Privacy Policy

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.*"

From 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian, ACT and Norfolk Island Government agencies.

This document outlines the 13 Australian Privacy Principles (APPs), 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. Australian Privacy Principles (APPs) (2013)

APP 1 — Open and transparent management of personal information
Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information
Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

3. APPs Details And Coastal Pathology Policies

The following information is copied from the Privacy Fact Sheet 17 – Australian Privacy Principles, and provides the text of the 13 APPs from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* which amends the *Privacy Act 1988*. For the latest versions of these Acts visit the ComLaw website: www.comlaw.gov.au.

PART 1—CONSIDERATION OF PERSONAL INFORMATION PRIVACY

AUSTRALIAN PRIVACY PRINCIPLE 1*—OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION*

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

Coastal Pathology will endeavour to comply with the Australian Privacy Principles at all times.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up to date policy (the *APP privacy policy*) about the management of personal information by the entity.

Coastal Pathology has and maintains a Privacy Policy.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

Coastal Pathology holds personal information such as: name, date of birth, address, phone numbers, Medicare/DVA number, health fund membership details.

(b) how the entity collects and holds personal information;

This information is generally obtained from pathology request forms and pathology specimen labels, referred to Coastal Pathology by a range of medical practitioners and health care facilities. The information is held in a secured encrypted database.

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

This information is used to assist in the healthcare of the person in question.

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

Individuals can enquire about accessing their personal information by contacting the Privacy Officer by email (enquiries@coastalapthology.com.au) or phoning 07 5456 4830 during office hours. Alternatively, please see the website for more details (www.coastalpathology.com.au).

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

Any complaints about privacy breaches can be submitted to the Privacy Officer (details above). If the individual is not satisfied with the response to their complaint, they may also contact the Office of the Australian Information Commissioner (Phone: 1300 363 992; Fax: 02 9284 9666; email: enquiries@oiac.gov.au; or Post: GPO Box 5218 SYDNEY, NSW, 2001).

(f) whether the entity is likely to disclose personal information to overseas recipients;

This information is not likely to be disclosed to overseas recipients.

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

This information is not likely to be disclosed to overseas recipients.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

The Privacy Policy is available on our website: www.coastalpathology.com.au .

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

A paper copy of our Privacy Policy can be obtained by contacting the Privacy Officer by email (enquiries@coastalapthology.com.au) or phoning 07 5456 4830 during office hours.

AUSTRALIAN PRIVACY PRINCIPLE 2*—ANONYMITY AND PSEUDONYMITY*

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/ tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

In pathology, an individual may have a test anonymously or under a pseudonym 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

PART 2—COLLECTION OF PERSONAL INFORMATION

AUSTRALIAN PRIVACY PRINCIPLE 3—COLLECTION OF SOLICITED PERSONAL INFORMATION

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

Coastal Pathology undertakes to collect personal/sensitive information which is necessary for its healthcare activity, and only by lawful and fair means and not in an unreasonably intrusive way. Consent is implied by the completion of a Pathology Request form by the person's medical practitioner. Also, 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.

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

AUSTRALIAN PRIVACY PRINCIPLE 4*—DEALING WITH UNSOLICITED PERSONAL INFORMATION*

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

In general, Coastal Pathology will not collect or hold unsolicited personal information.

AUSTRALIAN PRIVACY PRINCIPLE 5*—NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION*

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order— the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/ tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Coastal Pathology endeavours to abide by this APP at all times.

PART 3—DEALING WITH PERSONAL INFORMATION

AUSTRALIAN PRIVACY PRINCIPLE 6—USE OR DISCLOSURE OF PERSONAL INFORMATION

USE OR DISCLOSURE

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

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:

- 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

AUSTRALIAN PRIVACY PRINCIPLE 7*—DIRECT MARKETING*

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception—contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

Coastal Pathology endeavours to abide by this APP at all times.

AUSTRALIAN PRIVACY PRINCIPLE 8*—CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION*

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For *permitted general situation*, see section 16A.

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.

AUSTRALIAN PRIVACY PRINCIPLE 9*—ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS*

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For *permitted general situation*, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

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

Coastal Pathology collects, holds and uses government identifiers such as Medicare Number and DVA number, for purposes of ensuring patient identity and billing only.

AUSTRALIAN PRIVACY PRINCIPLE 10*—QUALITY OF PERSONAL INFORMATION*

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up to date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

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, Patients 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.

AUSTRALIAN PRIVACY PRINCIPLE 11*—SECURITY OF PERSONAL INFORMATION*

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

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, 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. 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 requirements are considered minimum requirements for good laboratory practice to ensure patient safety and good outcomes.

AUSTRALIAN PRIVACY PRINCIPLE 12*—ACCESS TO PERSONAL INFORMATION*

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

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

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

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/ tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

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 (12.3).
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

Refer to appropriate documentation in Office Manual which outlines the procedure based on the following principles:

- A written request is required. A letter of acknowledgement will be issued.
- To protect privacy, individuals will be required to supply positive photographic identification.
- Coastal Pathology will keep documentation of any discussion with the patient.
- With patient consent, every reasonable attempt will be made to notify the referring doctor of the request for access.
- Depending on the amount/nature of information required, there will be a variable 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.

AUSTRALIAN PRIVACY PRINCIPLE 13*—CORRECTION OF PERSONAL INFORMATION*

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

Coastal Pathology endeavours to abide by this APP at all times.

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.

If an individual thinks a health service provider has interfered with their privacy they can however, complain to the Australian Information Commissioner, but when the Australian Information 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 Australian Information 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 Australian Information Commissioner can make a formal determination. If a health service provider does not comply with the determination either the Australian Information Commissioner or the complainant can seek to have it enforced by the Federal Court. The Australian Information 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 Australian Information Commissioner's Hotline is 1300 363 992.

REFERENCES AND OTHER SOURCES OF INFORMATION

The **Office of of Australian Information Commissioner (**http://www.oaic.gov.au/)

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 (2013 Edition)

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