity
- providing access would be likely to prejudice a law enforcement function performed by, or on behalf of a law enforcement agency
- the request for access is of a kind that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again; or
- the individual has been able to access his or her health information and is making unreasonable and repeated requests for the same information in the same form.

If Coastal Pathology is satisfied that one or more of the above do not apply, information will be released according to the following procedure:

Procedure for Patients to Access Information

- A **written** request is required. A letter of acknowledgement will be issued.
- To protect privacy, individuals may require **positive** identification.
- Coastal Pathology will keep documentation of any discussion with the patient.
- Every reasonable attempt will be made to notify the referring doctor of the request for access.
- Depending on how old the information is, there may be an administration charge.
- A paper copy of requested information will be supplied within 30 days.
- Results will not be provided to anyone other than the patient (for example employers and relatives (with the exception of parents of minors)), without the **written consent** of the patient concerned.

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 Law and Coastal Pathology” describe our policies in relation to management of personal information.

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 our practice. Brochures are routinely available from our Collection Centres.

4. COMPLAINTS HANDLING

Coastal 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 our brochure entitled “Privacy Law and Coastal Pathology”.

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.

REFERENCES AND OTHER SOURCES OF INFORMATION

The **Federal Privacy Commissioner** (<http://www.privacy.gov.au/> & <http://www.privacy.gov.au/health/index.html>)

- “Guidelines on Privacy in the Private Health Sector”
- “Health Information and the Privacy Act 1988 - A short guide for the private health sector”.

The **Australian Medical Association (AMA)**

- “Privacy Kit for Medical Practitioners in the Private Sector”

The **Royal College of Pathologists of Australasia (RCPA)**

- Guideline on Australian Privacy Principles (2007)
- Guideline on Release of Pathology Results to Patients (2007)
-

Standards Australia (<http://www.standards.com.au/catalogue/script/search.asp>)

- 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.*
- AS 4700 Series – HL7 Implementation in Australia
- AS 4700.2 Pathology Orders and Results
- HB 262 : 2002 Pathology Electronic Messaging – Guidelines for pathology messaging between pathology providers and health service providers

The **National Pathology Accreditation Advisory Council (NPAAC)**

<http://www.health.gov.au/npaac/publication.htm>

- Requirements For Information Communication (2007 Edition)
- Guidelines for Approved Pathology Collection Centres (2006 Edition)
- Retention Of Laboratory Records And Diagnostic Material

The **Australian Association of Pathology Practices (AAPP)**

- “Privacy Policy in Community Pathology “ (2001)
- “Privacy and Pathology, Our Policy – To Protect You” (2001)

Queensland State Government Legislation

- Public Health Act 2005
- Public Health Regulation 2005

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

*2.1 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 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.

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.

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.